МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Збірник праць молодих науковців ЦНТУ

Випуск 12

Кропивницький – 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Збірник праць молодих науковців ЦНТУ

Випуск 12

Кропивницький – 2022

Збірник праць молодих науковців ЦНТУ. – Вип. 12. – Кропивницький: ЦНТУ, 2022 – 461 с.

Збірник праць молодих науковців складається зі змісту, статей та тез здобувачів вищої освіти по матеріалам дипломних робіт.

УДК 651.589

О. Репейник, магістр гр. ЕО-20м
С. Мартиненко, доцент
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНІ АСПЕКТИ СИСТЕМ ВОДОПОСТАЧАННЯ ТА ВОДОВІДВЕДЕННЯ АГРОФІРМИ «ЛІСОВА» ТА ШЛЯХИ ЇХ ПОКРАЩЕННЯ

Проаналізовано стан водозабезпечення та водовідведення в умовах сільськогосподарського підприємства «Агрофірма «Лісова»».

Розглянуто покращення видобувної води

водопостачання та водовідведення, магнітна обробка, гідрострумне очищення, відстійник, елеватор, свинарник

Водопостачання та водовідведення є важливою умовою ефективного господарювання та збереження довкілля.

Актуальність теми. В умовах зростаючого антропогенного навантаження на природні об’єкти, зокрема в сільському господарстві, якість водних ресурсів змінюється та потребує запровадження вдосконалених систем водопідготовки та очищення стічних вод.

Мета дослідження: знайти шляхи поліпшення умов використання водних ресурсів та запобігання скиду забруднених стічних вод у водойми

Завдання:

- вивчити питання забезпечення питною водою об’єктів агрофірми
- з’ясувати потребу в облаштуванні очисних споруд та відстійників

Об'єкт дослідження: система водопостачання та водовідведення Агрофірми «Лісова».

Предмет дослідження: використання та очистка водних ресурсів.

Результати досліджень.

Агрофірма «Лісова» займається веденням рослинництва та тваринництва, та поступово збільшує свої потужності, у зв’язку з чим є потреба у вдосконаленні системи водопостачання та поводження зі стічними водами. Споруди і технології водопідготовки обираються в залежності від потреб споживачів.

Схема водопостачання являє собою сукупність інженерно-технічних споруд, послідовно розташованих на місцевості (рис.1)

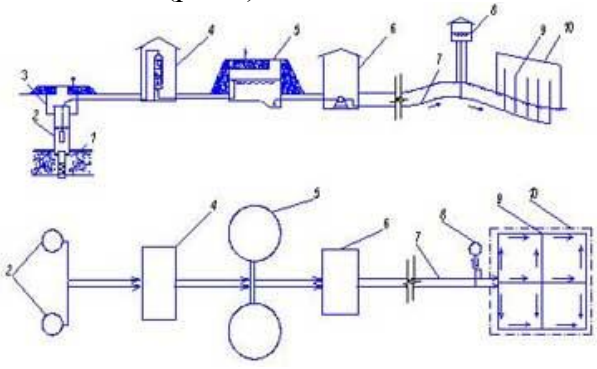


Рис. 1 - Схема водопостачання при використанні місцевих підземних вод: 1 - експлуатаційний водоносний пласт; 2 - водозабірна свердловина; 3 - насосна станція І підняття, 4 - станція поліпшення якості

води; 5 - резервуари чистої води; 6 - насосна станція II підняття; 7 - напірні водоводи; 8 - водонапірна башта, 9 - водопровідна мережа; 10 - об'єкт водопостачання.

«Спорудами для забору підземних вод (рис. 2) є як правило водозабірна свердловина. Вода з свердловин забирається з глибини електронасосами насосної станції I підняття, та подається на установку станції поліпшення якості води. Оброблену воду під залишковим напором насосів I підняття подають в резервуари чистої води (РЧВ). З РЧВ вода забирається насосами II підняття и подається по напірним водоводам у водонапірну башту.

У механізованих системах водопостачання агрофірми для створення потрібного тиску в мережі в період вимкнення насоса, створення і зберігання запасів та регулювання подавання води застосовано водонапірна споруда збірно-блочна безшатрова башта конструкції інженера А.А. Рожновського» [1,2].

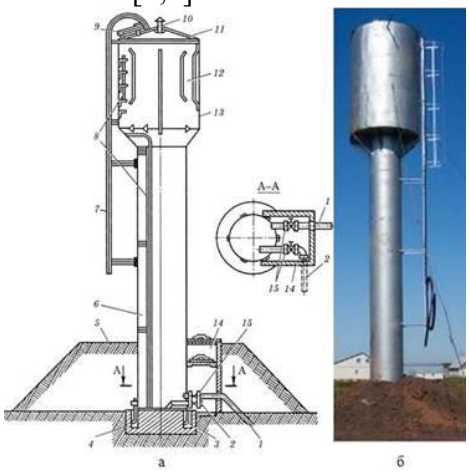


Рис. 2 - Будова безшатрової водонапірної башти конструкції А. А. Рожновського (а) та її загальний вигляд (б):

«1 – напірно-розвідна труба; 2 – зливна труба; 3 – анкерні болти; 4 – фундамент; 5 – земляний вал (обсипка); 6 – колона; 7 – зовнішня драбина; 8 – внутрішні драбини; 9 – люк; 10 – вентиляційна труба; 11 – накривка бака; 12 – утримувачі криги; 13 – бак; 14 – оглядовий колодязь; 15 – заслінка

Збірно-блочна водонапірна башта зварена з листового металу, має опору і бак, які під час експлуатації постійно заповнені водою. Башта не обігрівається і спеціальної теплоізоляції не має. Внутрішні стінки обладнані скобами, які ніби армують льодовий шар, що повільно намерзає завтовшки до 300 мм і цим утворює теплоізоляційну оболонку».[5,2,3]

Для покращення якості води ми пропонуємо застосовувати магнітну обробку.

Магнітна обробка води широко застосовується вже багато років у сільському господарстві та інших галузях як доступний, екологічно безпечний та ефективний метод.

Фізична дія магнітного поля на структуру води та катіони солей жорсткості відкриває широкі можливості для використання магнітної обробки води.

Великі перспективи використання магнітної обробки та у водопідготовці для пом'якшення води, оскільки прискорення процесу кристалізації солей у воді при магнітній обробці, призводить до значного зменшення концентрацій розчинених у воді катіонів Ca^{2+} і Mg^{2+} за рахунок процесу кристалізації та зменшення розмірів кристалів, що осаджуються з води, що нагрівається підданій магнітній обробці. Для видалення з води тонких суспензій, що важко осаджуються, використовується здатність намагніченої води прискорювати коагуляцію (злипання і осадження) зважених частинок з подальшим утворенням дрібнодисперсного осаду, що сприяє вилученню з води різного роду суспензій. [4,1]

Магнітна обробка води допомагає не тільки запобігати випаданню солей, що накипають з води, але й значно зменшувати відкладення органічних речовин, наприклад, парафінів.

Магнітна обробка води в порівнянні з традиційними способами пом'якшення води іонним обміном та зворотним осмосом технологічно проста, економічна та екологічно безпечна.

Оброблена магнітним полем вода не набуває ніяких побічних, шкідливих для здоров'я людини властивостей і суттєво не змінює сольового складу, зберігаючи якості питної води.

Використання інших методів та технологій обробки води пов'язане зі збільшенням матеріальних витрат та проблемами утилізації використаних у процесі водо підготовки хімічних реагентів (найчастіше кислот). При цьому часто доводиться вкладати додаткові матеріальні витрати, змінювати режим роботи теплових апаратів, застосовувати спеціальні хімічні реагенти, що змінюють сольовий склад води, що обробляється, та ін.

В іоннообмінних пом'якшувачах води використовуються Na+-катіоніти, які після катіонування регенеруються розчином хлористого натрію (NaCl). Це створює проблеми для довкілля через необхідність утилізації промивних вод із високим вмістом солей натрію. Воду пом'якшують також за допомогою зворотньоосмотичних мембранних фільтрів, які проводять її глибоке знесолення. Основні процеси магнітної обробки:

-при магнітній обробці води відбувається вплив на саму воду, на механічні домішки та іони накипеобразних солей і на природу фізико-хімічних процесів, що протікають у воді, розчинення і кристалізації;

- у воді, що пройшла магнітну обробку, можливі зміни гідратації іонів, розчинності солей, значення pH, що виражається у зміні хімічних реакцій та швидкості корозійних процесів.[6]

Розрахунок відходів, що утворюються та аналіз необхідності влаштування відстійника, виконано на основі того, що загальний об’єм відходів від свинарника, що потрапляють у відстійник 600 л, або 0,6 м^3 за добу.

Відходи елеваторного виробництва після гідрострумного очищення корпусів зерносховища, а точніше вода з пилом і частинками зернової продукції відправляється у відстійник. Очищення елеваторів відбувається не кожен день, а саме два рази на місяць, тому вода не так сильно витрачається, у відстійник потрапляє 1495 л води на одноразове очищення.

Таким чином, за місяць утворюється 1,8 м^3 стічних вод від свинарника та 1,495 м^3 від елеватора. Загалом 3,295 м^3. Об’єм відстійника становить 5,5 м^3, тобто він потребує викачки не частіше одного разу на місяць. Але склад стічних вод для елеватора та свинарника різний. Тому з нашої точки зору, потрібно встановити два відстійника. Один для свинарника (відстійник I), адругий для елеватора (відстійник II) після чого потрібно встановити загальну очисну вигрібну яму з гравієм для очистки стоків щоб забезпечити природне фільтрування стоків в грунт.

Так як для елеватора і свинарника ми пропонуємо зробити окремі відстійники, то для елеватора потрібний не такий великий відстійник як для свинарника, тому ми пропонуємо зробити його розміром в 1,5 м^3 та встановити насос для перекачування з відстійника у загальну очисну вигрібну яму.

Серія насосів «Womar - WQD 20-12-1,5 S» з багатолопатевим робочим колесом і ріжучим механізмом S. E. G (фреза) підходить для перекачування рідин з довгими ниткоподібними волокнами, а також для подрібнення твердих частинок великих розмірів в органічних рідинах.

Застосовується також для відкачування рідин з систем каналізації.

Розміри відстійників нами визначалися з таких міркувань. Для свинарника при щодобовому утворенні 465 л стоків (0,465м^3) рекомендуємо відстійник об’ємом 3,5 м^3 .

Схема водовідведення від виробничих приміщень та майданчиків агрофірми наведена на рис.3.

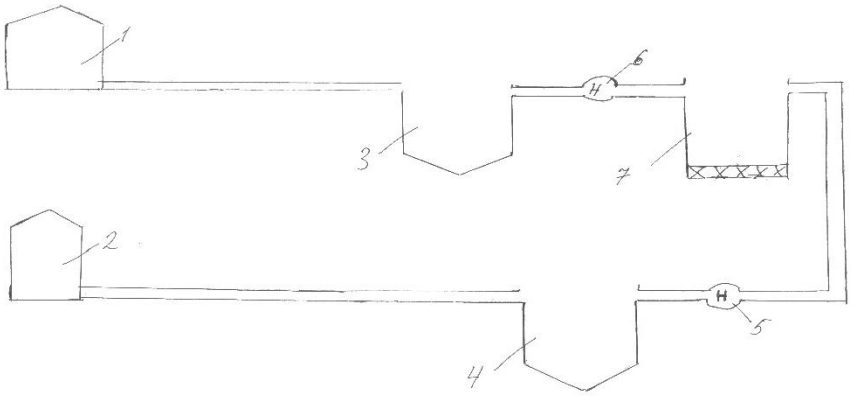


Рис.3 – Схема водовідведення від виробничих приміщень та майданчиків агрофірми
1.Свинарник; 2.Елеватор; 3.Відстійник I; 4.Відстійник II; 5. Насос I; Насос II; 7.Очисний відстійник з гравієм

Стоки з елеватора складають 1495 л (1,495м^3) за одне очищення. Оскільки очищення проводиться двічі за місяць, достатньо відстійника об'ємом 1,5 м^3. Перед наступним промиванням елеватора відстояні стоки перекачуються в загальну очисну вигрібну яму, а відстійник очищують від осаду.

Також потрібно встановити насос для перекачки з відстійника II у загальну очисну вигрібну яму. Також можна встановити насос «Womar - WQD 20-12-1,5 S».

Отже, для відкачування відстійника II (стоки від елеватора), насос буде задіяний 4 – 5 хвилин двічі на місяць. Для відкачування відстійника I (свинарник) потрібно вмикати насос орієнтовно на 40 хвилин теж двічі на місяць. Таким чином буде забезпечено якісне очищення стоків за рахунок достатньо довгого відстоювання. Обов'язково при цьому треба передбачити відкачування у верхній частині накопичених стоків для запобігання попадання в них осаду. Системи відведення стоків передбачають облаштування спеціальних резервуарів або відстійників, в яких накопичуються відходи, далі з часом утримання в ємності відбувається розділ на фракції за вагою. Вода перетікає, а важка фракція осідає на дно. Камери періодично очищують. Відстійники виконують із цегли як економічно доступний і простий варіант, досить тривалої експлуатації.

Очисний відстійник з гравієм потрібно встановити об'ємом 6 м3, щоб його вистачило для елеватора і свинарника. У відстійнику без дна не передбачено герметизації знизу. Фільтр із піску та дрібного щебеню дозволяє рідким стокам невпинно, хоч і повільно, просочуватися в грунт, де вже вони очищуються остаточно за допомогою деструкторів. Відстійник без герметизації дна, за рахунок властивостей грунту, утилізовує гноївку. Мікроорганізми поступово розкладають масу органічних забруднюючих речовин. Грунтові мікроорганізми та навіть дощові черв'яки беруть активну участь у нейтралізації органічної складової забруднень.

Стічні води надходять всередину ємності, а перекриття надійно захищає оточуючих від неприємних запахів. Відстояна рідка складова стічних мас просочується в нижні грунтові шари, а тверді включення осідають на поверхні піщано-гравійного фільтра. Стоки всередині ями з плином часу трохи змінюються за складом. Частково вони переробляються мікроорганізмами, тверді фракції перетворюються в осад, а рідка частина відділяється. З метою зменшити кількість стоків, щоб користуватися послугами асенізаторів якомога рідше, відстійник проектується "без дна". Стіни ємності для стоків ретельно закладають, а на дні залишають просвіт з грунтом. Фільтр виконується з природних матеріалів: піску, щебеню та гравію. Рідка частина стоків повільно просочується в грунт, а тверді фракції залишаються всередині каналізаційної ємності.

Висновок. Таким чином, влаштування системи водопідготовки та водовідведення є важливим економічним та природоохоронним заходом, оскільки дозволить на території виробничої діяльності агрофірми дотриматися санітарних норм та епідеміологічної безпеки,

забезпечить постійний доступ до якісної води та використання її в необхідних об’ємах для життєдіяльності та технологічних процесів елеватора і ферми.

Список літератури

1. Запольський А.К. Водопостачання, водовідведення та якість води: Підручник. - К.: Вища школа, 2005. - 671 с.
2. Хільчевський В.К. Водопостачання і водовідведення: гідроекологічні аспекти: Підручник. - К.: ВПЦ "Київський університет", 1999. - 319 с.
3. Водопостачання і водовідведення : навч. посіб. / О. О. Мацієвська; Нац. ун-т "Львів. політехніка". - Львів : Вид-во Львів. політехніки, 2015. - 140 с. - Бібліогр.: с. 137-140.
4. Хімія: Підручник для 10 кл. загальноосвіт. навч. закл. (профільн. рівень) / Н. М. Буринська, В. М. Депутат, Г. Ф. Сударева, Н. Н. Чайченко — К.: Педагогічна думка, 2010. — 290—292 с.
5. Водопостачання промислових підприємств / Литвиненко Л. Л, Орлов В. О, Орлов А. М. Видавництво: Знання / 2014 - С. 25.
6. https://ecosoft.ua/ua/blog/magnetic-water/

УДК 004

В. Якимчук, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ VOIP ДЛЯ МОДЕЛІ SAAS

У статті розроблено програмне забезпечення, яке призначено для системи VoIP для моделі SaaS. Метою розробки є дослідження та програмна реалізація системи VoIP для моделі SaaS. Об’єктом дослідження є процес VoIP для моделі SaaS. Предметом дослідження є методи VoIP для моделі SaaS. Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи VoIP для моделі SaaS. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерна інженерія, VoIP, SaaS

Постановка проблеми. VoIP (Voice over Internet Protocol) або IP-телефонія – це голосовий зв'язок через інтернет (у відмінності від традиційного телефонного зв'язку, що відбувається через телефонні лінії або мобільну GSM/3G/4G/5G мережу).

На даний момент основним призначенням IP-телефонії є дешеві або безкоштовні міжміські й міжнародні дзвінки. Для здійснення цих дзвінків вам потрібно скористатися послугами одного із провайдерів IP-телефонії й ви зможете дзвонити з комп'ютера, IP-телефону або звичайного телефону.

Однак, основна вигода VoIP для бізнесу – це можливість побудови більше ефективних систем корпоративних комунікацій з різними голосовими сервісами. Ефективність таких систем (у порівнянні із традиційними) полягає в наступному:

– більш просте й дешеве впровадження (так як VoIP системи будуються на базі існуючої інтранет-мережі);

– безкоштовний голосовий зв'язок усередині компанії (навіть при географічно розподіленій структурі бізнесу);

– можливість доступу до всіх комунікаційних можливостей будинку й у відрядженні (через інтернет);

– можливість інтеграції голосових сервісів у бізнес-застосунки й бізнес-процеси;

– просунуті можливості по записі розмов і веденню статистики.

Для реалізації систем корпоративних VoIP комунікацій служать IP-ATM і системи уніфікованих комунікацій на основі SaaS.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи VoIP для моделі SaaS

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи VoIP для моделі SaaS.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем VoIP для моделі SaaS.
– Дослідження системи VoIP для моделі SaaS.
– Програмна реалізація системи VoIP для моделі SaaS.

Об'єктом дослідження є процес VoIP для моделі SaaS.

Предметом дослідження є методи VoIP для моделі SaaS.

Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. IP-телефонія – це технологія, що зв'язує воєдино переваги телефонії й Інтернет. Донедавна мережі з комутацією каналів (телефонні мережі) і мережі з комутацією пакетів (IP-мережі) існували практично незалежно друг від друга й використовувалися для різних цілей. Телефонні мережі використовувалися тільки для передачі голосової інформації, а IP-мережі – для передачі даних. Технологія IP-телефонії поєднує ці мережі за допомогою пристрою, називаного шлюз або gateway. Шлюз являє собою пристрій, у який з однієї сторони включаються телефонні лінії, а з іншого боку – IP-мережа (наприклад, Інтернет).

Загалом передача голосу в IP-мережі відбувається в такий спосіб. Вхідний дзвінок і сигнальна інформація з телефонної мережі передаються на прикордонний мережний пристрій, називаний телефонним шлюзом, і обробляються спеціальною картою пристрою голосового обслуговування. Шлюз, використовуючи керуючі протоколи сімейства H.323, перенаправляє сигнальну інформацію іншому шлюзу, що перебуває на прийомній стороні IP-мережі. Прийомний шлюз забезпечує передачу сигнальної інформації на прийомне телефонне устаткування відповідно до плану номерів, гарантуючи наскрізне з'єднання. Після встановлення з'єднання голос на вхідному мережному пристрої оцифровується (якщо він не був цифровим), кодується у відповідності зі стандартними алгоритмами ITU, такими як G.711 або G.729, стискується, інкапсулюється в пакети й відправляється по призначенню на віддалений пристрій з використанням стека протоколів TCP/IP. Прихожі на прийомний шлюз IP-пакети перетворяться назад у телефонний сигнал і приймаючого абонента одержує виклик. Кінцеві споживачі послуги можуть навіть не догадуватися про те, як здійснюється цей дзвінок.

Оскільки при IP-телефонному дзвінку ніяк не задіяний міжнародний (міжміський) телефонний оператор, вартість цього дзвінка на порядок менше вартості традиційного телефонного з'єднання.

Однак дзвінок телефон-телефон є самим очевидним, але далеко не єдиним сервісом, що може надавати оператор IP-телефонії. Використовуючи IP-мережу, можна обмінюватися цифровою інформацією для пересилання голосових або факсимільних повідомлень між двома комп'ютерами в режимі реального часу. Застосування Internet дозволить реалізувати дану службу в глобальному масштабі. Для IP-телефонії найчастіше використовується стандарт H.323, що визначає передачу відео й аудіо по мережах з негарантованою якістю послуг, таким як Ethernet і IP. H.323 описує кілька елементів, у тому числі аудіо- і відеокодеки (кодери/декодери), комунікаційні протоколи й синхронізацію пакетів.

Види IP-телефонії

Голосовий зв'язок через IP-мережу може здійснюватися різними способами:

1. «Комп'ютер – комп'ютер». Даний варіант не являє приклад IP-телефонії, так як голос передається тільки по мережі передачі даних, без виходу в телефонну мережу. Для організації передачі трафіку користувач здобуває необхідне устаткування й програмне забезпечення, а також платить провайдеру за експлуатацію каналу зв'язку. Достоїнство цього варіанта полягає в максимальній економії засобів. Недолік – мінімальна якість зв'язку.

2. «Телефон – телефон». Для організації такого зв'язку необхідна наявність певних мережних пристроїв і механізмів взаємодії. Голосовий трафік передається через IP-мережу, як правило, на окремій дорогій ділянці. Пристроями, що організують взаємодія, є шлюзи, состиковані, з одного боку, з телефонною мережею загального користування, а з іншого боку – з IP-мережею. Голосовий зв'язок у такому режимі, у порівнянні з варіантом «комп'ютер – комп'ютер», коштує дорожче, однак якість її значно вище й користуватися нею зручніше. Для того щоб скористатися цією послугою, треба подзвонити провайдеру, що обслуговує шлюз, увести з телефонного апарата код і номер викликуваного абонента й розмовляти так само, як при звичайному телефонному зв'язку. Всі необхідні операції по маршрутизації виклику виконає шлюз.

3. «Комп'ютер – телефон». Тут відкривається більше можливостей використання для корпоративних користувачів, так як найчастіше застосовується корпоративна мережа, що обслуговує виклики від комп'ютерів до шлюзу, які вже потім передаються по телефонній мережі загального користування. Корпоративні рішення з використанням зв'язку « комп'ютер-телефон» можуть допомогти заощадити гроші, а необхідне для цього устаткування буде розглянуто нижче. Кінцевому користувачеві ніякого додаткового устаткування не потрібно. Досить мати під рукою телефон з можливістю тонального набору. Це потрібно для того, щоб, додзвонившись до оператора, увести свій код у тональному режимі, а далі дії абонента нічим не відрізняються від звичних. У більшості сучасних телефонних апаратів, включаючи таксофони й мобільні телефони, ця функція передбачена. Якщо такого телефону чомусь ні, то з функцією набору може впоратися біпер або, у крайньому випадку, спеціальна програма, яку можна скачати з Інтернету.

4. «Web – телефон». Ще одна нова послуга, що надають провайдери IP-телефонії – це дзвінок з Web-сайту або Surf&Call – рішення компанії VocalTec в області web-телефонії, що дозволяє здійснювати виклик, вибравши зі сторінки Інтернет посилання на ім'я викликуваного абонента. Це рішення спрямоване, насамперед, на розширення можливостей електронної комерції. Surf&Call дозволяє користувачам Інтернет прямо поговорити, наприклад, з торговельним представником або з фахівцем технічної підтримки його фірми, що цікавить. Установлення телефонного з'єднання відбувається при натисканні курсором на посилання, що представляє собою, наприклад, назва компанії, ім'я викликуваного абонента й т.д. на сторінці Інтернет. При цьому користувачеві не потрібно друга телефонна лінія або переривання роботи в Інтернет, необхідно лише завантажити невелике клієнтське програмне забезпечення, що звичайно можна знайти на тої ж Web-сторінці, і яке встановлюється автоматично. З іншої сторони Surf&Call дозволяє представникам компаній відповідати на питання, демонструвати Web-сторінки, передавати необхідну інформацію, поліпшуючи тим самим якість надаваних послуг.

Переваги IP-телефонії

Здешевлення телефонних переговорів. Впровадження технології VOIP у рамках обчислювальної мережі дозволяє зменшити сумарні витрати, пов'язані з веденням міжнародних і міжміських телефонних переговорів, а також почати процес міграції до технологій пакетної передачі мультимедійних даних. Крім того, з огляду на можливість виходу на міську телефонну мережу, використання цієї технології може звести до мінімуму оренду звичайних телефонних ліній.

Поліпшена якість зв'язку. Якість зв'язку можна оцінити, використовуючи наступні основні характеристики: рівень перекручування голосу; частота «провалля» голосових пакетів; час затримки (між проголошенням фрази першого абонента й моментом, коли вона буде почута другим абонентом). По всіх перерахованих характеристиках якість зв'язку

значно збільшилося в порівнянні з першими версіями рішень IP-телефонії, які допускали перекручування й переривання мови. Поліпшення кодування голосу й відновлення загублених пакетів дозволило досягти рівня, коли мова розуміється абонентами настільки добре, що співрозмовники не догадуються, що з'єднання відбувається за технологією IP-телефонії. Зрозуміло, що затримки впливають на темп бесіди. Відомо, що для людини затримка до 250 миллісекунд практично непомітна. Існуючі на сьогоднішній день рішення IP-телефонії не перевищують ця межа, так що розмова фактично не відрізняється від зв'язку по звичайній телефонній мережі. Крім цього, затримки зменшуються завдяки наступним трьом факторам:

– По-перше, удосконалюються телефонні сервери (їхні розроблювачі борються із затримками, поліпшуючи алгоритми роботи).

– По-друге, розвиваються частки (корпоративні) мережі (їхні власники можуть контролювати ширину смуги пропущення й, отже, величини затримки).

– По-третє, розвивається сама мережа Інтернет – сучасний Інтернет не був розрахований на комунікації в режимі реального часу. The Internet Engineering Task Force (IETF) разом з операторами мереж Інтернет пропонують нові технології, такі, як Reservation Protocol (RSVP), які дозволяють резервувати смугу пропущення.

Рішення проблеми зайнятої лінії. Уже давно аматори бороздити всесвітню мережу зіштовхуються із проблемою зайнятості телефонних ліній під час сеансу Dial-up. IP-телефонія дозволяє дуже елегантно вирішити цю проблему. Єдине, що повинен зробити абонент – це замовити на своєї АТМ переадресацію по сигналі «зайнято» на телефонний номер сервера IP-телефонії. При дзвінку на номер абонента під час Інтернет-сесії виклик переадресується на сервер IP-телефонії, що перетворює його в IP-пакети й відправляє на комп'ютер абонента. На комп'ютері абонента з'являється іконка «Вхідний дзвінок», кликнувши на яку він може поговорити із що дзвонить.

Підвищення якості факсимільного зв'язка. Так як, по суті факсимільне повідомлення – потік цифрових даних, а в технології VoIP дані передаються в цифровому виді, тому передача факсимільних повідомлень по аналогових лініях скорочується до мінімуму. А за рахунок того, що устаткування має можливість демодулювати сигнал перед передачею по IP-мережі й передавати закодоване в 64 Кбітному форматі факс-повідомлення в смузі 9,6 Кбіт, знижується навантаження на канали.

Інтеграція філій у єдину інформаційну структуру. Останнім часом з розвитком інформаційних технологій і збільшенням пропускної здатності каналів усе для найбільш оперативного рішення ділових завдань філії компанії поєднують в одне ціле, створюючи інтрамережу. Так як пропонована технологія використовує для передачі голосу саме мережі передачі даних, то з'являється можливість поєднувати не тільки комп'ютерні мережі, але й телефонні.

Віртуальні приватні мережі (VPN). IP-телефонія є ідеальною технологією для побудови віртуальних приватних мереж підприємства. Головна риса технології VPN – використання IP-мережі як магістраль для передачі корпоративного IP-трафіку. Мережі VPN вирішують завдання підключення корпоративного користувача до віддаленої мережі й з'єднання декількох віддалених ЛОМ і АТМ у єдину корпоративну мережу передачі голосу й даних.

Глобальний роумінг. IP-телефонія дозволяє операторам зв'язку дуже просто й з мінімальними витратами організувати роумінг послуг зв'язку. Це особливо актуально для операторів мобільного зв'язку – рішення, побудоване на технологіях IP-телефонії, на порядок дешевше традиційного, і має набагато більшу гнучкість.

Сполучений доступ в Інтернет. Голосові дані, факсимільні повідомлення передаються з використанням IP – основного набору протоколів Інтернет, дане рішення саме собою має на увазі доступ до ресурсів Мережі й очевидна економія на оренду ліній зв'язку й оплату послуг.

Мінімальні вкладення в устаткування. Якщо Ви використовуєте устаткування Cisco Systems, що відповідає всім сучасним стандартам, то Вам не буде потрібно прибігати до яким або витратам на додаткове устаткування, як телефонне так і комутаційне. Крім того, продукція Cisco має достатню гнучкість і масштабованістю, тобто нарощувати потужність, продуктивність і функціональні можливості можна поступово, відповідаючи потребам, що розвиваються.

Устаткування для IP-телефонії

Компанія Cisco Systems у цей час є лідером на ринку систем IP-телефонії, так як близько 92% трафіку VoIP передається по її устаткуванню. Недавно фірма оприлюднила власну стратегію розвитку пакетної телефонії, у рамках якої планується реалізація технологій VoIP, VoFR і навіть VoIP over ATM, що забезпечує якість голосу на рівні вимог, пропонованих до устаткування телекомунікаційних операторів (carrier-class quality). Компанія пропонує комплексний підхід до створення архітектурних систем з інтеграцією голосу, відео й даних Cisco AVVID (Architecture for Voice, Video and Integrated Data), що включають мережну інфраструктуру, клієнтські місця, серверні й користувальницькі додатки.

Рішення Cisco IP-телефонії складається з наступних компонентів: спеціалізовані цифрові IP-телефони (серії 7960/7940, 7910/7910+SW); керуючий сервер Cisco CallManager (на основі серверів MCS 7815-1000, MCS 7825-1133, MCS 7835-1266); голосові шлюзи для стикування IP-мереж з телефонною мережею загального користування (моделі Cisco 1750, 1760, VG200, 2600, 3600, 3700, Cisco 7200, AS5350, шлюзові модулі Catalyst 6000/6500, 4000), а також користувальницькі голосові додатки. Область застосування пропонованих VoIP-рішень охоплює користувальницьке прикінцеве устаткування (CPE), платформи доступу, що комутирується, виробу для ліній xDSL, кабельні інфраструктури й системи виділеного доступу, що забезпечують повну обробку трафіку.

Майбутнє IP-телефонії

У своєму розвитку IP-телефонія пройшла три етапи. На першому це була, скоріше, Internet-іграшка, придатна тільки для що квакає й сичить для зв'язку двох ентузіастів. Два комп'ютери, оснащені мікрофонами, динаміками, звуковими картами й не дуже складним програмним забезпеченням, дозволяли вести двосторонній діалог через Internet у реальному часі. Однак до зручностей звичайної телефонної послуги такий спосіб спілкування явно недотягав: абонентам потрібно було знати IP-адреса комп'ютера співрозмовника, домовлятися про час розмови, вибирати момент для більше якісної передачі мови, коли трафік Internet не зіштовхувався з більшими перевантаженнями й затримками. Крім того, при відсутності стандартів на обох комп'ютерах було потрібно встановити таке програмне забезпечення, щоб спосіб кодування голосу й упакування його в пакети був тим самим. Взаємодія між комп'ютером і телефоном, підключеним до звичайної телефонної мережі, не передбачалося. Зате витрати обмежувалися невеликою платою провайдеру Internet.

Другий етап ознаменувався появою стандартів IP-телефонії, насамперед – стандартів групи H.323. Розроблювачі цих протоколів виходили з того, що дві мережі – телефонна й IP – будуть співіснувати пліч-о-пліч досить тривалий час, а виходить, важливо регламентувати їхня взаємодія з обліком існуючих у традиційних телефонних мережах процедур установлення з'єднання, а також домовитися про спосіб передачі виклику й самого голосу по мережі IP. У стандартах H.323 визначається дві групи протоколів – протоколи транспортної площини (transport plane), називаною також користувальницькою площиною (user plane), і протоколи площини керування викликами (call control plane). На цьому етапі розвитку IP-телефонії мережа IP (Internet або приватна) широко використовувалася в якості транзитної між двома місцевими телефонними мережами. Дана схема реалізації загальнодоступних послуг IP-телефонії стала досить популярна в усьому світі. Для її реалізації операторові зв'язку не треба створювати власну дорогу транспортну інфраструктуру й мати безпосередній доступ до абонентів. Однак стратегічні перспективи такого підходу –

залишають бажати кращого через невисокий ступінь масштабованості й вузького спектра послуг.

Масштабованість обмежується декількома факторами. По-перше, провайдеру доводиться встановлювати численні однорангові зв'язки зі своїми друзями-суперниками по бізнесі. По-друге, протоколи обох площин необхідно реалізовувати у всіх елементах мережі IP-телефонії: і у воротарях, і в шлюзах, і в терміналах, що приведе до зайвої складності й дорожнечі всіх цих пристроїв. І, нарешті, користувачам надаються тільки базові послуги з обробки викликів, оскільки взаємодія із протоколами міжстанційної сигналізації SS7 і з послугами інтелектуальної мережі IN відсутній.

Крім того, діалог із сервером інтерактивної голосової відповіді при автентифікації абонента й завданні номера викликуваного абонента досить стомлюючий – набагато зручніше просто набрати цей номер з невеликою приставкою начебто 8-20 і одержати доступ до послуг міжнародної IP-телефонії. Але для цього провайдеру потрібний прямий доступ до абонента або домовленість із місцевими операторами про переадресацію таких викликів на шлюз IPTP за допомогою засобів інтелектуальної мережі (а вони поки підтримуються далеко не всіма місцевими операторами).

Таким чином, для виходу IP-телефонії на більше високий рівень національного або міжнародного оператора потрібні інші стандарти й устаткування, щоб мережі, побудовані на базі протоколу IP, могли рівноправно сусідити із традиційними телефонними мережами.

Багато хто з необхідних стандартів уже з'явилися й втілені в новому поколінні устаткування, що служить основою для третього етапу розвитку IP-телефонії. Така мережа може підтримувати власних абонентів і служити транзитною мережею для традиційних телефонних мереж з наданням повного спектра послуг, включаючи послуги інтелектуальної мережі IN. У вузлах IP-телефонії нового покоління відбувся чіткий поділ функцій на три групи – транспортну, керування викликами й прикладними сервісами. На цьому етапі підтримується весь спектр додаткових послуг, які можуть надавати для абонентів розвинені телефонні комутатори міського типу, у тому числі й за допомогою інтелектуальної мережі: переадресацію викликів відповідно до різних умов, телеголосування, безкоштовний дзвінок, дзвінок по спеціальному тарифі, скорочений набір і т.п.

Дуже важливо, що взаємодія між рівнями здійснюється через стандартні інтерфейси, а це створює серйозні передумови для побудови телефонних вузлів IP-телефонії на основі продуктів різних виробників із застосуванням загальноприйнятих способів обробки викликів.

Очевидно, що в IP-телефонії є майбутнє, але в якій послідовності й коли буде здійснюватися широкомасштабний перехід до неї поки невідомо, та й загальна криза телекомунікаційної галузі цьому явно не сприяє. Проте будемо сподіватися, що потенціал IP-телефонії, що набрав за багатьма ознаками достатню критичну масу, буде незабаром реалізований, і рядові користувачі й численні провайдери зможуть скористатися всіма її перевагами.

Розробка структурної схеми

Провідна телефонія за своє більш ніж віковий розвиток у силу технічних і економічних перешкод не змогла стати загальним надбанням людства. У розвинених країнах телефонні апарати були встановлені у всіх держустановах, комерційних фірмах, практично в кожній міській квартирі й сільському будинку, а от у нас стаціонарний телефонний зв'язок навіть наприкінці XX сторіччя залишалася для багатьох недосяжної не тільки у віддалених і малонаселених районах, але й у великих селищах. Але ж людям для оперативного рішення безлічі особистих і бізнес-питань необхідно мати можливість голосового спілкування «тут і зараз».

Мобільна телефонія, що почала свою експансію біля сорока років тому, значно підвищила доступність голосового зв'язку, особливо на неохоплених стаціонарним зв'язком територіях, і за короткий час стала технологією масового застосування.

Провідна й бездротова технології освоїлися у своїх нішах і благополучно співіснували, не турбуємі конкурентами, ще яких-небудь десять років тому, коли раптом з'явився третій «суперник» – VoIP-технологія. І суперник цей виявився небезпечний, насамперед, тим, що надав можливість істотно меншої оплати за ті ж мінути голосового зв'язку, які могли б бути витрачені в мережах його попередників. Причому він може легко «впроваджуватися» і в стаціонарні, і в мобільні зони, здійснюючи зв'язок з абонентами й першої, і другої технології мовного спілкування. Не говорячи вже про «власний контингент на власної VoIP-території».

Технологія VoIP для моделі SaaS: чому дешевше?

Для надання послуг стаціонарної телефонії необхідно було створити інфраструктуру у вигляді кабельних ліній зв'язку величезної довжини. Для мобільної – побудувати базові станції передачі радіосигналу. А фізичним середовищем для технології VoIP для моделі SaaS став Інтернет, тобто провайдерам нового телекомунікаційного напрямку не довелося створювати свою інфраструктуру: є Інтернет – є можливість пропозиції сервісів VoIP для моделі SaaS, що й відбито в «ім'ї» технології – Voice over Internet Protocol – «голос по інтернет-протоколу».

Витрати на будівництво базових станцій вертаються операторові в оплаті за розмови по мобільних телефонах. Провайдери VoIP-технології, що впровадилися в «готову» мережу Інтернет, таких витрат на VoIP для моделі SaaS устаткування не несли, і, відповідно, у тарифах за послуги зв'язку вони не присутні.

Правда, назва VoIP для моделі SaaS не повною мірою характеризує технологію, що дозволяє здійснювати приймально-передачу не тільки мови (цьому сегменту привласнена ім'я «IP телефонія»), але й відеоконтенту й, взагалі, будь-яких даних, представлених у цифровому виді. Однак оскільки сьогодні найбільш затребувана саме IP-телефонія, то на її прикладі ми й розглянемо всі основні техніко-економічні показники VoIP для моделі SaaS, попутно відзначивши, що ця технологія крім роботи в Інтернеті може бути реалізована в будь-яких виділених цифрових каналах, що підтримують інтернет-протокол і складових IP-мережа.

Отже, перший доданок економічності IP-телефонії (вірніше було б, напевно, сказати – «від'ємник») – це відсутність інвестицій у створення інфраструктури, які в операторів стаціонарного й мобільного зв'язку повинні окупитися, для чого вони «незримо присутні» у їхніх тарифах.

Друга обставина, що дозволила провайдерам IP-телефонії встановити мінімальну планку оплати їхніх послуг, полягає в тім, що в телефонних мережах загального користування (ТМЗК, ТфЗК), оплата розмови визначається його тривалістю й довжиною виділеного каналу. А в IP-телефонії оплачується лише підключення до Інтернету й обсяг переданого трафіку.

Третя стаття витрат провайдерів стаціонарного зв'язку, що закладається в тарифи, як це ні парадоксально звучить, – оплата пауз у розмовах. Справа в тому, що в традиційних мережах з комутацією каналів оплата вважається за час «оренди» каналу. І те, що паузи в розмові, по суті, – марна витрата часу, біллінгова система не враховує, а просто вважає мінути «оренди» каналу й множить їх на тариф. А в IP-телефонії є механізм блокування передачі пауз (діалоговим, складовим, значеннєвим, затрачуваним абонентом на пошук потрібних слів, відволікань від розмови й т.п.), які можуть становити до 40-50 % часу заняття каналу передачі.

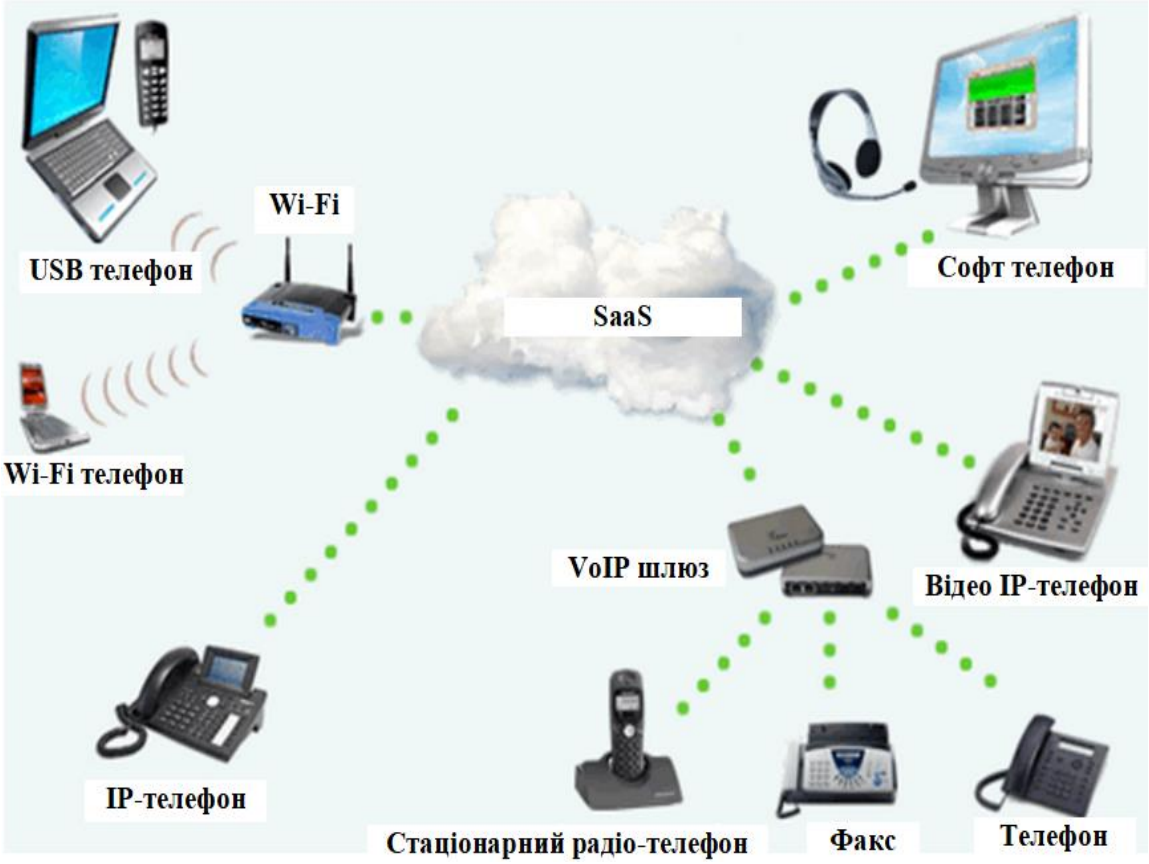


Рисунок 1 – Структурна схема системи

VoIP для моделі SaaS телефонія забезпечує приймально-передачу мови між комп'ютерами (з підключеними мікрофонами й навушниками або динаміками), комп'ютером і стаціонарним (аналоговим і цифровим) телефоном, мобільним і IP-телефонами, а також між будь-якими з перерахованих видів телефонів у довільних комбінаціях. Відзначимо, що звичний нам аналоговий телефонний апарат можна перетворити в IP-телефон, включивши між його входом і інтернет-розеткою аналоговий телефонний адаптер (VoIP ATA).

Кожний IP-телефон (із провідним і бездротовим входом/виходом або убудованим аналоговим модемом) підключається до Мережі інтернет-провайдером, потім проходить реєстрацію в оператора послуг IP-телефонії, одержуючи при цьому логін і пароль.

Але для використання цієї технології наявність спеціального апарата необов'язково, якщо встановити на комп'ютері програму-клієнт, що імітує телефон, і підключити до ПК навушники й мікрофон або USB-телефон, що виконує функції навушників і мікрофона. Такий комп'ютерно-програмний комплекс називається софтфоном (програмним телефоном). ПЗ SoftPhone можна безкоштовно скачати на web-сайті провайдеру IP-телефонії, після чого там же зареєструвати свій пристрій. Самою популярною безкоштовною програмою для VoIP для моделі SaaS телефонії у світі є Skype.

Різновидом програмних телефонів є двhрежимні GSM/WiFi (стільниковий/VoIP) мобільні телефони, використовувані у двох «іпостасях»: в GSM-мережі вони поводяться як стільниковий телефон, а в WiFi-зоні (при встановленому в телефоні ПЗ SoftPhone) – в IP-мережі. Причому в другому режимі роумінг у мобільній мережі практично безкоштовний.

Відеотелефон – устаткування, що працює по VoIP для моделі SaaS технології, забезпечує ефект присутності в офісі абонента, що перебуває «на іншому кінці проведення», завдяки чому підвищується результативність бізнес-переговорів.

Для організації голосового зв'язку, здійснюваної між комп'ютерами, IP-телефонами й відеотелефонами, досить з'єднати їхнім кабелем з інтернет-розеткою й увійти в Інтернет. А для зв'язку IP-мережі із ТМЗК необхідне застосування аналогових VoIP для моделі SaaS

шлюзів FXS або FXO. У випадку ж цифрових телефонних мереж ISDN (Integrated Services Digital Network) їхній зв'язок із Всесвітньою павутиною забезпечується цифровими VoIP-шлюзами.

VoIP-шлюзи дозволяють підключитися до мереж декількох операторів для створення декількох маршрутів трафіку з мінімальними тарифами, зарезервувати їх для використання при виникненні перевантажень і відмов у мережах стаціонарного й мобільного зв'язку. При цьому, завдяки наявності альтернативних маршрутів, компанії можуть досягти помітного зменшення витрат на послуги зв'язку, збільшивши до того ж доступність абонентів, що перебувають у мережах, які підтримують різні технології передачі голосу.

В VoIP-шлюзах можуть бути створені віртуальні об'єкти, що визначають маршрутизацію телефонних дзвінків, що дозволяє компанії «безмежно» підключати прямі номери в будь-якій державі планети (ця технологія називається Direct Inward Dialing, DID).

VoIP-шлюзи – міжмережеве устаткування VoIP для моделі SaaS для переведенняу голосового трафіку між мережами традиційної телефонії й мережею передачі даних.

Ще одне достоїнство IP-телефонії: можливість простого нарощування в офісі кількості номерів (так званої «номерної ємності»), що, як правило, на превелику силу вдається зробити в ТфЗК (і те, якщо в оператора стаціонарного зв'язку є технічна можливість).

Як ми вже відзначали на початку розділу, привабливість IP-телефонії для масового користувача полягає в економії оплати за голосовий зв'язок у порівнянні з оплатою за такі ж переговори в стаціонарних і мобільних мережах. Цей показник, звичайно, важливий і бізнес-сегменту, для якого, виявляється, є ще один «бонус» – низькі витрати на створення корпоративної мережі IP-телефонії (апаратна IP ATM, програмні ATM, віртуальні ATM) на основі існуючої УАТМ.

Підводні камені технології VoIP для моделі SaaS

Ви вже наслишані про переваги й вигоди IP-телефонії й навіть неодноразово бачили устаткування й програми для VoIP для моделі SaaS у роботі в когось зі своїх друзів. Сподобалося. І от ви вирішуєте впровадити її в себе. Але чи розповіли вам про парочку «підводних каменів», які можуть звести «на ні» всі ваші очікування? А вони є.

Відома приказка, що затверджує, що «недоліки є продовження наших достоїнств», може бути віднесена до усім без винятку технологіям. І, звичайно ж, до IP-телефонії. У цій технології «кульгають» якість передачі голосу й безпека. Але ці ущербності можна усунути, якщо розібратися в їхніх корінняx.

Отже, у ТфЗК якість мови не викликало дорікань тому, що в цій технології, заснованої на комутації каналів зв'язку, «пісня ллється» безупинно в одній і тої ж «трубі». А VoIP-технологія передає ту ж «пісню» вроздріб (у вільні тепер каналах) відповідно до інтернет-протоколу, здійснюючи комутацію пакетів даних (як це прийнято в передачі будь-якої інформації з Інтернету). І якщо, наприклад, у передачі текстів і фотознімків, ця пакетна послідовність може закінчитися «коли вийде», і ми спокійно почекаємо її закінчення й відкриємо «готовий добуток», те голосовий зв'язок працює в режимі реального часу й не чекає, коли прийде наступний пакет.

Тому якщо час затримки в одержанні пакетів і їхня пропажа перевищують установлені стандартом величини, це неминуче позначається на розбірливості, чистоті, рівні гучності, появі луни, хрипів і інших некомфорних для слухового сприйняття звуків. Але, як говориться в популярному мультфільмі, «неприємність цю ми переживемо». Природно, за допомогою системного інтегратора, що зможе зробити всі роботи для інтелектуальної обробки затримок одержання пакетів, інтерполяції (часткового відновлення) інформації, що перебувала в загублених пакетах, лунапридушення й керування рівнем голосового сигналу. І буде всі так само добре, як вам дозволив побачити на своїй фірмі ваш друг.

З безпекою – складніше, адже в програму вашого візиту на фірму друга «за замовчуванням» не входила презентація на цю тему. Напевно, вам розповідали, що розмови по IP-телефоні простіше прослуховувати, чим при використанні звичайного стаціонарного

апарата. І ці слухи небезпідставні, оскільки для втручання в розмову, що відбувається по ТфЗК, необхідно фізичне підключення до лінії, по якій ви ведете бесіду. А це досить важко (хоча й можливо).

Якщо ж ви користуєтеся послугами IP-мережі, то досвідчений хакер без особливої праці може «обчислити» вашу IP-адресу й непомітно (програмним шляхом) влізти у ваші розмови, не тільки підслухуючи їх, але й блокуючи й навіть коректуючи. І тут, щоб не вдаватися в зайві для читача подробиці, можна сказати, що фахівці з інсталяції VoIP-технології, здатні створити IP-мережа, рівень захисту якої буде вище, ніж у традиційної провідної телефонної мережі.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів VoIP для моделі SaaS. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем VoIP для моделі SaaS. Досліджена система VoIP для моделі SaaS. На основі отриманих результатів досліджень створена програмна реалізація системи VoIP для моделі SaaS. Розроблені алгоритми дозволяють успішно вирішувати завдання VoIP для моделі SaaS. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
3. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
4. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
5. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
6. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19
7. Дреев А.Н. Повышение оперативности доставки данных повышенной востребованности в телекоммуникационных системах и сетях / А.Н. Дреев, А.А. Смирнов, Е.В. Мелешко // Проблеми і перспективи розвитку ІТ-індустрії 25-26 квітня 2013 р. Системи обробки інформації. – Випуск 3 (110). Том 2. – Харків: ХУПС. – 2013. С. – 199.
8. Дрєєв О.М. Середньостатистичний та найімовірніший час доставки багатопакетного повідомлення в телекомунікаційній системі або мережі / О.М. Дрєєв, О.А. Смірнов // V Всеукраїнська науково-практична конференція "Інформатика та системні науки" ІСН – 2014, 13-15 березня 2014 року, м. Полтава – С. 92
9. Дреев А.Н. Экстраполяция квазипериодических процессов с аддитивными помехами / А.Н. Дреев, А.А. Смирнов // П’ята Міжнародна науково-практична конференція "Інформаційні технології та моделювання в економіці" 15-16 травня 2014 р. – Черкаси – С. 59
10. Дреев А.Н. Статистическая модель передачи многопакетного сообщения в телекоммуникационной системе или сети / А.Н. Дреев, А.А. Смирнов // «Компьютерное моделирование в наукоемких технологиях (КМНТ-2014)» Харьков, 28-31 мая 2014 года – С. 137-140

УДК 004

К. Шкуренко, магістр гр. КІ-20МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОТИДІЇ ШАХРАЙСЬКИМ ДІЯМ У МЕРЕЖІ ІНТЕРНЕТ

У статті розроблено програмне забезпечення, яке призначено для системи протидії шахрайським діям у мережі Інтернет. Метою розробки є дослідження та програмна реалізація системи протидії шахрайським діям у мережі Інтернет.Об'єктом дослідження є процес протидії шахрайським діям у мережі Інтернет. Предметом дослідження є методи протидії шахрайським діям у мережі Інтернет. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи протидії шахрайським діям у мережі Інтернет. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, шахрайські дії, Інтернет

Постановка проблеми. Фішинг-атаки – злочин 21-го століття. Засоби масової інформації щодня публікують списки організацій, чиї клієнти піддалися фішинговим атакам. Як тільки фішери розробляють нові прийоми атак, бізнес реагує на це розробкою нових засобів оборони, захисту персональних даних своїх клієнтів, залучає зовнішніх експертів по посиленню захисту електронної пошти. У свою чергу клієнти так само намагаються захиститися від потоку «офіційних» листів і створюють більш строгі правила спілкування [1-5].

Схований серед куп електронної макулатури, та роблячий обхід багатьох із кращих сьогоднішніх антиспамових фільтрів, новий вектор напад призначений для крадіжки конфіденційної особистої інформації. Професійні злочинці тепер використовують спеціально сформовані повідомлення, щоб заманити жертви в пастки, розроблені для крадіжки електронної тотожності користувачів [4-7].

Назва даного типу атак – Phishing (фішинг); процес обману або соціальна розробка клієнтів організацій для наступного крадіжки їхніх ідентифікаційних даних і передачі їхньої конфіденційної інформації для злочинного використання. Злочинці для свого напад використовують spam або комп'ютери-боти. При цьому розмір компанії-жертви не має значення; якість особистої інформації отриманої злочинцями в результаті напад, має значення саме по собі [8-9].

У той час як багато організацій вводять більше строгі правила у фільтрації спама, вони так само повинні приймати проактивні міри в боротьбі з фішингом. Розуміючи інструменти й методи, використовувані криміналітетом, і аналізуючи можливі діри у безпеці периметра, організації зможуть заздалегідь захиститися від багатьох популярних і успішних напрямків подібних атак.

Дана стаття присвячена дослідженню деяких видів фішингу, що дозволить більш успішно захищатися від них, та розробці антифішингового програмного забезпечення.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи протидії шахрайським діям у мережі Інтернет

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи протидії шахрайським діям у мережі Інтернет.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем протидії шахрайським діям у мережі Інтернет.
– Дослідження системи протидії шахрайським діям у мережі Інтернет.
– Програмна реалізація системи протидії шахрайським діям у мережі Інтернет.

Об'єктом дослідження є процес протидії шахрайським діям у мережі Інтернет.

Предметом дослідження є методи протидії шахрайським діям у мережі Інтернет.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Напрямки фішингових атак

Фішери повинні використовувати масу методів шахрайства для того щоб здійснити успішні напади. Самі загальні включають:

– напад " людин у середині " (in-the-middle Attacks);
– напад підміни URL;
– напад, що використовують Cross-site Scripting;
– попередньо встановлені сесії атак;
– підміна клієнтських даних;
– використання уразливості на стороні клієнта.

Напад "людин у середині" (in-the-middle)

Одним із самих успішних способів одержання керування інформацією клієнта й ресурсами є напад "людин у середині". У цьому класі атак нападаючий розташовує себе між клієнтом і реальним додатком, доступним через мережу. Із цієї точки, той хто нападає може спостерігати й робити запис всіх подій.

Ця форма нападу успішна для протоколів HTTP і HTTPS. Клієнт з'єднується із сервером нападаючих, начебто з реальним сайтом, у той час як сервер нападаючих робить одночасне підключення до реального сайту. Сервер нападаючих у такому випадку відіграє роль проксі-сервера для всіх з'єднань між клієнтом і доступним через мережу прикладним сервером у реальному масштабі часу.

У випадку безпечного з'єднання HTTPS, підключення SSL установлюється між клієнтом і проксі-сервером нападаючих (отже, система нападаючих може робити запис усього трафика в незашифрованому стані), у той час як проксі-сервер нападаючих створює своє власне підключення SSL між собою й реальним сервером.

Для проведення успішних атак "людина в середині ", той хто нападає повинен бути приєднаний прямо до клієнта замість реального сервера. Це може бути виконане за допомогою безлічі методів:

– DNS Cache Poisoning
– URL Obfuscation
– Browser Proxy Configuration

Прозорі проксі-сервери

Розташований у тім же сегменті мережі або розташований на маршруті на реальний сервер (наприклад, корпоративний гейтвей), transparent proxy service може перервати всі дані, пропускаючи весь вихідний HTTP і HTTPS через себе. У цьому випадку ніякі зміни конфігурації на стороні клієнта не потрібні.

DNS Cache Poisoning (отруєння кеша DNS)

DNS Cache Poisoning може використовуватися, щоб перервати нормальну маршрутизацію трафика, вводячи помилкові адреси IP для ключових імен домену. Наприклад, той хто нападає модифікує кеш доменної системи імен мережного міжмережного захисту так щоб весь трафик, призначений для адреси IP MyBank тепер ішов на адресу IP проксі-сервера того, хто нападає.

URL Obfuscation

Використовуючи даний метод, зловмисник змінює зв'язок замість реального сервера на з'єднання з їх проксі-сервером. Наприклад, клієнт може переходити на посилання до <http://www.mybank.com.ch/> замість <http://www.mybank.com/>

Конфігурація проксі-сервера в браузері клієнта

Даний тип атаки може бути легко замічений клієнтом при огляді настроювань браузера. У багатьох випадках зміна настроювань браузера буде здійснено безпосередньо перед фішинг-повідомленням.

Напад підміни адрес

Таємниця багатьох фішингових нападів полягає в тому, щоб змусити одержувача повідомлення випливати за линком (URL) на сервер зловмисник, не розуміючи, що він був обманутий. На жаль фішери мають доступ до все більшого арсеналу методів щоб заплутати кінцевого клієнта.

Самі звичайні методи підміни адрес включають:

– Bad domain names.
– Friendly login URL's.
– Host name obfuscation.
– URL obfuscation.

Погані імена домену

Один з найбільш тривіальних методів підміни використання поганих імен домену. Розглянемо фінансовий інститут MyBank із зареєстрованим доменом *mybank.com* і пов'язаний із клієнтом діловий сайт <*http://privatebanking.mybank.com*>. Фішер міг установити сервер, використовуючи кожне з наступних імен, щоб заплутати реальний хост адресата:

http://privatebanking.mybank.com.:

– http://mybank.privatebanking.com/
– http://privatebanking.mybonk.com/
– http://privatebanking.mybank.com/
– http://privatebanking.mybank.hackproof.com/

Важливо звернути увагу на те, що, оскільки організації реєстрації доменов рухаються в напрямку інтернаціоналізації їхніх послуг, отже, можлива реєстрація імен доменів на інших мовах і певних наборах символів. Наприклад, “о” у символах кирилиці виглядає ідентично стандартному ASCII “o”, але доменне ім'я буде іншим.

Нарешті, це варто відзначати, що навіть стандартний набір символів ASCII ураховує двозначності типу верхнього регістра “i” і нижнього регістра “L”.

Friendly Login URL's

Багато web-браузерів ураховують складний URL, що може включити розпізнавальну інформацію типу ім'я вхідного в систему й пароля. Загальний формат – URL://username:password@hostname/path.

Фішери можуть замінити ім'я користувача й поле пароля. Наприклад наступний URL установлює *ім'я користувача = mybank.com*, *пароль = ebanking*, і ім'я хоста адресата – *evilsite.com.*

<http: // mybank.com:ebanking@evilsite.com/фішинг/fakepage.htm>

Цей дружній вхід у систему URL може успішно обдурити багатьох клієнтів, які будуть уважати, що вони фактично відвідують законну MyBank сторінку. Через успіх даного методу, багато поточних версій браузерів забрали підтримку даного методу кодування URL.

Підміна імен хостів

Більшість користувачів Internet знайомо з навігацією по сайтах і послугам, використовуючи повне ім'я домену, типу www.evilsite.com <http://www.evilsite.com>. Для того щоб web-браузер міг зв'язатися з даним хостом по Internet, ця адреса повинен бути перетворений на адресу IP, типу 209.134.161.35 для www.evilsite.com <http://www.evilsite.com>. Це перетворення IP-адреси в ім'ї хоста досягається за допомогою серверів доменних імен. Фішер може використовувати адресу IP як частина URL, щоб

заплутати хост і можливо обійти системи фільтрації змісту, або сховати адресат від кінцевого користувача.

Наприклад наступний URL:

<http: // mybank.com:ebanking@evilsite.com/фішинг/fakepage.htm>

міг бути заплутаним по наступному сценарію:

<http: // mybank.com:ebanking@210.134.161.35/login.htm>

У той час як деякі клієнти знайомі із класичним десятковим поданням адрес IP (000.000.000.000), більшість із них не знайомо з іншими можливими поданнями. Використовуючи ці подання IP у межах URL, можна привести користувача на фішерский сайт.

Залежно від додатка, що інтерпретує адресу IP, можливе застосування різноманітних способів кодування адрес крім класичного пунктирно-десяткового формату. Альтернативні формати включають:

– Dword – значення подвійного слова, тому що це складається по суті із двох подвійних "слів" 16 біт; але виражено в десятковому форматі,

– Восьмеричний

– Шестнадцатеричний.

Ці альтернативні формати найкраще пояснюються, використовуючи приклад. Розглянемо URL <http://www.evilsite.com/>, перетворюючи до IP-адреси 210.134.161.35. Це може інтерпретуватися як:

– Десяткове число – *<http: // 210.134.161.35/>*

– Dword – *http:// 3532038435/*

– Восьмеричний – *<http: // 0322.0206.0241.0043/>*

– Шестнадцатеричний – *<http://0x2.0x86.0x1.0x23/>* або навіть *<http:/0x286A123/>*

– У деяких випадках, можливо навіть змішати формати (наприклад *<http:// 0322.0x86.161.0043/>*).

Підміна URL

Щоб гарантувати підтримку місцевих мов у програмному забезпеченні Internet типу web-браузерів, більшість програмних забезпечень підтримує додаткові системи кодування даних.

Cross-site Scripting Attacks

Типові формати CSS ін'єкції в достовірний URL включають:

Повна заміна HTML типу:

<http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm>

Вбудоване впровадження сценарію, типу:

*http: // mybank.com/ebanking? Page=1*client = <СЦЕНАРІЙ> evilcode <http: // mybank.com/ebanking? Page=1*client = % 3cSCRIPT%3eevilcode>...*

Наприклад, клієнт одержав наступний URL за допомогою електронного фішинг-листа:

<http: // mybank.com/ebanking? URL=http: // evilsite.com/phishing/fakepage.htm>

У той час як клієнт дійсно спрямований і пов'язаний з реальним MyBank додатком мережі, через помилкове кодування додатка банком, *ebanking* компонент прийме довільний URL для вставки в межах поля *URL* повернутої сторінки. Замість додатка, що забезпечує розпізнавальну форму MyBank, впроваджену в межах сторінки, зловмисник пересилає клієнта до сторінки під керуванням на зовнішньому сервері *(<http: // evilsite.com/phishing/fakepage.htm>)*.

Методи протидії фішинговим атакам

Як може звичайний користувач протистояти атаці фішерів? Насправді, варто задуматися над декількома правилами:

1. Ніколи не відповідайте на листи, що запитують вашу конфіденційну інформацію
2. Відвідаєте веб-сайт банку шляхом введення його URL-адреси через адресний рядок браузера

3. Регулярно перевіряйте стан своїх онлайн-рахунків
4. Перевірте рівень захисту відвідуваного вами сайту
5. Виявіть обережність, працюючи з електронними листами й конфіденційними даними
6. Забезпечте захист своєму комп'ютеру
7. Завжди повідомляйте про виявлену підозрілу активність

Розглянемо даного правила докладніше.

Ніколи не відповідайте на листи, що запитують вашу конфіденційну інформацію

Як правило, банки й фінансові компанії, що займаються електронною комерцією, розсилають персоніфіковані звернення клієнтам, а фішери – ні! Фішери часто використовують кричаще звучні заголовки листів типу «Терміново! Ваші реквізити можуть бути викрадені!» для того, щоб змусити користувача негайно перейти по посиланню.

Варто пам'ятати, що поважаючі себе компанії ніколи не запитують у клієнтів паролі або дані рахунків за допомогою електронної пошти. Навіть, якщо вам здалося, що лист легітимний – не варто відповідати на нього, краще приїхати в офіс компанії або, у крайньому випадку, передзвонити їм по телефоні.

Варто пам'ятати про обережність при відкриванні вкладень в електронні листи або при завантаженні через Інтернет по посиланнях, незалежно від того, хто є відправником цих листів!

Відвідування веб-сайту банку або компанії

Для відвідування веб-сайту банку наберіть в адресному рядку браузера його URL-адресу.

Фішери часто використовують так звані «схожі» адреси. Однак якщо піти по такому «схожому» посиланню, ви можете потрапити на фішерский сайт замість справжнього сайту банку.

Це не дасть вам повну гарантію безпеки, однак зможе вберегти хоча б від деяких видів атак фішеров.

Регулярно перевіряйте стан своїх рахунків

У випадку виявлення підозрілої транзакції негайно зв'яжіться з вашим банком. Одним з найпростіших засобів перевірки стану рахунку є так званий SMS-банкинг.

Не менш розповсюджений спосіб на сьогоднішній день пов'язаний з лімітуванням операцій. У такому випадку клієнтові досить установити суму гранично можливого зняття готівки або платежу в торговельній точці, і банк не дозволить ні йому, ні шахраєві вийти за встановлені рамки.

Перевірте рівень захисту відвідуваного вами сайту

Перед введенням конфіденційної інформації на сторінці сайту вашого банку, не заважає провести пару перевірок, щоб переконатися у використанні банком криптографічних методів.

По-перше, перевірте веб-адресу в адресному рядку браузера. Якщо веб-сайт, що ви вирішили відвідати, розташований на захищеному сервері, то адреса повина починатися з "https://" ("s" від security), а не зі звичайного "http://".

По-друге, перевірте також стан іконки із зображенням замка в статусному рядку вашого браузера. Ви можете перевірити рівень криптозахисту, обумовлений кількістю біт, поводивши курсор мишки над цією іконкою.

Виявіть обережність, працюючи з електронними листами й конфіденційними даними

Більшість банків мають на своїх веб-сайтах сторінку з питань безпеки, де повідомляється інформація про те, як проводити транзакції в захищеному режимі, а також загальні ради по захисту конфіденційних даних: ніколи й нікому не відкривайте свої PIN-Коди або паролі, не записуйте їх і не використовуйте той самий пароль для всіх своїх онлайн-рахунків.

Не відкривайте спамові листи й не відповідайте на них, тому що цими діями ви даєте відправникові листа коштовну інформацію про те, що він роздобув діючу електронну адресу.

Користуйтеся здоровим глуздом, коли читаєте електронні листи. Якщо щось у листі вам здається неправдоподібним або настільки гарним, що не віриться, то, швидше за все, так воно і є.

Захистить свій комп'ютер

Варто пам'ятати, що найбільш ефективним захистом від троянських програм служить антивірусне ПЗ. Останнім часом деякі антивірусні компанії стали вбудовувати у свої продукти так звані антифішингові фільтри. Зокрема, антифішинговий фільтр вбудований у ПЗ від Лабораторії Касперского, Symantec і т.д. Крім того, у сучасних версіях браузерів з'явилися свої варіанти антифішингових фільтрів.

З великою часткою ймовірності можно затверджувати, що лист фішинговий, якщо:

– тема й тіло листа бідно відформатовані й містять багато помилок;

– лист починається з безликого вітання типу «Дорогий клієнт»;

– манера викладу листа така, начебто вас хочуть урятувати від якоїсь неприємності і єдиний спосіб не втратити свої гроші – повідомити конфіденційну інформацію про стан ваших рахунків.

А от рекомендації при використанні банківської картки в мережі Інтернет, розроблені українськими фахівцями:

– не відповідайте на електронні листи, у яких нібито від імені банку вас просять надати персональну інформацію. Зв'яжіться з банком по номеру телефону, що відомий вам як дійсний, щоб з'ясувати дійсність листа;

– ніколи не переходьте по посиланнях у таких листах (навіть на сайт банку), тому що вони можуть вести на шахрайські сайти;

– ніколи не розкривайте персональну інформацію або інформацію з карти (рахунку) через Інтернет;

– користуйтеся послугами тільки відомих і перевірених торговельних підприємств. Перевагу необхідно віддавати підприємствам, підключеним до програм Verified by Visa (Перевірено Візою) і Secure Code (Безпечний Код);

– перевіряйте адреси інтернет-сайтів, до яких ви підключаєтеся, тому що зловмисники можуть використовувати схожі назви для створення шахрайських ресурсів;

– уникайте користуватися послугами інтернет-ресурсів сумнівного змісту: найчастіше вони створюються спеціально для одержання інформації про банківські карти й наступного її неправомірного використання;

– контролюйте свою електронну пошту, не відкривайте повідомлення від невідомих адресатів, не передавайте свої особисті дані;

– поставте на свій комп'ютер антивірусне програмне забезпечення й регулярно робите його відновлення й відновлення інших використовуваних вами програмних продуктів;

– робіть покупки тільки зі свого комп'ютера. Не користуйтеся інтернет-кафе й іншими доступними засобами, де можуть бути встановлені програми-шпигуни, що запам'ятовують конфіденційні дані, що вводяться вами;

– вибирайте паролі, які не пов'язані з вашим днем народження або іншими персональними даними. Не записуйте паролі й нікому не повідомляйте їх.

Засоби антифішингу в Windows

Система Windows покликана стати самою безпечною з коли-або випущених версій Windows. Вона постачена новими функціями для забезпечення безпечної роботи користувачів в Інтернеті.

Захистіть свій комп'ютер

Підвищте рівень захисту від програм-шпигунів. Захисник Windows — це антишпигунська програма для системи Windows. Вона дозволяє уникнути з роботи комп'ютера, втрати конфіденційних даних і появи небажаних спливаючих рекламних вікон, викликаних програмами-шпигунами й іншими потенційно небажаними програмами.

Переглядайте веб-сторінки з більшою впевненістю в захищеному режимі оглядача Internet Explorer. Ця функція, що є тільки в системі Windows, обмежує повноваження користувача при роботі з оглядачем Internet Explorer, надаючи йому досить прав для перегляду веб-сторінок, але не дозволяючи змінювати файли й настроювання. Це забезпечує захист комп'ютера від атак через Інтернет.

Додаткові можливості захисту в центрі забезпечення безпеки. Центр забезпечення безпеки Windows повідомить користувача й допоможе вжити заходів по усуненню проблеми, якщо встановлене програмне забезпечення не оновлене або рівень безпеки занадто низок і існує потенційна небезпека. Центр забезпечення безпеки Windows у системі Windows удосконалений. У нього додані відомості про антишпигунські програми, настроювання оглядача Internet Explorer і параметрах керування обліковим записом користувача.

Одержіть додатковий контроль над роботою програм. За замовчуванням у системі Windows програми запускаються в більш безпечному режимі. При роботі більшості додатків у випадку спроби виконати потенційно небезпечну операцію, що вимагає повноважень адміністратора, у системі Windows виводиться запит на одержання згоди користувача. Це дозволяє знизити ризик проникнення вірусів, програм-шпигунів і інших погроз. Щоб захистити сімейний комп'ютер, створіть більш безпечні стандартні облікові записи користувачів для всіх членів родини й використовуйте їх при виконанні щоденних завдань. У цьому випадку, якщо дитина спробує встановити яку-небудь програму, комп'ютер запросить пароль облікового запису адміністратора. Якщо дитина його не знає, вона не зможе самостійно встановити нові програми або перевизначити параметри батьківського контролю.

Захистіть особисті дані

Використовуйте антифішинг-фільтр для захисту облікових даних. Оглядач Internet Explorer у складі системи Windows має фільтр, що при перегляді веб-вузлів повідомляє про можливість фішинг-атаки з метою розкрадання конфіденційної інформації. Фільтр виконує перевірку за списком відомих веб-вузлів фішингу, обновлюваному кілька разів у годину, а також виявляє підозрілі веб-вузли, ще не занесені в базу даних.

Видалення даних журналу користування Інтернетом одним клацанням. Інформація про відвідуваний веб-вузли й відомості, що вводяться при перегляді веб-вузлів, зберігаються в різних місцях на комп'ютері. В оглядачі Internet Explorer у системі Windows не потрібно видаляти особисті дані в різних місцях. З функцією видалення історії перегляду можна видалити всі відомості про перегляд одним клацанням миші.

Архівуйте й відновлюйте настроювання, файли й додатки. У системі Windows є більше повний і простий засіб резервного копіювання, чим базова програма архівації системи Windows XP. Нова програма архівації Windows забезпечує додаткові можливості збереження резервних копій даних. Користувачам більше на прийде турбуватися про регулярну архівацію даних. Зручний майстер дозволяє становити розклад архівації й указувати місце збереження резервних копій.

Захистіть свою родину

Захистіть дітей, використовуючи батьківський контроль. Windows надає широкий спектр потужних засобів батьківського контролю, що допомагають спостерігати за тим, як діти користуються комп'ютером, контролювати цей процес і забезпечувати їхня безпеку.

Переглядайте докладні звіти про дії. Windows створює докладні звіти про дії дітей на комп'ютері, включаючи відомості про те, у які ігри вони грали, які веб-вузли відвідували і які додатки запускали.

Установіть обмеження перегляду веб-вузлів. Безкоштовна веб-служба, надавана із системою Windows, дозволяє обмежити типи веб-вузлів, які може відвідувати дитина. Можна обмежити перегляд веб-вузлів по категоріях, наприклад заблокувати всі веб-вузли з порнографічним умістом або азартними іграми, а також окремі веб-вузли по URL-адресі. Ці обмеження підтримуються більшістю веб-оглядачів.

Контролюйте гри, у які грає дитина. Система Windows дозволяє легко вказати, у які ігри можуть грати діти. З її допомогою можна:

– дозволяти або забороняти дітям грати в певні ігри;

– обмежити можливість грати в ігри, призначені для певного віку;

– блокувати ігри, що містять інформацію, небажану для перегляду або прослуховування дітьми.

Установіть межі часу роботи за комп'ютером. У системі Windows можна вказати, коли й протягом якого часу дитина може користуватися комп'ютером.

Дії у випадку фішинг-атаки

Ви можете зробити все для запобігання крадіжки особистих даних у результаті фішинг-атаки, але повну безпеку й захист не може гарантувати жодна система й жоден методи. Якщо ви підозрюєте, що вже відповіли на фішинг-повідомлення, указавши особисту або фінансову інформацію або ввівши її на фальшивому веб-вузлі, ви ще можете звести збиток до мінімуму.

Крок 1 Заявіть про порушення безпеки

Якщо ви думаєте, що ваша особиста інформація піддалася небезпеки або була викрадена, негайно повідомите про обставини події в наступні організації:

– **У компанію по випуску кредитних карт, якщо ви подали відомості про кредитну карту.** Це потрібно зробити в першу чергу. Чим раніше в організації довідаються, що ваш рахунок піддався небезпеки, тим легше їм буде захистити вас.

– **У компанію, чиє ім'я, на вашу думку, було використано.** Помніть, що звернутися в організацію потрібно безпосередньо, а не через отримане повідомлення електронної пошти.

– **У Центр скарг на шахрайства в Інтернеті (IFCC).** Центр Internet Fraud Complaint Center (IFCC) — це результат партнерства ФБР і національного центра по боротьбі зі злочинами «білих комірців» (NW3C). Він працює по усьому світі за підтримкою правоохоронних органів і представників галузі, негайно закриває підроблені веб-вузли й виявляє за ними зловмисників, які стоять за ними.

– **Федеральна комісія з торгівлі.** Якщо ви думаєте, що ваша особиста інформація піддалася небезпеки або була викрадена, повідомте про обставини події у Федеральну комісію з торгівлі (FTC): національний центр по розкраданнях особистих даних і відвідайте її веб-вузол, щоб довідатися, як звести можливий збиток до мінімуму.

Про фішинг-атаку можна також повідомити в робочу групу Anti-phising Working Group за адресою reportphising@antiphising.org, а також у Федеральну комісію з торгівлі (FTC) за адресою spam@uce.gov. Для цього створіть нове повідомлення, адресоване цим групам, і вкладіть в нього шахрайське повідомлення електронної пошти. Можна також повністю скопіювати його й вставити в нове повідомлення. Намагайтеся не використовувати команду «Переслати», оскільки цей формат може виключити деяку інформацію й зажадати ручної обробки повідомлення.

Крок 2 Змініть паролі для всіх облікових записів.

Якщо ви думаєте, що повідомили пароль у відповідь на фішинг-сообщение або ввели його на шахрайському веб-вузлі, перемініте його якомога швидше.

Крок 3 Регулярно перевіряйте банківські звіти й звіти по кредитних картах

Роблячи це принаймні щомісяця, ви зможете піймати шахраїв і зупинити їх, перш ніж вони нанесуть вам відчутний збиток.

Крок 4 Застосовуйте новітнє антивірусне й антишпигунське програмне забезпечення

Деякі шахрайські повідомлення електронної пошти можуть містити шкідливі або небажані програми, які відслідковують дії користувача або просто сповільнюють роботу комп'ютера.

Розробка структурної схеми

На структурній схемі (рисунок 3.1) зображена розроблена під час дипломного проектування система протидії шахрайським діям у мережі Інтернет.

Розробка системи антифішингу повинна ґрунтуватися на потужній базі – браузері з розширеними можливостями. Так як найпоширеніший браузер Microsoft Internet Explorer

поширюється із закритим вихідним кодом, а також має сховану структуру, що негативно впливає при написанні додаткових програм і плагінів на його основі й проаналізувавши існуючі на даний момент браузери, і їхні розподілені системи захисту , я зупинив свій вибір на браузері FireFox.

Він має величезну кількість переваг, головна з яких – надання великої кількості підпрограм що дозволяють одержати доступ до пошти, використанню Інтернет-пейджерів систем IRC, Viber, Telegram, WhatsApp, AIM.

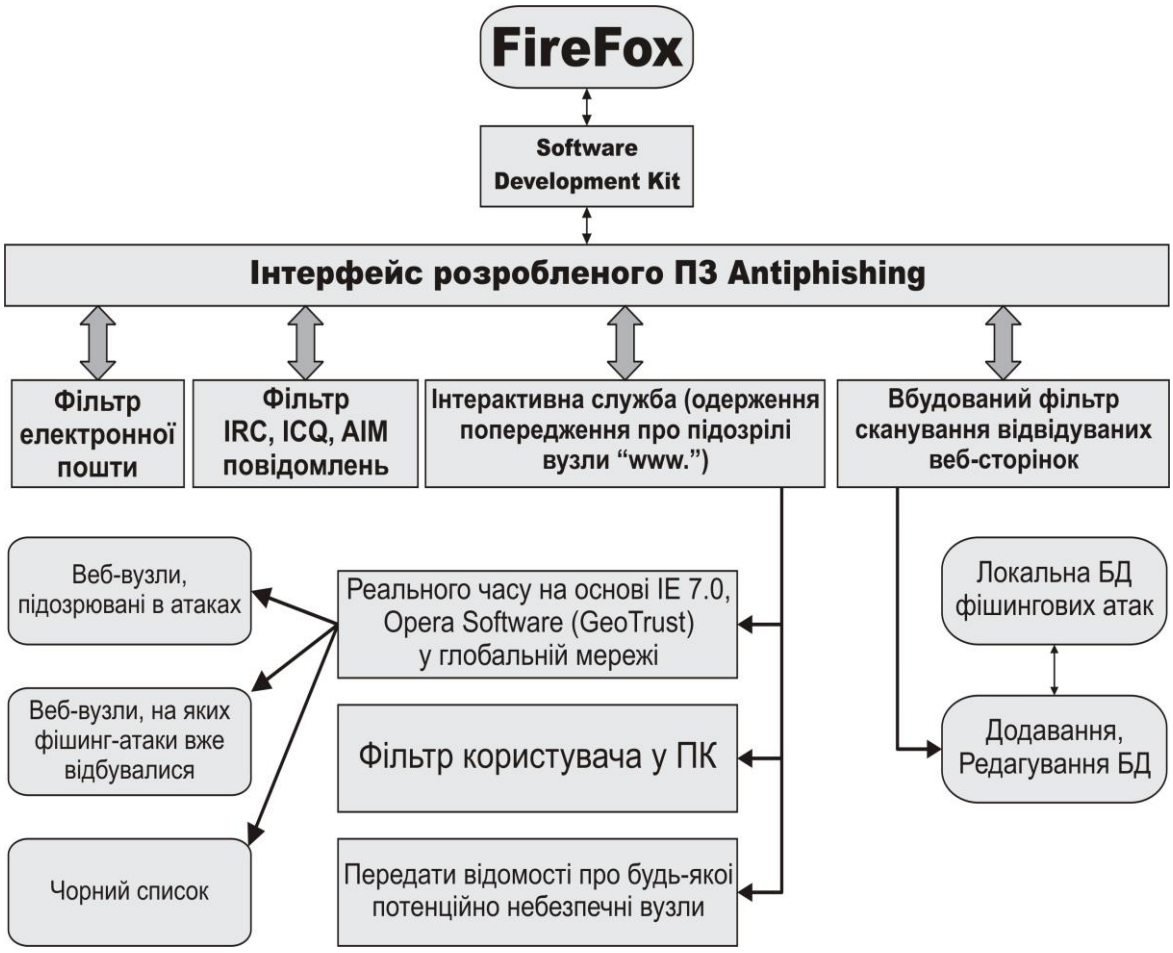


Рисунок 1 – Структурна схема роботи та взаємодії системи

FireFox розповсюджується із частково відкритим кодом і має розширений набір засобів (Software Development Kit) для написання й розповсюдження додатків на його основі.

Як показано на рисунку 1, система антифішингу заснована на браузері FireFox і робить взаємодію через Software Development Kit.

Розглянемо загальні можливості розробленого програмного забезпечення зображені на схемі. Через розроблену систему антифішингу відбуваються наступні дії:

1. Фільтр електронної пошти – дозволяє частково убезпечити поштові повідомлення від фішингових атак розширеним керуванням і контролем даних, що надходять,. Фільтр спільно працює з антивірусними програмними продуктами й фаєрфолами (якщо такі присутні в операційній системі) не викликаючи конфліктних ситуацій і зависань тому що працює через браузер Firefox.

2. Фільтр IRC, Viber, Telegram, WhatsApp, AIM повідомлень – При використанні внутрішньої програми спілкування через Інтернет-пейджери IRC, Viber, Telegram, WhatsApp, AIM – розроблене програмне забезпечення антифішингу дозволяє контролювати процес передачі файлів і не дати зробити несанкціонований запуск шкідливої програми на ПК.

3. Інтерактивна служба (одержання попередження про підозрілі вузли “www.”) – складається із трьох підрозділів, які дозволяють інтерактивно контролювати WEB контент, який попадає на машину користувача.

3.1 Реального часу на основі IE, Opera Software (GeoTrust) у глобальній мережі – з версії браузерів IE і Opera з'явився новий безкоштовний Інтернет сервіс, який надає доступ до всесвітньої бази перевірки веб-вузлів. В Інтернеті існує величезна кількість посилань на сайти при переході на які, відбувається запуск шкідливого програмного забезпечення й крадіжка особистої інформації, у даних випадках антивирустні програми неспроможні тому що використовуючи помилки ОС шкідливі програми одержують статус перевірених. За допомогою цього безкоштовного сервісу й розробленого в дипломному проекті можна значною мірою усунути можливість запуску такого шкідливого коду.

Інтерактивний сервіс повертає наступні повідомлення:

– Веб-вузли, підозрювані в атаках;

– Веб-вузли, на яких фішинг-атаки вже відбувалися;

– Чорний список .

3.2 Фільтр користувача в ПК – локальний фільтр блокування доступу складений користувачем. Існують різні ситуації під час роботи ПК, фільтр користувача дозволяє скласти список ресурсів доступ на який буде заборонений при переадресаціях і.т.ін.

3.3 Передати відомості про будь-які потенційно небезпечні вузли – можливість послати в інтерактивну службу дані для перевірки на наявність на сайті фішингово-шкідливого коду.

4. Вбудований фільтр сканування відвідуваних веб-сторінок – розширені можливості переходу на сторінки, які відвідувалися, з перевіркою на можливу переадресацію, а також база шаблонів відомих шкідливих кодів з можливістю редагування.

4.1 Додавання, Редагування БД – можливість редагування й ручного додавання шаблона відомих шкідливих кодів.

4.2 Локальна БД фішингових атак – шаблонів відомих шкідливих кодів.

За допомогою даних засобів імовірність фішингової атаки через електронну пошту й Spam, фішинг-атаки з використанням web-контента, фальсифиция рекламних банерів, IRC і передача IM-повідомлень, використання троянських програм значно зменшується надаючі користувачеві надійну систему захисту.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів протидії шахрайським діям у мережі Інтернет. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем протидії шахрайським діям у мережі Інтернет. Досліджена система протидії шахрайським діям у мережі Інтернет. На основі отриманих результатів досліджень створена програмна реалізація системи протидії шахрайським діям у мережі Інтернет. Розроблені алгоритми дозволяють успішно вирішувати завдання протидії шахрайським діям у мережі Інтернет. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко

С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

А. Шаповалов, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ТА ВІДНОВЛЕННЯ ДАНИХ В ХМАРНИХ СЕРВІСАХ

У статті розроблено програмне забезпечення, яке призначено для системи захисту та відновлення даних в хмарних сервісах. Метою розробки є дослідження та програмна реалізація системи захисту та відновлення даних в хмарних сервісах. Об'єктом дослідження є процес захисту та відновлення даних в хмарних сервісах. Предметом дослідження є методи захисту та відновлення даних в хмарних сервісах. Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту та відновлення даних в хмарних сервісах. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, захист даних, відновлення даних, хмарні сервіси

Постановка проблеми. Усе було б дуже просто, якби дані перебували під постійним захистом від всіх видів погроз, забезпечення їхнього захисту не робило впливу на бізнес-операції й дані вдавалося миттєво відновити. Але, як і у всіх інших аспектах, що мають відношення до інформаційних технологій, при проектуванні інфраструктури ефективного захисту даних доводиться йти на певні компроміси.

Головними атрибутами оцінки ефективності рішень для захисту й відновлення даних є вікно резервного копіювання, цільова точка відновлення (Recovery Point Objective, RPO) і цільовий час відновлення (Recovery Time Objective, RTO). Ці параметри характеризують час,

виділюваний для операцій резервного копіювання, інтервал між двома такими операціями й тривалість процедури відновлення, виконуваної у випадку помилки, збоїти або аварії.

Кожний з них є також мірилом простою:

- часу, протягом якого дані недоступні в процесі резервного копіювання;
- часу, що потрібно для відтворення нових, ще не зарезервованих даних;
- часу, яке потрібно затратити на операцію відновлення.

Залежно від того, яке місце в організації займають система й дані, які захищаються, тривалість простою, викликаного операціями захисту або відновлення, тим або іншим способом відіб'ється й на фінансових показниках.

Середня вартість простою в різних галузях становить 5600 доларів у хвилину, або більше 300 тис. доларів у годину. Неприступність критично важливих даних обходиться великим організаціям у мільйони доларів у годину.

Усе було б дуже просто, якби дані (особливо мають важливе значення для бізнесу) перебували під постійним захистом від всіх видів погроз, забезпечення їхнього захисту не робило впливу на бізнес-операції й дані вдавалося миттєво відновити у всіх ситуаціях. Але є й четвертий показник ефективності – вартість.

Як і у всіх інших аспектах, що мають відношення до інформаційних технологій, та й у повсякденному житті, при проектуванні інфраструктури ефективного захисту даних доводиться йти на певні компроміси, щоб:

- кожному конкретному набору даних, залежно від його цінності для організації, надавалися мінімальні рівні сервісу (вікно резервного копіювання, RPO, RTO), абсолютно необхідні для ведення бізнесу;
- організація несла мінімально можливі витрати.

Інвестиції в рішення для захисту даних найкраще розглядати як витрати на страхування, які не приносять організації доходів і інших вигід, поки не трапляється якась серйозна неприємність, після чого впливають лише на показники прибутку. Однак у дійсності всі не зовсім так.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи захисту та відновлення даних в хмарних сервісах

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи захисту та відновлення даних в хмарних сервісах.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем захисту та відновлення даних в хмарних сервісах.
- Дослідження системи захисту та відновлення даних в хмарних сервісах.
- Програмна реалізація системи захисту та відновлення даних в хмарних сервісах.

Об'єктом дослідження є процес захисту та відновлення даних в хмарних сервісах.

Предметом дослідження є методи захисту та відновлення даних в хмарних сервісах.

Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення.

математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Стратегія захисту й резервного копіювання даних повинна враховувати розширення сфери IT, у яку тепер входять не тільки ЦОДи, але й публічні хмари, а також периферійні обчислення.

Резервне копіювання й захист даних зараз важливіше, ніж коли-або, оскільки ми вступили в епоху хмар і рухаємося до усе більше розосередженого екосистемі IT. Але в будь-якій екосистемі надійний план резервного копіювання повинен базуватися на аудиті підметів захисту даних і на процесах, які можуть бути використані для забезпечення їхньої безпеки.

Масштаби захисту даних

Захист даних охоплює широкий спектр сценаріїв, у т.ч. наступні:

– ушкодження – системне ПЗ або застосунки випадково змінюють контент;
– помилка користувача – користувачі ненавмисно видаляють дані;
– відмова устаткування – різного роду проблеми з носіями інформації, збої серверів і т.п.;
– втрата устаткування – його вихід з ладу в результаті пожежі, повені або крадіжки;
– зловмисне знищення – різні дії, спрямовані на видалення даних або відмову в доступі до них, наприклад, за допомогою вимагацького ПЗ.

Хоча більшість таких сценаріїв ставляться до приватних ЦОДів, що розширюється використання публічних хмар означає, що ці середовища також повинні бути захищені.

Отже, для захисту даних варто використовувати застосунки, що запускаються на власній площадці, а також працюючі в якості платформи хмарного ПЗ, такі як Office365 або SalesForce.com.

Сервіси публічних хмар начебто названих вище не роблять резервне копіювання даних за замовчуванням, тільки для відновлення після системних збоїв. Тому відновлення повідомлень електронної пошти після їхнього видалення лягає на власника даних і повинне бути передбачене планом захисту.

Оскільки величезна інфраструктура доступна через Інтернет, IT-підрозділам варто також подбати про захист від витоків даних (DLP).

Дотримання рівнів обслуговування

Задовольнити потреби бізнесу в забезпеченні безпеки даних можна завдяки застосуванню різних рівнів обслуговування до захисту й відновлення даних. Іншими словами, параметри відновлення визначають мети захисту.

Двома головними критеріями є час відновлення (Recovery Time Objective, RTO) і точка відновлення (Recovery Point Objective, RPO). Останній визначає обсяг припустимої втрати даних. Наприклад, RPO=0 означає, що повинні бути відновлені всі дані, які були наявні на момент збою.

Реплікація або резервне копіювання

Захист даних виробляється за допомогою ряду доступних технологій.

Реплікація – це процес створення безлічі надлишкових копій даних розраховуючи на те, що хоча б одна з них збережеться після катастрофи.

Звичайно реплікація здійснюється за допомогою синхронного або асинхронного копіювання з використанням масиву пам'яті. Але копіювання може вироблятися на рівні гіпервізору й застосунку. Платформи баз даних уже надають можливість реплікації за допомогою таких інструментів, як доставка журналів (log shipping). Платформи NoSQL дозволяють робити реплікацію по моделі погодженості в остаточному підсумку (eventual consistency).

Варто пам'ятати, що тільки реплікації недостатньо для повного захисту даних. Синхронна реплікація, наприклад, створить репліку ушкоджених даних. А асинхронна репліка не відбиває останніх змін.

Погодженість в остаточному підсумку

Погодженість в остаточному підсумку застосовна також до розподіленого зберігання. Наприклад, до об'єктних сховищ.

Коли затримка не має великого значення, дані можна розподілити географічно за допомогою алгоритмів з кодом надмірності (erasure coding) і асинхронного реплікування у фоновому режимі, іменованого погодженістю в остаточному підсумку.

Одним з головних переваг використання коду надмірності є можливість відновлення даних з підмножини захищеного контенту без створення додаткових повних копій.

Код надмірності здатний захистити, наприклад, від втрати даних у чотирьох точках при збільшенні ємності зберігання всього на 25%. Це дозволяє здійснювати захист багатохмарних об'єктних сховищ, що поширюється одночасно на кілька хмарних провайдерів і власні ЦОДи підприємств.

Моментальні знімки й відстеження змінених блоків даних

У найбільш сучасних платформах резервного копіювання застосовуються створення моментальних знімків і відстеження змінених блоків даних (changed block tracking, CBT).

Моментальні знімки фіксують дані застосунків на певний момент часу й робляться відповідно до графіка, звичайно під час пауз в операціях уведення-виводу застосунків, щоб гарантувати цілісність даних.

CBT дозволяє одержати доступ до потоку змінених даних у джерела замість того, щоб копіювати весь набір даних і займатися його дедуплікацією за допомогою пристрою або ПЗ резервного копіювання.

Найбільш очевидним є застосування моментальних знімків і CBT на віртуальних серверах, де гіпервізори типу VMware vSphere надають доступ до потоку змінених із часу останнього моментального знімка даних. Потім ПЗ резервного копіювання створює синтезовані образи з повних і часткових резервних копій для відновлення даних у майбутньому.

Крім того, CBT добре працює з гіперконвергентними рішеннями, де потік змінених даних забезпечується на інтегрованому рівні зберігання. Nutanix Acropolis надає таку можливість для блокових сховищ, прикріплених до віртуальних машин, і для даних, що зберігаються в Nutanix Files.

CBT і моментальні знімки дозволяють набагато швидше обробляти резервні копії даних, особливо в мережах резервного копіювання. Провайдери публічних мереж надають можливість виготовлення моментальних знімків на своїх платформах для підключених до віртуальних машин пристроїв блокового зберігання. Моментальні знімки даних переносяться на більше дешеві носії для довгострокового зберігання.

Хмари

Публічні хмари створюють деякі нові проблеми й можливості для захисту даних.

Як вказувалося вище, застосунки захищають дані, використовуючи моментальні знімки.

Публічні хмари можуть використовуватися для зберігання даних, що захищаються, і архівування моментальних знімків. Вони також відмінно підходять для зберігання резервних копій завдяки можливості доступу з будь-якої географічної точки й убудованому захисту від втрати даних і збоїв. Немає необхідності піклуватися про масштабування сховища резервних копій, оскільки провайдер гарантує практично необмежену масштабованість.

Але використання публічних хмар для зберігання резервних копій має деякі недоліки.

По-перше, що досягається за допомогою дедуплікації даних економія обсягу не передається клієнтові. Тому ПЗ резервного копіювання повинне робити дедуплікацію до запису даних у хмару.

По-друге, варто враховувати проблему продуктивності. Швидкість відновлення даних з публічної хмари залежить від наявної смуги пропущення й часто обмежується провайдером.

Зараз більшість провайдерів підтримують зберігання резервних копій у публічних хмарах. У багатьох випадках програмно-апаратні рішення (які доповнюють розглянуті нижче апаратні рішення) можуть використовуватися також для відновлення даних у публічній хмарі як первинній системі зберігання. Це означає, що публічні хмари здатні заміняти традиційні площадки, призначені для віднолення після катастроф.

Устаткування

Устаткування, що дозволяє використовувати публічну хмару в якості репозиторія резервних копій, розгортається на власній площадці підприємства. Воно кешує дані локально, тоді як архівування колишніх моментальних знімків і резервних копій відбувається на недорогих системах, таких як об'єктні сховища, на власній площадці або в публічній хмарі.

Оскільки відновлення даних звичайно виробляється за допомогою найбільш свіжої версії резервної копії, архівування в публічній хмарі за допомогою апаратного рішення є економічним і дозволяє IT-підрозділам дотримувати угод про рівень обслуговування.

Вимагацьке ПЗ й безпека

Новим є розгортання застосунків у публічних ЦОДах і на периферії обчислювальних середовищ. Для надання локальних сервісів часто використовуються невеликі ЦОДи або машинні зали. При такому розосередженні обчислювальної потужності й даних набагато більше систем піддаються небезпеки зараження вимагацьким ПЗ.

При атаках з використанням вимагацького ПЗ хакери встановлюють на зламані сервери або ПК код, що шифрує локальні дані, і вимагають викупу за їхнє розблокування й надання до них доступу.

Виробники систем зберігання допомагають захиститися від подібних атак за допомогою простого відновлення даних з резервних копій, а також допомагають визначити, де відбулася атака, за допомогою відстеження змінених даних у відведене на резервне копіювання час.

Захист від вимагацького ПЗ – тільки частину необхідної сьогодні захисту даних. Резервні копії повинні зашифровуватися й надійно захищатися при мінімальному контрольованому доступі тільки до тих з них, які використовуються для відновлення даних.

Формування стратегії

Як міняється захист даних? Які стратегії варто використовувати IT-підрозділам?

Якщо колись захист даних будувалася навколо поділюваного зберігання й гіпервізору, то сьогодні методи захисту набагато більше різноманітні.

Тому захист вимагає безлічі процесів резервного копіювання й спостереження за статусом резервних копій, що зберігаються на власній площадці й поза нею.

Така стратегія повинна бути прив'язана до мобільності даних, оскільки в майбутньому застосунку можуть стати набагато більше мобільними й мати потребу в крос-платформному відновленні даних.

Імовірно, головною проблемою для адміністраторів зберігання й фахівців із захисту даних у найближчі роки буде домогтися, щоб дані застосунків можна було зробити доступними або вчасно їх відновити незалежно від того, де виконується робоче навантаження.

Таким чином, у майбутньому акцент, імовірно, буде зроблений на самих даних, щоб забезпечити їхню постійну доступність незалежно від платформ, на яких вони зберігаються.

В умовах збільшення числа серверів, систем зберігання, мережних платформ і застосунків, а також територіально розподіленого розміщення ресурсів IT-інфраструктура стає дуже складною. Розвиток технологій у сполученні із щорічним ростом обсягів даних на 40-50% і ще більш твердими вимогами до рівня сервісу з боку зацікавлених осіб надзвичайно ускладнило завдання захисту даних. На структурній схемі (рисунок 1) показані можливі ситуації, які необхідно враховувати при складанні плану захисту й відновлення даних.

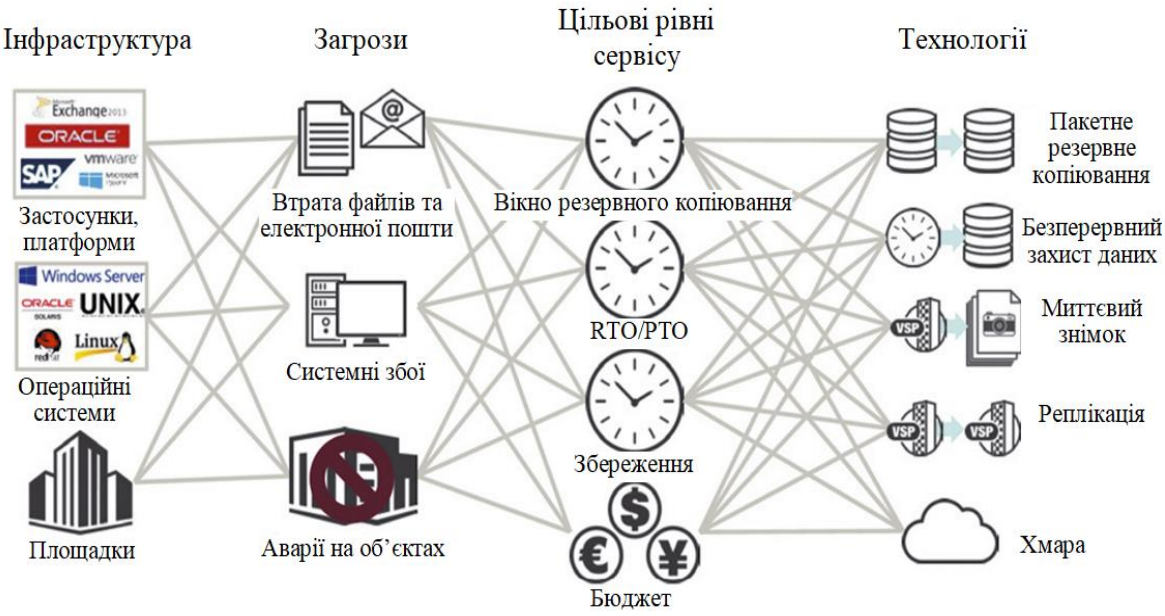


Рисунок 1 – Структурна схема системи

Адміністратори резервного копіювання зіштовхуються з масою інфраструктурних складностей. Кожний компонент інфраструктури необхідно захищати від різноманітних погроз і враховувати при цьому цільові рівні сервісу кожного підрозділу-бізнесу-підрозділу. Вони визначають політики, яким повинен випливати набір рішень для захисту даних, що, у свою чергу, приводить до розширення спектра використовуваних технологій.

У контексті захисту й відновлення даних часто говорять про «вікно резервного копіювання», під яким розуміють тривалість виконання операцій резервного копіювання. З технічної точки зору це невірно. Насправді вікно резервного копіювання являє собою повний інтервал (з урахуванням часу запуску й зупинки), необхідний для виконання резервного копіювання певної системи або набору даних.

Вікно резервного копіювання – один із чотирьох цільових показників, використовуваних для оцінки ефективності процесу захисту даних. До трьох іншим ставляться цільова точка відновлення, цільовий час відновлення й загальних витрат.

Якщо виконання резервного копіювання займає більше часу, ніж припустиме вікно резервного копіювання, можливі наслідки для бізнесу очевидна: або процедура резервного копіювання зупиниться до моменту її завершення з ризиком втрати важливих або навіть критичних даних, або її дозволено буде продовжити. У кожному разі це відіб'ється на рівні готовності системи, що захищається, а отже, і на багатьох операціях.

Найчастіше вікно резервного копіювання представляється неминучим злом. Бізнес визнає необхідність такого простою. Створення резервної копії має важливе значення для виживання організації, незважаючи на те що знижує операційну ефективність і рентабельність. Якщо підприємству вдасться скоротити тривалість створення резервних копій і зменшити або навіть ліквідувати вікно резервного копіювання, у нього з'явиться можливість відшкодувати упущену вигоду.

Інша категорія витрат, пов'язаних з тимчасовими витратами, обумовлена часом, що адміністратор витрачає на підтримку операцій резервного копіювання. Колись резервне копіювання виконувалося вручну і являло собою дуже трудомістку операцію. Адміністраторові резервного копіювання було потрібно:

– виконати необхідну установку й внести зміни в конфігурацію для кожної нової системи або користувача;

– маркірувати щодня записувані стрічки, після чого запустити процедуру резервного копіювання й проконтролювати її виконання;

– витягти стрічки для їхнього транспортування в центр післяаварійного відновлення або сховище;

– стерти інформацію зі стрічок, на яких зберігаються неактуальні резервні копії, для їхнього повторного використання;

– у випадку збоїти усунути неполадки й запустити знову процедуру створення резервної копії (якщо вікно резервного копіювання дозволяє це).

Інтелектуальні політики, автоматизація роботи систем, технології автоматичного виявлення, використання дискових сховищ і реплікація в центр післяаварійного відновлення дозволяють мінімізувати прикладені зусилля й скоротити витрати. Ці функції й підходи допомагають виключити більшу частину ручної праці й скоротити час, затрачуваний на виконання операцій по захисту даних. Однак багато компаній усе ще додержуються старих методів, відмовляючись від резервного копіювання або передаючи ці функції незалежним постачальникам послуг.

Щоб підвищити рівень готовності даних, знизити ризики й скоротити витрати, всі організації – як великі, так і малі – повинні застосовувати сучасні технології захисту даних.

За допомогою пропонованих рішень вікно резервного копіювання можна мінімізувати або навіть виключити. Такі результати досягаються за рахунок повністю інтегрованих технологій безперервного захисту даних (Continuous Data Protection, CDP) на рівні блоків і погоджених з додатками моментальних знімків, які робляться за допомогою спеціальних апаратних засобів. У результаті усувається необхідність сканування файлової системи для пошуку інкрементних змін і скорочується тривалість копіювання даних – до декількох секунд.

Постійне інкрементне резервне копіювання

Засоби створення моментальних знімків і CDP обробляють тільки нові й змінені дані. Використання інкрементної моделі на постійній основі виключає потреба в періодичному повнім резервному копіюванні (або синтетичному повнім резервному копіюванні), властивій більшості інших рішень. Залежно від швидкості зміни даних і тривалості їхнього зберігання такий підхід дозволяє зменшити обсяг збережених резервних копій більш ніж на 90%.

Припустимо, звичайне підприємство, працює п'ять днів у тиждень і 50 тижнів у році. Їм накопичено 100 Тбайт даних, середня швидкість зміни яких становить 10% (10 Тбайт) у день і 50% (50 Тбайт) у тиждень. Резервні копії для оперативного відновлення зберігаються 12 тижнів, а дані, потребуючі більше тривалого зберігання, архівуються.

Це крайній випадок, що ілюструє відмінності традиційної й постійної інкрементної моделі. У типовому середовищі загальний обсяг змінених даних звичайно становить 50% у рік (50 Тбайт), що еквівалентно 1% у тиждень (1 Тбайт) і 0,2% у день (200 Гбайт).

При комбінації повного й інкрементного резервного копіювання, а також у використовуваної Hitachi Data Instance Director (HDID) моделі постійного інкрементного копіювання обсяг щоденної копії становить 10 Тбайт. Однак, у першому випадку у вихідні резервуються 100 Тбайт, тоді як у другому ніяких копій не створюється.

З урахуванням створення первісної повної резервної копії (100 Тбайт) загальний обсяг резервних копій за 12 тижнів складе:

– повне й інкрементне резервне копіювання: 1900 Тбайт (1,9 Пбайт);

– постійне інкрементне резервне копіювання: 700 Тбайт (0,7 Пбайт).

Завдяки дедуплікації даних постійне інкрементне резервне копіювання дозволяє скоротити необхідну ємність зберігання на 63% без додаткових фінансових витрат і зниження продуктивності системи. У скільки обійдуться придбання, керування й підтримка сховища з резервними копіями обсягом 1,2 Пбайт? По суті, це 2,4 Пбайт додаткові простори, тому що ми хочемо реплікувати сховище з резервними копіями в центр післяаварійного відновлення. Якщо дані з копіями зберігаються довше трьох місяців, економія виявиться ще більшою.

У типовому ж середовищі, де за рік міняється 50% даних, для зберігання традиційних резервних копій протягом 12 тижнів знадобиться 1,3 Пбайт, а для зберігання постійних

інкрементних копій – усього 112 Тбайт. Таким чином, економія досягне 91%. Наведене зменшення обсягів ще раз підтверджує, що при традиційному резервному копіюванні майже всі зберігати^ся данние, що, надлишкові.

Керування вікном резервного копіювання – це перший крок до зниження витрат і ризиків, пов'язаних із захистом даних, до забезпечення більше ефективного післяаварійного відновлення й поновлення операційної діяльності.

Як RPO впливає на RTO?

Цільова точка відновлення (RPO) указує на прийнятну для підприємства періодичність створення резервних копій і, таким чином, визначає момент часу, у який можливе відновлення даних. Якщо RPO рівняється 24 год, виходить, однієї операції резервного копіювання в день цілком достатньо. Крім того, даний показник характеризує:

- частоту виконання операцій резервного копіювання;
- обсяг нових даних, які підприємство ризикує втратити.

RPO принципово відрізняється від цільового часу відновлення (RTO). За допомогою RTO можна зрозуміти, як довго буде виконуватися процедура відновлення системи або застосунки або відновлення доступу до набору даних після незапланованої події, викликаного помилкою людини, збоєм устаткування або природним катаклізмом.

RTO визначає, яка тривалість простою (а отже, грошові втрати, ризики й упущена вигода), з яким організація готова миритися у випадку збоїти або аварії. Найчастіше для різних типів даних і видів збоїв установлюється різний цільовий час відновлення – наприклад, друга година для втраченого файлу або електронного листа, шоста година для запуску сервера, що відмовив, і два дні на відновлення операцій у випадку збоїти, що затронули весь об'єкт.

Оскільки RPO і RTO – принципово різні поняття, багатьох цікавить, чи роблять вони вплив один на одного. Як правило, на це питання відповідають негативно, але спосіб досягнення RPO самим безпосереднім образом відбивається на дотриманні RTO.

Представимо, що у вас дуже більша база даних, резервну копію якої можна створити тільки за довгі вихідні. Щоб зменшити RPO до 24 год, щоночі необхідно робити резервні копії журналів бази даних або журналів повторного виконання. У результаті можна відновити останню повну копію бази даних, а потім повторно виконати всі транзакції, збережені в журналах бази даних або журналах повторного виконання.

Число й розміри файлів, які потрібно відновити й використовувати поряд з файлами бази даних, можуть рости дуже швидко, особливо якщо ви маєте справу з масштабним кластерним середовищем на зразок Oracle Real Application Clusters (RAC). Отже, чи буде час, затрачуване на відновлення останньої повної резервної копії й всіх журналів, відповідати відведеному для великої системи баз даних RTO? Відповідь, мабуть, негативний, якщо тільки RTO не виміряється тижнями й місяцями. Така методологія захисту бази даних може бути використана для створення прийнятних цільових точок відновлення, але вона не підходить для дотримання прийнятного цільового часу відновлення.

Схожу ситуацію ми спостерігаємо й при традиційному повному + інкрементном резервному копіюванні, описаному раніше. При такій моделі повна резервна копія звичайно створюється кожні вихідні, а інкрементна – щодня протягом робочого тижня. Якщо збій відбувся в понеділок і потрібно виконати повне відновлення, ніяких труднощів це викликати не повинне: дані відновлюються з останньої резервної копії, зробленої у вихідні.

Якщо ж збій відбудеться в п'ятницю, потрібно відновити повну резервну копію, зроблену в попередні вихідні, а потім послідовно всі інкрементні набори з понеділка по четвер. У п'ятницю процедура відновлення буде виконуватися значно довше, ніж у понеділок. Чи враховується ця обставина в RTO? Крім того, відновлення наприкінці тижня – набагато більше ризикований процес, що складається з декількох етапів, виконуваних вручну. Можливо, деякі з відновлюваних даних прийдеться переписувати до чотирьох разів.

Очевидно, що в міру подальшого збільшення обсягів даних і ускладнення IT-систем використовувані підходи прийде поліпшувати, щоб забезпечити дотримання вимог до

резервного копіювання (RPO) і відновленню (RTO). Компанія Hitachi пропонує рішення, здатне захистити великі бази даних і критично важливі застосунки й значно поліпшити показники RPO і RTO. Воно містить у собі три складові:

– Моментальні знімки й технології реплікації на базі сховища, які:

– виключають із системи керування базами дані операції по захисту даних;

– усувають необхідність у вікні резервного копіювання й пов'язані з ним простої;

– дозволяють виконувати операції резервного копіювання набагато частіше, скорочуючи обсяги нових даних, піддані ризику втрати, на 90% і більше.

– Моментальні знімки й програмне забезпечення реплікації для застосунків і баз даних, які:

– переводять бази даних і застосунку в готове до резервного копіювання (відключене) стан;

– створюють у сховище моментальний знімок, після чого база даних і додаток звільняються для нормального функціонування;

– забезпечують швидке й повністю погоджене відновлення операційної діяльності протягом декількох хвилин, а не тижнів;

– Сервіси оцінки й впровадження, які визначають і конфігурують оптимальне рішення для унікального середовища підприємства.

RPO – можлива схована вартість RTO

Що ставиться до RTO? Залежно від конкретного визначення сюди можуть увійти деякі або навіть усе з наступних складових:

– тривалість вивчення й діагностики події;

– тривалість виконання коригувальних дій: установка нового сервера, заміна диска, відсторонення співробітника, що став причиною неполадок, переклад операцій у резервний центр;

– тривалість переустановки операційної системи й застосунків при виникненні такої необхідності;

– тривалість відновлення всіх потрібних даних з резервної копії або системи післяаварійного відновлення;

– час, витрачений на запуск і тестування відновленого середовища.

Все це виливається в дуже тривалу процедуру й приводить до простоїв. Протягом певного проміжку часу якась частина підприємства не може займатися виробничою діяльністю, що впливає на валовий дохід або прибуток або на те й інше.

Крім того, є параметр, що часто залишається за рамками зазначеного списку, але при цьому самим безпосереднім образом відбивається на тривалості повного відновлення й загальної вартості відновлення. Мова йде про цільову точку відновлення (RPO). Якщо RPO рівняється 24 год (як правило, резервне копіювання виконується вночі), то це означає, що ви готові примиритися із втратою нових даних, отриманих протягом доби.

Найчастіше RPO вибирається із практичних міркувань: наприклад, певну систему можна відключити тільки на ніч або на вихідні. Разом з тим RPO варто визначати з урахуванням вимог бізнесу, а не тільки виходячи з обмежень наявного програмного забезпечення для резервного копіювання.

Уявимо собі, що параметр RPO дорівнює 24 год, а збій системи відбувся о шостій годині вечора, при цьому всі дані, що втримуються там, віддалені або знищені. Можна, звичайно, відновити їх з останньої резервної копії, але вся інформація, створена й змінена після цього, буде загублена.

Ви готові упокоритися із втратою цих даних? Можливо, там присутні кілька великих замовлень із системи продажів, результати проектування за день і багато інші важливі для організації відомості. Просто знизаєте плечима й рушите далі? Звичайно ні. Дані необхідно відновити, тобто ввести заново. Процес цей зажадає якогось часу, протягом якого

співробітники могли б займатися творчою діяльністю, що знов-таки впливає на ефективність бізнесу протягом усього періоду відновлення.

Таким чином, ніж більше інтервал між операціями резервного копіювання (RPO), тим більше даних прийде відновлювати у випадку збоїти й тем вище витрати. Причому це можуть бути не просто матеріальні витрати. Представте тільки, що ви звертаєтеся до клієнта із проханням повторити раніше зроблене замовлення на мільйон доларів, тому що ваша система дала збій!

Міркуючи над цією головоломкою, нескладно прийти до бажаного виводу: необхідно скоротити час, а виходить, і гроші, які доводиться затрачати в процесі відновлення після будь-якого збою. Для цього потрібно:

– значно зменшити вікно резервного копіювання, що обмежує частоту операцій копіювання (RPO);

– істотно збільшити частоту операцій копіювання, щоб якнайменше даних піддавалося ризику втрати, після якої їх доводиться вводити заново;

– прискорити виконання операцій відновлення – як локальних (відновлення операційної діяльності), так і віддалених (післяаварійне відновлення).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту та відновлення даних в хмарних сервісах. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем захисту та відновлення даних в хмарних сервісах. Досліджена система захисту та відновлення даних в хмарних сервісах. На основі отриманих результатів досліджень створена програмна реалізація системи захисту та відновлення даних в хмарних сервісах. Розроблені алгоритми дозволяють успішно вирішувати завдання захисту та відновлення даних в хмарних сервісах. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
2. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
3. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
4. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
5. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
8. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
9. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.

10. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.

УДК 004

В. Чаус, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЛЯ АУДИТУ БЕЗПЕКИ НА БАЗІ ТЕХНОЛОГІЇ SECURITY INFORMATION & EVENT MANAGEMENT

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Метою розробки є дослідження та програмна реалізація системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Об'єктом дослідження є процес кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Предметом дослідження є методи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, Security Information, Event Management

Постановка проблеми. Системи захисту постійно розвиваються й адаптуються до нових видів погроз. Кількість джерел інформації, з яких надходять дані по поточному стані захищеності, росте з кожним днем. Коли інфраструктура занадто складна, неможливо встежити за загальною картиною яка відбувається у ній в ній. Якщо вчасно не реагувати на виникаючі погрози й не запобігати їх, користі не буде навіть від сотні систем виявлення вторгнень. На допомогу приходять системи Security Information and Event Management (SIEM).

Перед системою SIEM ставляться наступні завдання.

Консолідація й зберігання журналів подій від різних джерел – мережевих пристроїв, застосунків, журналів ОС, засобів захисту. Заглянувши в будь-який стандарт ІБ, ви побачите технічні вимоги до збору й аналізу подій. Вони потрібні не тільки для того, щоб виконати вимога стандарту. Бувають ситуації, коли інцидент побачили пізно, а події вже давно затерті або журнали подій чому-або недоступні, і причини інциденту виявити фактично неможливо. Крім того, з'єднання з кожним джерелом і перегляд подій займе багато часу. У противному випадку, без аналізу подій, є ризик довідатися про інцидент у вашій компанії з новиних стрічок.

Надання інструментів для аналізу подій і розбору інцидентів. Формати подій у різних джерелах розрізняються. Текстовий формат при більших обсягах сильно стомлює, знижує ймовірність виявлення інциденту. Частина продуктів класу SIEM уніфікує події й робить їх більше читабельними, а інтерфейс візуалізує тільки важливі інформаційні події, акцентує на них увагу, дозволяє відфільтрувати некритичні події.

Кореляція й обробка за правилами. По одній події не завжди можна судити про інцидент. Найпростіший приклад – «login failed»: один випадок нічого не виходить, але три й більше таких події з одним обліковим записом уже можуть свідчити про спроби підбора. У

найпростішому випадку в SIEM правила представлені у форматі RBR (Rule Based Reasoning) і містять набір умов, тригери, лічильники, сценарій дій.

Автоматичне оповіщення й інцидент-менеджмент. Основне завдання SIEM – не просто зібрати події, але автоматизувати процес виявлення інцидентів з документуванням у власному журналі або зовнішній системі HelpDesk, а також вчасно інформувати про подію.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

Огляд існуючих систем кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management.

Дослідження системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management.

Програмна реалізація системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management.

Об’єктом дослідження є процес кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management.

Предметом дослідження є методи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. З появою перших засобів захисту інформації виникли перші пекучі питання: як довідатися, що зведені барикади працюють і захищають? як швидше реагувати на оповіщення? як зрозуміти, які погрози вдалося запобігти? Чи працює наш файерволл, можна довідатися, виконавши ICMP ping: якщо правила в ACL (access control list) працюють, то відповідей, що містять echo reply, бути не повинне. Можна через консоль пристрою переглянути журнал подій, розбираючи сотні або тисячі рядків вручну й намагаючись побачити відбиту або виявлену погрозу.

Час – гроші

Журналів подій, одержуваних від одних тільки активних засобів захисту, – багато, не говорячи вже про критичні сервери, бази даних, застосунках. За допомогою цих журналів можна виявити несанкціоновані спроби доступу, мережеві атаки, аномалії, що ведуть до порушення безперервності бізнесу або політик безпеки. Щоб відкрити журнал подій, потрібно виконати послідовність дій, які вимагають часу: запустити додаток, підключитися до консолі, вивести список подій і вивчити його. Навіть якщо допустити, що один співробітник відповідає тільки за контроль антивірусного ПЗ (припустимо, що є централізована консоль керування), установку відновлень і IPS (припустимо, що їх не більше 2-4), – на перегляд подій від цих джерел і розбір проблем за останню добу в нього піде біля години. Відзначимо людський фактор: офіцер може бути завантажений іншими справами, може боліти або бути у відпустці, відволіктися від роботи або виконати її для проформи. Тепер порахуйте, скільки людино-годин потрібно, щоб аналізувати журнали подій на критичних активах хоча б раз у добу? Урахуйте в розрахунках заробітну плату кваліфікованого співробітника, здатного виявити погрози в цих журналах подій, урахуйте час, необхідне для підключення до СЗІ у вашій філії по повільних каналах зв'язку. Дорого? Так, виходить кругла сума, назвавши яку керівництву, ви, швидше за все, будете виставлені з кабінету.

Отже, ви встановили засоби захисту, настроїли їх, вони працюють, – що вам ще потрібно? SIEM заміняє не один десяток людей, працює оперативно й не буде просити про підвищення зарплати.

Захист бізнесу

Головне завдання ІБ – забезпечити захист бізнесу й безперервність бізнес-процесів. Що для цього потрібно? Описуються бізнес-процеси, визначаються активи, проводиться їхній аудит (включаючи сканування й пентести), складається модель порушника, вивчаються ризики, складається план їхньої мінімізації. Які міри приймаються для мінімізації ризику? Створюються політики, проводиться навчання користувачів, установлюються засоби захисту інформації, змінюються конфігурації, установлюються відновлення…Ми все це зробили – і залишили як є? до наступного циклу PDCA?

Тримати руку на пульсі

Принцип «поставити й забути» в ІБ не застосуємо. Абсолютного захисту не існує, і самі малоймовірні ризики можуть гукнутися зупинкою бізнесу й величезних фінансових втрат. Будь-яке програмне й апаратне забезпечення може перестати працювати або бути невірно налаштоване – і пропустити погрозу. Бачили панель керування в сучасних літаках? Всі важливі індикатори зібрані воєдино з дотриманням ергономіки й пріоритету. Пілот і його помічник не можуть не побачити порушення критично важливого показника. Так і в SIEM: у випадку будь-якого відхилення від baseline або політик (курс літака) або порушення працездатності активу в результаті збоїв або погроз (неполадки в устаткуванні) – оператори-пілоти будуть негайно сповіщені.

Чому негайно й що буде через годину? Віруси поширюються в лічені секунди, у зловмисників є автоматизовані комплекси для аналізу й експлуатації уразливостей. Подія про що посипались RAID-масиви в системі, що перебуває в промисловій експлуатації, завтра вам буде вже не цікаво, тому що частина даних (або навіть усі) будуть загублені. Чим більш оперативно ви будете інформовані, чим швидше уживете заходів, – тим менше фінансових втрат понесе ваш бізнес. Добре, якщо той що відбувся інцидент не буде мати наслідків.

Превентивного захисту не існує

Якщо ми встановлюємо централізоване антивірусне ПЗ – необхідно переконатися, що воно встановлено скрізь, правильно зконфігуровано, працює з актуальними базами. Як? За допомогою журналів подій.

Навіщо? Представте, що ви автоматизували установку корпоративного антивірусного ПЗ й відновлення баз. Аудит журналу подій ви здійснюєте раз у два-три дні, але відбувся збій, в ОС на робочій станції, що коштує на складі, не запускається сервіс і вона заражена вірусом, що поширюється по мережі. Абсолютно не факт, що на всіх серверах заборонений, приміром, автозапуск, установлені всі заплатки: у реальному житті такого практично не буває. Автоматично розміщений використовуючий уразливість троян з автозапуском і поширенням по мережі або підробленому ярлику на загальному мережевому ресурсі приводить до колапсу всієї компанії. Поки ви будете в авральному режимі аналізувати те, що відбулося – бізнес, швидше за все, буде простоювати, а начальство – нервувати й обурюватися. Фінансову оцінку збитків від простою підприємства легко зробити самостійно, благо це не так складно. Крім того, подібні збої мають властивість негативно впливати на премії й зарплату.

Контрольована погроза, прийнятий ризик

На практиці зустрічаються випадки, коли безпека йде врозріз із бізнесом. Трапляються ситуації, коли не можна поставити відновлення, щоб закрити уразливість (причин маса: сертифікація, нестабільність роботи, «не протестовано», конфлікт із іншим ПЗ), або, наприклад, неможливо заборонити RPC, оскільки бізнес-додаток перестане працювати. Витрати на усунення погрози можуть перевищувати можливі втрати, тому ризик «приймається». Однак ми можемо контролювати подібні ризики за допомогою SIEM, реагувати на виникаючі інциденти, повертаючи по закінченні року засоби, виділені на покриття операційних ризиків, назад у бюджет. Природно, що в цьому випадку не може бути

й мови про перегляд оператором журналів міжмережевого екрана без автоматичного аналізу й реєстрації інцидентів як способу контролю ризиків.

Немає причини – усі винуваті

Ви напевно зіштовхувалися з випадками, коли для рішення інциденту немає даних: відсутня інформація про точний час і місце виникнення (не вважаємо дзвінки від користувачів), про те, що передувало інциденту; і ми не можемо відповісти на головні питання – чому відбувся інцидент і хто в цьому винуватий. Ні, це потрібно не для того, щоб покарати винних (хоча це теж іноді необхідно). Головне, що необхідно з'ясувати за підсумками інциденту, – що робити, щоб інцидент не повторився. Причому одного тільки убудованого в ОС журналу (Windows event log або syslog) може виявитися недостатньо.

Системний адміністратор

У зрілій розгалуженій інфраструктурі права адміністрування делегуються досить широкому колу співробітників. Природно, всі ці співробітники проходять перевірку служби безпеки, і ми їм довіряємо. Але на практиці найчастіше позначається людська психологія: співробітник, порушивший базу даних, RAID, що приніс на особистій флешці вірус, через якого «устав» бізнес-процес, під страхом звільнення й штрафу, загнаний у кут – заметає сліди, видаляючи або підробляючи журнали подій. Якщо не зібрати вчасно ці журнали, то бізнесу буде нанесена шкода у вигляді фінансових втрат і зіпсованої репутації. Зібрані вчасно й консолідовані в сховище журнали подій допоможуть вам прийняти правильне рішення за підсумками інциденту. Здійснити видалення даних (подій і інцидентів) з SIEM непомітно не вийде: залишаються записи в системному журналі, здійснюється контроль цілісності. Докази у вигляді журналів подій в SIEM-системах допоможуть вашої організації в рішенні судових питань.

Хто знає, що це за скрипт?

Безумовно, можна побудувати керування журналами і яке-ніяке керування подіями на «самописних» сценаріях. Журнали збирати через syslog або відкрите ПЗ. Можна все оформити на PowerShell, «батники», sh-сценарії, а про інциденти повідомляти на електронну пошту. Як зручно й дешево!

Так, це прийнятно для малого бізнесу. Повернемося до нашого приклада з літаком. Заберемо подумки всі індикатори із приладової панелі (або зітремо їхньої назви), а повідомлення про неполадки будемо направляти пілотові по СМС і на електронну пошту…Як швидко пілотові набридне лазить у кишеню за телефоном і розбирати вхідні листи?

SIEM-системи мають функцію самодіагностики й контролю роботи компонентів. Це не розкидані отут і там «батники», цілісність і працездатність яких дуже важко проконтролювати. При використанні розрізнених сценаріїв практично неможливо буде захиститися від підміни вмісту або перегляду адміністративного облікового запису в незашифрованому виді. На відміну від SIEM: це комплексна система, що повідомляє про безперервність збору подій, про збої в роботі своїх компонентів, про доступ до системних функцій і т.п.

Захищайте не тільки критичні активи

Представимо, що ви захистили критичні (на вашу думку) активи, наприклад бізнес-додаток або базу даних. Все добре, грошей витрачено в міру, заощадили на відсутності СЗІ для робочих станцій і двофакторної авторизації для мобільних користувачів. Користувачів «затисли» груповими політиками. От тільки не врахували, що двері із замком, що коштує посередині поля, – абсолютно неефективна. Зловмисники одержать користувальницький і адміністративний аккаунт із незахищених робочих станцій або з мобільних пристроїв і з абсолютно легітимними запитами до вашої суперзахищеної бази даних «витягнуть» усе, що тільки можна. Деструктивні дії давно не в моді. Ви довідаєтеся про витік інформації з новин – і зачудуєтеся: адже всі ваші сервери були надійно захищені! Це приклад типової атаки по моделі APT. Запущені процеси, нові бібліотеки в ОС, нові сервіси, відкриті порти й

з'єднання, підвищення привілеїв – все це можна побачити в журналах подій на робочих станціях, які не були, на вашу думку, критичними активами…

Захист повинна бути комплексним. Доказ тому – інциденти з Bit9 і RSA, які чомусь не поставили розроблювальний ними захист на свої ж робочі станції.

Подання

Засоби захисту, як правило, є сигнатурними, тобто створюються на основі аналізу вже відомих погроз (віруси, мережеві атаки, навіть словники в DLP). Нові погрози ви можете виявити тільки із застосуванням складних алгоритмів кореляції, на основі мільйонів подій і показників, а також аналізу baseline. Людський мозок не завжди здатний комплексно проаналізувати такий обсяг даних. Однак абстракція подань в SIEM-системах сприяє своєчасному виявленню погроз операторами. Система робить всі попередні розрахунки й виводить показники. Як мінімум, приміром, на основі аналізу baseline система повідомляє про новий DynDNS-трафік, про те, що зафіксовано по 10 безуспішних спроб входу з різних активів від імені доменного адміністратора. Як правило, система здатна повідомити про троян або брутфорс (залежно від складу правил кореляції й можливостей конкретної системи). Застосування більше складних алгоритмів кореляції дозволить довідатися причину інциденту (наприклад, виявити підключення користувачем модему, у результаті якого відбулося зараження трояном і брутфорс). Людині не під силу самостійно здійснювати такий аналіз на підставі мільйонів текстових подій. Можливість налаштовування панелей візуалізації корисна як окремим співробітникам, так і для роботи SOC (security operation center), а також підрозділів IT і техпідтримки.

Відповідність (compliance)

У ряді регіональних, міжнародних, національних, галузевих стандартів є вимоги до організації процесу керування журналами. Всі SIEM-системи мають шаблони, що відповідають міжнародним стандартам, і можливість додавання своїх шаблонів для формування звіту про відповідність до збору й зберіганню подій. У випадку із саморобною системою вам доведеться витратити значні ресурси, щоб зробити подібні шаблони у форматі звітів або інтерфейсу для аудитора.

Акценти

Невірне реагування на інциденти порівнянно з некоректним поводженням світлофора. ІБ- і IT-підрозділи будуть нездатні вирішувати першочергові завдання по забезпеченню бізнес-процесів. SIEM має мінімально необхідні засоби організації процесу реєстрації інцидентів (або має можливість інтеграції зі службою підтримки), що сприяє контролю рішення інцидентів і нагромадження бази знань. В SIEM є можливість інтеграції й пріоритезації інцидентів залежно від їхнього впливу на бізнес-процеси, від цінності активу й небезпеки погрози. У деяких системах можлива інтеграція із системами керування ризиками.

Існує помилкова думка, що SIEM плодить велику кількість інцидентів, на які підрозділ ІБ попросту не встигає реагувати. Необхідно розуміти, що SIEM – це не рішення «з коробки» і, як і у випадку з DLP-системами, тут необхідно правильне впровадження, інтеграція із джерелами подій, індивідуальний підхід до активного набору правил і алгоритмам кореляції. Гнучка система виключень і правильне налаштовування SIEM гарантують вам акцент тільки на критично важливих подіях – без флуда.

Поділитеся подіями

SIEM – це система не тільки для ІБ. Помилки й збої в операційних системах, мережевому встаткуванні, ПЗ – інформацію про усе це співробітники IT-відділу можуть почерпнути в SIEM. IT-відділу також хочеться дізнаватися про виникаючі інциденти не по дзвінку користувачів, а заздалегідь (тим більше, що – як і інциденти ІБ – IT-інциденти можна запобігти).

SIEM – не занадто просте рішення для процесу керування журналами, до того ж досить дороге для впровадження в малому й середньому бізнесі. Для його експлуатації вам необхідно мати як мінімум одного кваліфікованого співробітника, що буде забезпечувати

контроль безперервності збору подій, управляти правилами кореляції, коректувати й обновляти їх з появою нових погроз і відповідно до змін в інфраструктурі. Установка SIEM у якості «чорного ящика» з активацією всіх передвстановлених правил кореляції без належного контролю й керування приведе до розтрати бюджету.

При успішному впровадженні ви одержите:

кореляцію й оцінку впливу IT- і ІБ-подій і процесів на бізнес;

SOC з аналізом ситуації в інфраструктурі в режимі реального часу;

автоматизацію процесів виявлення погроз і аномалій;

автоматизацію процесів реєстрації й контролю інцидентів;

аудит політик і стандартів відповідності, контроль і звітність;

задокументоване коректне реагування на виникаючі погрози ІБ і IT у режимі реального часу із пріоритезацією залежно від впливу погроз на бізнес-процеси;

можливість розслідування інцидентів і аномалій, у тому числі ті, що відбулись давно;

доказову базу для судових розглядів;

звітність і показники (KPI, ROI, керування подіями, керування уразливостями).

Я навів лише деякі приклади того, як SIEM допоможе вашому бізнесу в забезпеченні безперервності, підвищенні оперативності, у рішенні проблем і інцидентів.

Розробка структурної схеми

Давайте подивимося, із чого структурно складається SIEM. Як видно, для SIEM характерно більше число джерел і вони одержали можливість реагувати на «позаштатні» ситуації: наприклад, якщо в користувача раптово помінялася активність (раніше просто переглядав сторінки, використовуючи HTTP, а зараз починає активно ганяти трафік «назовні» через інші протоколи, наприклад) – те це привід згенерувати «подію». Крім цього, SIEM здатні аналізувати минаючий у мережі трафік без використання додаткового «заліза» або ПЗ (шляхом перекладу вільної мережевої карти сервера SIEM в «нерозбірливий» режим роботи), відслідковувати активність застосунків – і це крім основної функції, що залишилася, «збір логів із джерел» і «аналіз подій». Також SIEM можуть відслідковувати й віртуальні інфраструктури.

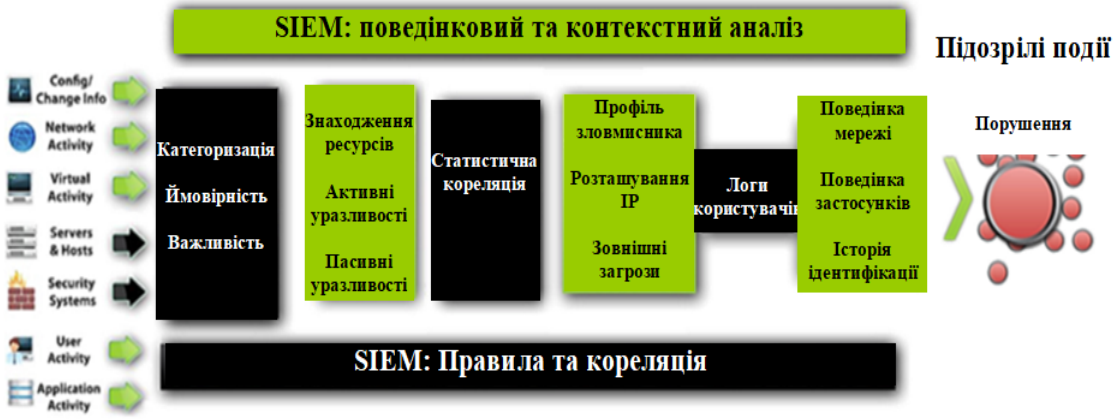


Рисунок 1 – Структурна схема системи

Та й сам аналіз став більше інтелектуальним – число «злочинів», що вимагають розгляди фахівцем, при використанні SIEM зменшується десь на 25-30%, це досягається за рахунок того, що вже накопичено якусь статистику рутинних операцій, установлюється якийсь поріг спрацьовування для «нетипових» операцій (скажемо, користувач user1 звичайно займається редагуванням і відправленням документів по smtp, але якщо він для відправлення раптом стане використовувати інший протокол – та подія, що вимагає уваги, буде згенеровано не відразу, а тільки при подоланні деякого порога частоти (або кількості) таких подій. Зрозуміло, ураховуються дані мережевої активності й т.д.).

Але! Багато менеджерів затверджують, що якщо у вас є SIEM %siem_name%, те немає необхідності установки DLP, IDS, сканерів уразливостей і т.д. Насправді, це не так. SIEM може відстежити якісь аномалії в мережевому потоці, але нормальний аналіз вона провести не зможе. SIEM, власне кажучи, марна без інших систем безпеки. Основна перевага SIEM – збір, зберігання й аналіз логів – буде зменшено на 0 без джерел цих самих логів.

Часта фраза в листівках «SIEM %siem_name% – легкість і швидкість впровадження, мінімум помилкових спрацьовувань, не вимагає переналаштовування вже наявних засобів безпеки...». Це не так. Можна, звичайно, обійтися мінімумом переналаштовувань – просто перенаправляти весь потік подій із пристроїв і систем безпеки на SIEM. На правильно налаштованій SIEM це не викличе значного збільшення числа помилкових спрацьовувань, але серйозно навантажить сервер БД (і викличе розростання БД). Що в підсумку виллється в збільшенні часу обслуговування БД і, можливо, до пропуску якихось дійсно важливих інцидентів безпеки. Тому, подумати – що ж саме відправляти на SIEM із уже наявних пристроїв, а що залишити на відкуп уже наявної системи безпеки – прийде. Приклад – можна перенаправляти всі логи антивірусу, установленого на ПК користувача, безпосередньо на SIEM – включаючи події про відновлення баз – але потрібно чи це вам? Особливо якщо врахувати, що деякі джерела можуть генерувати однотипні або повторювані події. Звичайно, в SIEM у більшості випадків передбачена можливість їхнього об'єднання, але це знову-же викликає зайві навантаження на сервер SIEM.

Варто особливо звернути увагу на можливість збирати flow-потоки (NetFlow, sFlow і т.д.) – корисна річ для відсічення зайвої інформації про трафік в мережі й, у той же час, одержання додаткової корисної інформації про стан мережі, отриманої безпосередньо з мережевих пристроїв.

Також як не буває легкого впровадження. Перед запуском потрібно провести масу аналітичної роботи, визначити, які події важливі, які немає й т.д.

В остаточному підсумку – питання – кому потрібні системи такого класу? Потрібні ці системи, на погляд автора, тим, у кого більша мережева інфраструктура й хто хоче хоч якось упорядкувати події й бути в курсі інцидентів. Але при цьому готовий до більших витрат, окупність таких систем не моментальна, користь, на перший погляд, не очевидна. До того ж, дані системи вимогливі до «заліза». Хоча, була в одній листівці вдала фраза: «SIEM дозволяє CIO пояснити проблеми IT мовою бізнесу». До того ж, дані системи вимогливі до «заліза».

Фраза не позбавлена підстав: звіти, створювані сучасними SIEM, мало того, що в різних форматах, так ще й, що налаштовуються під потреби конкретної організації, найчастіше дозволяють одержати всі необхідні дані на двох-трьох аркушах формату А4, представлені у вигляді зрозумілих і наочних графіків або цифр.

На закінчення, хочеться підбити підсумок: SIEM (або продуктів, що називають себе такими) – багато. Але, оскільки по кишені вони в основному лише великим замовникам – вони будуть звертати увагу на лідерів.

У світлі цього, не зовсім ясно, які перспективи в опенсорсних SIEM-систем, на мій погляд, це не той продукт, що легко можна замінити опенсорсним без ризику втрати переваг у вигляді регулярних відновлень і кваліфікованої підтримки. З іншого боку, існує позитивний приклад OpenBSD.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Досліджена система кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Розроблені алгоритми дозволяють успішно вирішувати завдання кібербезпеки для аудиту безпеки на базі технології Security Information & Event Management. Проведено аналіз предметної галузі в ході якого

були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Метод обнаружения вредоносного программного обеспечения. Часть 1. Корреляционный анализ сетевого трафика // А.А.Смирнов, Д.А. Даниленко, Е.В.Мелешко // Науково-технічний журнал «Інформаційно-керуючі системи на залізничному транспорті» – Випуск 4(95). – Х.: УкрДАЗТ – 2012. – С. 8-14.
2. Смирнов А.А. Методы обнаружения вредоносного программного обеспечения в телекоммуникационных системах и сетях / Д.А. Даниленко // Збірник наукових праць "Системи обробки інформації". – Випуск 3(101) том 2. – Х.: ХУПС – 2012. – С. 152-155.
3. Смирнов А.А. Системы обнаружения и предотвращения вторжений для защиты телекоммуникационных сетей от вредоносного программного обеспечения / Д.А. Даниленко, А.А. Смирнов, А.В. Коваленко // Системи управління, навігації та зв'язку. – Випуск 1 (21) том 2. – Київ: ДП «ЦНДІНУ». – 2012. – С. 183-186.
4. Смирнов А.А. Системы обнаружения и предотвращения вторжений для защиты компьютерных сетей от вредоносного программного обеспечения / Д.А. Даниленко, А.А. Смирнов, И.Г. Кирилов // Збірник тез доповідей науково-практичної конференції «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку». м. Харків. 21-22 березня 2012 р. – Харків. АВВ МВС. – 2012. – С. 70-71.
5. Смірнов О.А. Дослідження методів виявлення вторгнень в телекомунікаційні мережі для підвищення інформаційної безпеки // Д.О. Даниленко // Збірник тез науково-практичної конференції «Захист інформації в інформаційно-комунікаційних системах». м. Київ. 24-27 квітня 2012 р. – Київ: НАУ. – 2012. – С. 22-25.
6. Смирнов А.А. Исследование систем обнаружения и предотвращения вторжений для защиты телекоммуникационных сетей от вредоносного программного обеспечения / Д.А. Даниленко // Збірник тез доповідей VIII наукової конференції «Новітні технології – для захисту повітряного простору». Харків. 18-19 квітня 2012 р. – м. Харків. ХУПС. – 2012. – С. 45.
7. Смирнов А.А. Исследование методов сигнатурного обнаружения вредоносного программного обеспечения в телекоммуникационных системах и сетях // Д.А. Даниленко // Збірник тез XIII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 13-14 квітня 2012 р. – Кіровоград: КНТУ. – 2012. – С. 43-45.
8. Смирнов А.А. Исследование методов проактивной защиты от вредоносного программного обеспечения в телекоммуникационных системах и сетях / Д.А. Даниленко // Збірник тез V міжнародної науково-практичної конференції «інтегровані інтелектуальні робототехнічні комплекси» (ІПРТК-2012). м. Київ. 15-16 травня 2012 р. – Київ: НАУ. – 2012. – С. 314-315.
9. Смирнов А.А. Метод обнаружения вредоносного программного обеспечения на основе корреляционного анализа сетевого трафика / Д.А. Даниленко // Матеріали XII всеукраїнської наукової інтернет-конференції «Наукові дослідження: зв'язок теорії і практики». м. Тернопіль. 29-30 квітня 2012 р. – Тернопіль: ТНЕУ. – 2012. – С. 9-10.
10. Смирнов А.А. Метод детектирования вредоносного трафика в телекоммуникационных сетях на основе использования bds-тестирования / Д.А. Даниленко // Збірник тез V міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2012). м. Київ. 13-15 червня 2012 р. – Київ: НАУ. – 2012. – С. 121.

УДК 004

В. Хлистун, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ПРОГРАМНО ВИЗНАЧАЄМОГО ЦОД НА БАЗІ ТЕХНОЛОГІЙ FUJITSU

У статті розроблено програмне забезпечення, яке призначено для системи програмно визначаємого ЦОД на базі технологій Fujitsu. Метою розробки є дослідження та програмна реалізація системи програмно визначаємого ЦОД на базі технологій Fujitsu. Об'єктом дослідження є процес програмно визначаємого ЦОД на базі технологій Fujitsu. Предметом дослідження є методи програмно визначаємого ЦОД на базі технологій Fujitsu. Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи програмно визначаємого ЦОД на базі технологій Fujitsu. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, програмно визначаємий ЦОД, Fujitsu

Постановка проблеми. Цифрова трансформація робить весь зростаючий вплив на бізнес і суспільство. При цьому самі інформаційні технології змушені мінятися прискореними темпами, щоб не відстати від прогресу. Одне із ключових змін в IT виражається в тому, що, програмне забезпечення змінює світ. За останнє десятиліття цей процес зайшов досить далеко, але за легкою доступністю застосунків і сервісів ховаються невидимі для більшості змін в інфраструктурі.

Майбутнє ЦОД – за гібридними рішеннями. Хмари прийшли, щоб залишитися. Fujitsu не збирається конкурувати з мегапровайдерами хмарних послуг, такими як Amazon, Google, Microsoft, які надають доступні послуги в необмежених обсягах.

Сервіси з оплатою в міру використання корисні для деяких областей IT. В Fujitsu є подібна глобальна хмарна система з оплатою за використання за назвою Fujitsu Cloud Service K5, але вона орієнтована на азіатські ринки. Вона присутня на європейському й американському ринку, але скоріше допомагає нам надавати власні рішення, чим конкурує із продуктами вищезгаданих компаній.

Fujitsu фокусується на гібридних рішеннях. Fujitsu є постачальниками Azure Stack і VMware Cloud Foundation, в Fujitsu також є власна версія всіх необхідних механізмів керування, за допомогою яких ЦОД із традиційною формою володіння – як корпоративні, так і орендовані – можуть взаємодіяти із хмарними сервісами.

Однак нікому більше не цікава інфраструктура, оскільки ключовим фактором є мобільність застосунків. Замовники виходять із того, що необхідна інфраструктура вже є (хоча якщо її ні, у вас великі проблеми). Вони хочуть говорити не про інфраструктуру, а про застосунки й мобільність рішень.

Як показує аналіз ринку, навантаження вертаються із хмар назад у корпоративні ЦОД – і це характерно як для американського, так і для європейського ринку. Це викликано побоюваннями щодо інформаційної безпеки, незадоволеністю часом відгуку й, як це не здасться дивним, високими витратами. Нерідке розгортання гіперконвергентної інфраструктури на площадці замовника виявляється вигідніше. Таким чином, є цілий ряд стимулів, щоб залишити деякі рішення в традиційних ЦОД.

У випадку, коли ключове значення має мобільність застосунків, типовою моделлю є розробка в хмарі, по завершенні якої застосунок вертається на площадку замовника й там же виконується протягом усього свого життєвого циклу. Це пов'язане з тим, що ціна розробки не настільки критична, як сам ЦОД, продуктивність і наступні витрати.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи програмно визначаємого ЦОД на базі технологій Fujitsu

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи програмно визначаємого ЦОД на базі технологій Fujitsu.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

Огляд існуючих систем програмно визначаємого ЦОД на базі технологій Fujitsu.

Дослідження системи програмно визначаємого ЦОД на базі технологій Fujitsu.

Програмна реалізація системи програмно визначаємого ЦОД на базі технологій Fujitsu.

Об’єктом дослідження є процес програмно визначаємого ЦОД на базі технологій Fujitsu.

Предметом дослідження є методи програмно визначаємого ЦОД на базі технологій Fujitsu.

Методи дослідження базуються на методах теорії комп’ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Останні три-чотири роки спостерігався відхід від модульної (blade) серверної архітектури – партнери Fujitsu партнери її вже практично не використовують. Причина цього – високі витрати на ввод-вивід. У випадку блейд-серверів висока обчислювальна потужність концентрувалася в невеликому обсязі, платою за це було дороге ввод-вивід. Під платою я маю на увазі не фунти або рублі, а високі накладні витрати на ввод-вивід, оскільки все компоненти було потрібно з'єднувати між собою.

На даний момент тенденцією є перехід на горизонтально масштабовані архітектури, стимулом до чого служить розвиток мережних технологій і високопродуктивних технологій. Вони будуть розвиватися доти, поки їм на зміну не прийде модель із загальною пам'яттю, про яку Fujitsu говорили вище, – ефективна розподілена модель когерентної пам'яті з фізично роздільними блоками.

До недавніх часів продуктивність підсистеми зберігання мала ключове значення при проектуванні рішення, однак незабаром це буде вже не так. Восени цього року Intel продемонструвала пам'ять Apache Pass (Optane DIMM), і вже в наступному році почнуться її масові поставки. Критичний для продуктивності ввод-вивід буде здійснюватися за допомогою шини між процесором і пам'яттю, так що це (продуктивність СЗД) не буде мати значення. Підсистеми зберігання будуть служити для забезпечення безпеки даних, зовнішньої реплікації, переміщення й міграції даних і т.п., тоді як основні ресурси зберігання, ключові для роботи застосунків, будуть перебувати усередині сервера.

Із цієї причини ніхто з великих гравців більше не інвестує в розробку більше швидких жорстких дисків, оскільки в них немає потреби – усе буде робитися в NVRAM. Наявні диски цілком здатні справлятися з тим, що від них потрібно, – захист, реплікація, міграція. До слова, розмови про смерть магнітної стрічки йдуть стільки, скільки я себе пам'ятаю. Однак, на мій погляд, для перерахованих завдань стрічка релевантна настільки ж, як і диски. Тому для них погроза навіть більше, ніж для стрічки, хоча, звичайно, і ті й інші буде ще застосовуватися якийсь час, але навряд чи Fujitsu побачимо нове покоління 3, 5-дюймових дисків зі швидкістю обертання 22K RPM і більше високою щільністю запису.

Навіть такі виробники, як Toshiba і Seagate, інвестують у твердотільні накопичувачі. Однак і SSD – лише проміжне рішення між зовнішнім зберіганням і пам'яттю усередині сервера.

Загалом кажучи, в Fujitsu є власні мережні продукти, однак вони продаються в основному в Азії. У Європі й Північній Америці Cisco займає пануюче положення на ринку, так що Fujitsu їх там не просуває. Хоча в Fujitsu і є мережні компоненти, ринкова частка Fujitsu не настільки велика й лінійка мережного устаткування не настільки відома, щоб мало сенс витрачати сили на конкуренцію з визнаними вендорами. Однак традиційні мережні рішення поступово будуть витіснятися програмно-визначаємими, так що згодом цей сегмент стане усе менш і менш прибутковим.

В Fujitsu трохи інший підхід до ринку, ніж у великих американських компаній. Крім мережного устаткування, в Fujitsu є багато продуктів, які пропонуються тільки на японському ринку (або переважно японському ринку), такі як мобільні телефони, телекомунікаційні продукти й навіть мейнфрейми. Американської ж компанії пропонують за рубежем усе, що в них є в прайс-листі.

В Fujitsu є гіперконвергентні рішення, причому не одне, а цілих чотири:

Azure Stack.

VMware VCF, де використовується програмний стек VMware ESX.

Nutanix на апаратній платформі Fujitsu.

Рішення Fujitsu на базі Open Stack Ubuntu Linux.

Де яке варто використовувати, залежить винятково від вимог замовника.

Azure Stack переважніше, якщо замовник уже використовує Azure, але не навпаки. VCF вигідно для тих, у кого вже є корпоративні ліцензії VMware, але надмірно дорого для тих, у кого їх немає. Власне рішення Fujitsu підійде тим, хто робить ставку на рішення з відкритим вихідним кодом. Для всіх інших – Nutanix.

Замовники не хочуть більше говорити про те, як їм надавати інфраструктуру. Вони припускають її наявність як щось саме собою що розуміє. Вони виходять із того, що, маючи справу з такою компанією, як Fujitsu, HPE або будь-яким іншим великим вендором комплексних рішень, вони не повинні ні про що турбуватися й можуть зосередитися на питаннях бізнесу.

Засоби керування інфраструктурою центрів обробки даних (Data Center Infrastructure Management; DCIM) призначені для віддаленого моніторингу використання ресурсів ЦОД, стану навколишнього середовища, переміщення активів і інших параметрів, а також для регулювання окремих компонентів інфраструктури дата-центра: від вентиляторів усередині серверів до системи безпеки.

Програмне забезпечення з категорії DCIM також дозволяє генерувати звіти, спрощує планування потужностей і розподіл ресурсів, так само як і забезпечити максимально ефективне використання електроенергії, устаткування й площі.

Останнім часом усе більше широке поширення знаходить більше сучасна варіація на тему DCIM. Мова йде про рішення з категорії DMaaS (Datacenter Management as a Service або Керування дата-центром як послуга). Що таке DMaaS? Це хмарний сервіс, заснований на програмному забезпеченні DCIM.

Але це не просто версія програмного забезпечення DCIM, випущена з використанням бізнес-моделі SaaS. Концепція DMaaS виводить процес збору й обробки даних про інфраструктуру ЦОД на якісно новий рівень: дані про устаткування й пристрої збираються з безлічі центрів обробки даних, а потім – поєднуються й аналізуються.

Деякі розроблювачі програмного забезпечення також додають у свої DMaaS-рішення підтримку анонімного збору даних, що надходять із серверних ферм різних клієнтів . Такий підхід необхідний для виявлення трендів і виробітку корисних рекомендацій на основі результатів вивчення дійсно більших наборів даних.

Саме ця особливість DMaaS, на думку експертів, може потенційно трансформувати керування дата-центрами – особливо якщо можливості DMaaS-рішень у цій області будуть розширені за рахунок технології машинного навчання.

Ключовим завданням у даному контексті є застосування штучного інтелекту з метою прогнозування й запобігання інцидентів і збоїв інфраструктури дата-центрів, а також виявлення неефективності при використанні ресурсів і/або недостачі потужностей.

Два перших гравці на ринку DMaaS – Schneider Electric і Eaton. Обоє виробника одержали безліч даних із клієнтських ЦОД завдяки своєму багаторічному досвіду роботи в індустрії дата-центрів, включаючи проектування й створення модульних ЦОД і допоміжного устаткування для дата-центрів, систем розподілу електроенергії й охолодження.

Доступ до даних такого роду, що надходять від широкого кола клієнтів з різноманітними ЦОД, являє собою реальну цінність для DMaaS-рішень, які дозволяють операторам ЦОД порівнювати інфраструктуру своїх дата-центрів з погляду ефективності із глобальними контрольними показниками.

Наприклад, DMaaS-рішення EcoStruxure IT від Schneider Electric, містить контрольні показники, отримані за підсумками аналізу вихідної інформації з дата-центрів більш ніж 500 клієнтів і 2,2 млн датчиків.

Чим більше даних буде збиратися із центрів обробки даних різних типів для статистичного аналізу з використанням комбінації машинного навчання, виявлення аномалій і відтворення потоків подій, тим більше «розумними» будуть ставати DMaaS-рішення.

Наявність великих наборів даних про продуктивність конкретного устаткування в певних середовищах (при певній температурі, вологості, тиску повітря й так далі) може дозволити постачальникам DMaaS-рішень із більшою точністю прогнозувати, наприклад, ризики збоїти устаткування.

З обліком того, що простої дата-центрів шкодять підприємствам, що володіє ними, як у фінансовому, так і в репутаційному плані, легко зрозуміти передумови для зростаючої привабливості інструментів з категорії DMaaS, які можуть забезпечити мінімізацію даунтаймів і багато інших коштовних переваг.

На думку експертів, DCIM-рішення будуть програвати в конкурентній війні проти DMaaS, оскільки останні простіше розгорнути й використовувати. До того ж нові продукти забезпечують додаткові переваги. Але це лише думки. Реальні тренди будуть визначати оператори ЦОД, «голосуючи гаманцем».

Ринок програмного забезпечення для керування інфраструктурою центрів обробки даних (Data Center Infrastructure Management; DCIM) продовжує активно формуватися. Але сама концепція вже цілком оформилася з погляду визначення й очікувань клієнтів в області функціональності програмного забезпечення. Аналітики відзначають, що на даному етапі усе ще спостерігається деяка плутанина: усе більше розроблювачів ПЗ починають додавати в назви своїх продуктів акронім «DCIM», у той час як у дійсності ці рішення не здатні справлятися з усіма завданнями, які по полечу «сьогоденню» комплекту ПЗ DCIM.

Незалежне дослідницьке агентство Enterprise Management Associates (EMA) недавно опублікувала звіт про ринок DCIM, визначивши базовий понятійний апарат, якому варто використовувати під час обговорення DCIM-рішень, а також представивши список постачальників подібного ПЗ. EMA визначає комплект ПЗ DCIM як рішення, що «дає цілісне подання про IT-екосистемі й динамічно оцінює взаємозв'язку між конкретним пристроєм і всіма іншими». Це означає, що якщо в оператора ЦОД є система керування енергопостачанням, то він використовує не DCIM-рішення, а спеціалізоване програмне забезпечення трохи іншого плану. Якщо вендор називає свій продукт для моніторингу якості навколишнього середовища «DCIM-рішенням», то він уводить клієнта в оману.

До числа самих прогресивних і успішних вендорів експерти EMA віднесли Emerson, iTRACS, Cormant, FieldView, Nlyte, Raritan і Modius. Аналітики назвали продукти ще трьох компаній «справжніми» DCIM-рішеннями, але не включили їх у доповідь, тому що виникли проблеми з одержанням інформації від цих вендорів при підготовці документа до публікації. Мова про наступні компанії: CA, IBM і Schneider Electric.

У доповіді проаналізована архітектура кожного рішення, а також легкість його інтеграції в систему, функціональність, швидкість розгортання й зручність адміністрування,

цінова привабливість і впливовість вендора (популярність бренда). Аналітики також зрівняли різні продукти на основі цих критеріїв. Кращим було назване рішення Trellis, постачальником якого виступає компанія Emerson Network Power. Експерти Enterprise Management Associates назвали цей продукт найбільш комплексним, а також найпривабливішим у плані співвідношення « ціна-якість». Вони відзначили широкі можливості Trellis в області підтримки візуалізації й відображення інформації в реальному часі, а також удалий механізм інтеграції з усіма провідними технологічними платформами.

Тим менш, щоб одержати більше повну картину, у даній роботі проаналізували представників деяких вендорів зі списку EMA, щоб довідатися, скільки вони просять за свої рішення, і в якому напрямку вони розвивають свої технології.

Ціна DCIM

Цілком природно, що першою справою клієнт звертає увагу на ціну. Вартість комплектів ПЗ, а також те, як постачальники визначали її, були одними із ключових критеріїв при порівняльному аналізі різних вендорів експертами Enterprise Management Associates. Коли ви розробляєте програмне рішення, що підключається майже до всіх пристроїв у будинку, визначення вартості дуже швидко може стати вкрай складним і заплутаним процесом. Фахівці EMA рекомендують вендорам уникати цього шляхом розробки простих для розуміння клієнтів і простих з погляду проведених розрахунків моделей ціноутворення для DCIM-рішень.

Цінник на всі продукти, які вивчали аналітики Enterprise Management Associates, виставлявся на основі числа «кінцевих вузлів», з якими програмне забезпечення обмінюється інформацією, будь то стійкі з мережним устаткуванням, сервери або інші пристрої. Як правило, вендори розраховують експлуатаційні витрати як відсоток від загальної вартості ліцензії, при цьому деякі виробники пропонують клієнтам бонуси, такі як безкоштовне технічне обслуговування протягом року.

Тепер пройдемося безпосередньо по окремим вендорам. Так, компанії Raritan клієнт платить певну суму за кожну стойку, що обслуговується, с IT-устаткуванням у машзалі дата-центру. Вартість обслуговування стійки залежить від складності рішення, що постачальникові необхідно розгорнути в даті-центрі. Якщо рішення має багато компонентів, є більшим і складним, то воно, цілком очікувано, буде більше дорогим. Ще одним фактором є площа розгортання (кількість що обслуговуються машзалів). У цьому випадку клієнти виграють від ефекту масштабу. За словами представника компанії, розгортання DCIM-рішення Raritan на 100 серверних шаф (включаючи один рік обслуговування програмного забезпечення) буде коштувати біля $ 49 тис.

Компанія iTRACS (недавно була придбана CommScope) вибрала аналогічний підхід до ціноутворення, тобто гроші із клієнтів вона також бере за обслуговуються елементи, що, інфраструктури. Але у випадку iTRACS усе не обмежується серверними стійками – ціна може калькулюватися також виходячи із числа кондиціонерів, що обслуговуються, (CRAC), блоків розподілу електроживлення (PDU) і інших IT- і інфраструктурних активів, які розміщаються в дата-центрі. Розмір оплати у всіх випадках той самий, незалежно від типу активу. Тут також є знижки при збільшенні сукупного розміру обслуговується системи, що.

Подібна модель ціноутворення функціонує дуже добре, тому клієнти швидко розуміють механізм її роботи. Складності в області ціноутворення, з якими зштовхнулися інші постачальники, обернулися з розвитку ринку DCIM-рішень. Раніше були рішення, ціна яких визначалася на основі потужності об'єкта або елементів інфраструктури ЦОД, а також площі машзалів, що привело до плутанини на ринку.

Набагато легше взяти масив активів, підключити до системи й визначити вартість відповідно до їх кількості. Немає даних щодо середнього розміру оплати, що iTRACS бере за обслуговуються активи, що, але є дані, що ця цифра «значно менше» $ 1000 з розрахунку на стійку.

Компанія Cormant перейшла на більш деталізований підхід до ціноутворення, якщо порівнювати з iTRACS і Raritan. Фахівці Cormant при визначенні вартості свого DCIM-

рішення ґрунтуються на кількості реальних пристроїв, які вони також називають «активам». Джерело безперебійного живлення (ДБЖ) або систем кондиціювання повітря отут як і раніше вважається окремими активами, але серверна шафа тепер розділена на складові: один сервер або окремий мережний комутатор у випадку Cormant являють собою готельні активи.

Застосовувана компанією цінова модель краще або гірше, ніж підходи конкурентів: Зрештою, це просто трохи інша модель ціноутворення. Ключовою перевагою моделі Cormant є те, що вона дозволяє клієнтові розраховувати на більшу гнучкість, якщо його серверні стійки слабко й нерівномірно заповнені IT-устаткуванням.

Розміщення DCIM-рішення від Cormant у дата-центрі на 100 стійок при повній їхній комплектації обійдеться в $ 18 тис. Платіж разовий. У вартість не входить техпідтримка, за яку прийдеться платити окремо щороку. Техпідтримка є необов'язковою, але більшість клієнтів за неї платять.

Ще один вендор, компанія Nlyte, пропонує два варіанти оплати свого програмного забезпечення DCIM: разова оплата або підписка. Більшість компаній вибирають варіант разової оплати. Ціноутворення отут також походить із розрахунку на стійку (ціна перебуває в районі $ 1000 за стійку).

Функціонал DCIM-рішення

Відповідно до методики EMA, «сьогодення» DCIM-рішення повинне автоматизувати, як мінімум, три основні функції:

– збір даних;

– моделювання інфраструктури;

– створення аналітичної звітності.

Збір інформації, у даному контексті, означає створення централізованого сховища всіх даних, що надходять із пристроїв, і постійний моніторинг кожного з них, а також моніторинг таких речей, як споживання енергії, температура, вологість і повітряні потоки. Програмне забезпечення використовує ці дані, щоб створити цифрову модель інфраструктури, що обновляється в міру зміни інфраструктурних елементів. В ідеалі вона (модель) представлена в зручному графічному форматі. Вона є ключовим елементом DCIM-рішення, тому що відображає взаємозв'язку між пристроями усередині інфраструктури. Аналітична підсистема займається інтерпретацією даних, які збирає DCIM-рішення, дозволяючи знайти проблеми або визначити причини неефективності.

Сама по собі концепція DCIM є досить новою, тому автоматизація в кожній із цих областей продовжує розвиватися. Всі вендори зі списку EMA постійно додають нові функції у свої продукти, і ці доповнення, як правило, стосуються саме тих трьох областей автоматизації, які виділили експерти Enterprise Management Associates. Вендори розширюють можливості своїх рішень всілякими способами: розвивають безпосередньо функціонал, збільшують ступінь інтеграції своїх продуктів з іншими рішеннями або поглинають конкурентів і використовую їхні наробітки.

Поліпшення DCIM-рішень

З останніх нововведень можна відзначити наступне. Компанія Nlyte зайнялася розширенням можливостей свого програмного забезпечення в області 3D-моделювання й моніторингу електроживлення в режимі реального часу, моніторингу енергоефективності й збору даних з датчиків умов навколишнього середовища. Компанія також купила ліцензію на повноцінний движок для бізнес-аналітики, що тепер дозволяє ПЗ генерувати найрізноманітніші звіти для потреб операторів. Велика бібліотека дозволяє зробити звіти гранично зрозумілим для різнопланових фахівців, що діють у рамках організації – від операторів ЦОД до фінансових менеджерів.

Ще одна нова доробка дозволяє програмному забезпеченню Nlyte самостійно пропонувати операторові ЦОД найбільш підходяще місце для розміщення додаткових елементів інфраструктури (наприклад, нового сервера). Компанія розробила цю технологію без сторонньої допомоги й успішно неї запатентувала, а тепер пропонує іншим вендорам купити ліцензію – бажаючих поки немає.

У майбутніх релізах фахівці Nlyte планують зосередитися на підвищенні якості моделювання. На цей момент вендор випустив уже шосту версію свого програмного забезпечення. Компанія Nlyte працює на ринку DCIM біля семи років.

Рішення Cormant були доступні на ринку вже більше восьми років, хоча раніше продукти компанії з лінійки CableSolve і не позиціонувалися як DCIM. Вендор перемінив назву свого продукту з CableSolve на Cormant на початку 2013 року.

Недавно відбувся реліз сьомої версії цього комплекту програмного забезпечення. Компанія готовить нову версію практично щороку або півтора, а також допрацьовує функціональність за допомогою проміжних релізів, які попадають на ринок у кожному кварталі. З останніх доповнень можна відзначити перехід від стандартного застосунки на веб-сервіс, що, на думку аналітиків, стало більшим кроком уперед. Крім того, зовсім недавно Cormant додала у свій продукт повноцінну підтримку планшетів і смартфонів, а також додаткові можливості в області візуалізації. Найближчим часом фахівці Cormant хочуть збільшити прогнозно-аналітичну функціональність свого продукту.

В iTRACS недавно з'явилася функція інтелектуального керування доступним простором. Крім того, компанія розширює інтеграцію свого DCIM-рішення із продуктами інших вендорів. Це дозволяє одержати нові джерела даних, за допомогою яких і здійснюється моделювання. До числа цих вендорів відносяться Intel (Data Center Manager), Power Assure і RF Code. З метою сприяння такої інтеграції iTRACS створила платформу DCIM Open Exchange Framework, що чимсь нагадує інтерфейс прикладного програмування (API). Ця платформа дозволяє продуктам сторонніх компаній підключатися до рішення iTRACS для двонаправленного обміну інформацією.

У випадку компанії Raritan, що звичайно щорічно додає по парі нових функцій з нагоди релізу чергової версії свого DCIM-рішення, технологічний розвиток зосереджений на двох речах: автоматизація й спрощення продукту для кінцевих користувачів. Недавно компанія поліпшила API для свого веб-сервісу – тепер у її програмне забезпечення можна інтегрувати більше рішень сторонніх виробників. Крім того, з'явилися спеціальні звіти й діаграми по керуванню енергоспоживанням, за допомогою яких клієнти можуть легко знайти гарячі точки в машзалі. Ще одним важливим нововведенням є диспетчер підключень, що обчислює рівень силовий навантаження в кожній точці ланцюга електроживлення.

Автоматизації на фізичному рівні

Технологія автоматизації всього дата-центра нам поки ще недоступна, але вже зараз у даній роботі можемо спостерігати усе більше активне використання робототехніки й інтелектуальних апаратних рішень у середовищі ЦОД. Роботизовані маніпулятори вже контролюють величезні стрічкові бібліотеки в дата-центрах Google (ці пристрої можуть завантажувати й вивантажувати стрічкові накопичувачі в міру необхідності). При цьому дискусії із приводу концепції автоматизації ЦОД за допомогою робототехніки ведуть фахівці й інших великих інтернет-компаній, а також постачальників устаткування для дата-центрів. Крім того, активно розвиваються й конвергентні обчислювальні системи начебто Cisco UCS, за допомогою яких оператори ЦОД уже зараз можуть створювати потужні моделі адаптації інфраструктури відповідно до потреб поточних і нових користувачів.

Концепції « Lights-Out» у ЦОД

Робота дата-центра за принципом «Lights-Out» припускає керування IT- і допоміжною інфраструктурою в умовах відсутності фізичного доступу до цих ресурсів). Недавно цією концепцією стали цікавитися великі вендори. Приміром, компанія Panduit анонсувала новий набір послуг Industrial Automation Advisory Services, які покликані зблизити IT-фахівців і інженерів з метою підвищення ефективності підключення, керування й автоматизації промислових мереж і систем керування. В офіційному прес-релізі вендора сказано, що «для збереження конкурентоспроможності сучасним промисловим організаціям доводиться збільшувати обсяги виробництва й знижувати витрати при збереженні якості й безпеки... З урахуванням стрімкої конвергенції мереж створення адекватної фізичної інфраструктури, а

також механізмів керування нею в режимі реального часу, моніторингу, збір даних і конфігурування пристроїв починають грати ще більш важливу роль».

Для повноти картини відзначимо, що згідно із прогнозом Gartner Research, у період з 2020 по 2022 роки 80 відсотків даунтаймів критично важливих ЦОД будуть викликані горезвісним «людським фактором» і прорахунками при створенні робочих процесів. При цьому більше 50 відсотків із цих відключень дата-центрів будуть викликані проблемами при зміні / конфігуруванні / інтегруванні елементів IT- і допоміжної інфраструктури. Нова ініціатива Panduit саме-таки покликана звести ризик даунтайма внаслідок перерахованих вище інцидентів до нуля. Фахівці вендора досконально вивчають поточний стан фізичного й віртуального середовища в ЦОД клієнта й розробляють рекомендацій з оптимізації в області підвищення ефективності й автоматизації.

Автоматизація на логічному рівні

Можливості віртуалізації, хмарних обчислень і сучасного ЦОД безупинно переплітаються, що дає кінцевим користувачам нові можливості й інструменти. Автоматизація пов'язаних із цим переплетенням робочих процесів на логічному рівні має вирішальне значення. Чому? Тільки так можна динамічно контролювати приплив користувачів і підбудовувати під нього обчислювальні потужності, а також вчасно адаптувати інфраструктуру під нові типи хмарного контента й механізми взаємодії кінцевих користувачів і ЦОД.

Платформи начебто Citrix Provisioning Services або Unidesk значно спрощують розгортання віртуалізованих десктопів / застосунків і контроль над ними. Інші платформи начебто CloudPlatform, OpenStack і Eucalyptus допомагають домогтися більше глибокої логічної автоматизації, спрощуючи оркестровку хмарних платформ. З їхньою допомогою організації можуть контролювати окремі хости, кластери, різні зони й навіть основні ресурси віртуальних машин. Не будемо забувати й про системи автоматизації IT-процесів і керування конфігураціями, які пропонує Puppet Labs і ряд інших компаній. Ці рішення дозволяють адміністраторам створювати єдиний підхід до автоматизації. З таким набором інструментів IT-фахівець може управляти повністю гетерогенною інфраструктурою. Подібний інструментарій дозволяє одночасно й досить ефективно контролювати такі платформи як VMware, Amazon EC2, Juniper Networks, Google Compute Engine і навіть системи класу “bare metal”. Крім того, дані інструменти дозволяють організаціям застосовувати просунуті політики безпеки й дотримувати нормативних вимог.

Роль і перспективи роботів в автоматизації ЦОД

Пошуковий гігант Google із завидною швидкістю скуповує виробників робототехніки. Це факт. За останні шість місяців Google купила 8 компаній, що займаються проектуванням і виробництвом роботів. Мова про Boston Dynamics (саме свіже придбання американців), Autofuss, Bot & Dolly, Schaft, Industrial Perception, Meka, Redwood Robotics і Holomni. Чому пошуковий гігант скуповує виробників робототехніки? Ніхто не знає напевно (за виключення, мабуть, керівництва компанії), але Google давно славиться підвищеною увагою до оптимізації й підвищення ефективності своїх дата-центрів. Використання роботів у ЦОД відкриває величезні можливості для автоматизації. Логічно припустити, що інженери інтернет-компанії вже затурбувалися адаптацією технологій куплених стартапів для дата-центрів. Не відстає від конкурента й Amazon: на складах інтернет-ритейлера вже зараз трудяться майже півтори тисячі роботів Kiva Systems (Amazon купила цю компанію наприкінці 2012 року за $ 775 млн.), які ніколи не зіштовхуються один з одним і нічого не роняють. Цілком можливо, що інженери компанії вже створюють щось подібне для її ЦОД.

Очевидно, що робототехніка ще не швидко зможе замінити людей усередині дата-центрів. Але завдяки появі нових і подальшому розвитку існуючих технологій (наприклад, силовимірювальних систем і систем машинного зору, RFID і т.д.) вони усе краще підходять для автоматизації повторюваного / рутинної людської праці, підвищуючи продуктивність IT-фахівців. При цьому нові технології дозволяють роботам підбудовуватися під мінливе навколишнє середовище, а не покладатися повною мірою на складену раніше модель

оточення. За прикладами далеко ходити не потрібно – у даній роботі розповідали про подібні системи протягом усього року. Нижче ви можете виявити інформацію про пару свіжих проектів:

– Роботизований пристрій для ЦОД уже представили інженери IBM. Фахівці "блакитного гіганта" скористалися технологічною базою компанії iRobot для створення роботизованої платформи моніторингу навколишнього середовища. Їхній утвір може переміщатися усередині машзалів без втручання з боку. Після того, як машина попадає в машзал ЦОД, вона спочатку знаходить стіну, а потім починає переміщатися по периметрі приміщення, постійно вимірюючи рівень температури й вологості. В остаточному підсумку пристрій створює теплову карту всього внутрішнього простору. Дані в режимі реального часу передаються в репозиторій спеціалізованого комплекту програмного забезпечення IBM. На їхній основі створюються комплексні звіти про тепловий режим ЦОД і рівні вологості усередині машзалів.

– Напрочуд схожий девайс за назвою DC Robot (або Data Center Robot) розробили інженери індійського підрозділу транснаціональної корпорації EMC. Завдяки бортовими камерами й роботизованою платформі для досліджень iRobot Create, що складається з надійного й недорогого мобільного шасі й ряду датчиків, DC Robot здатний вільно переміщатися по машзалам. Робот допомагає операторам ЦОД контролювати температуру, вологість і вібрації в машзалах дати-центра. Пристрій збирає дані з використанням трьох цифрових датчиків, а потім передає цю інформацію через Wi-Fi на будь-який сумісний термінал для подальшої обробки. Спеціалізоване програмне забезпечення EMC перетворить дані в теплову карту, що, у свою чергу, допомагає операторам ЦОД визначити області, де температурний режим повинен бути скоректований у ту або іншу сторону.

На думку експертів, у найближчі роки роботи будуть усе більш активно трудитися разом з людьми. Примітно, що зовсім недавно Американський національний інститут стандартизації (American National Standards Institute; ANSI) переглянув свій стандарт на системи безпеки промислових об'єктів, зм'якшивши вимоги до організації спільної роботи машин і людей. Принципово новий моментом є те, що укладачі стандарту вже не заперечують проти того, щоб роботи й люди трудилися в буквальному значенні бік-об-бік, тоді як раніше машини рекомендувалося поміщати під спеціальні огородження, при цьому люди не повинні були до них наближатися, коли роботи виконували поставлені завдання в автоматичному режимі. Устаткування для забезпечення безпеки піддалося істотному вдосконаленню з моменту останнього перегляду стандарту ANSI, і тепер роботи можуть збирати більше інформації про їхнє оточення, чим коли-або колись.

Подивимося правді в очі, Є деякі речі, які люди завжди будуть робити краще, ніж роботи. Але якщо в даній роботі зможемо розробити процеси, що дозволяють роботові взяти на себе 90% навантаження, не травмуючи при цьому людини-оператора ЦОД, коли той робить все інше, ці пристрою почнуть із величезною швидкістю з'являтися у всіх дата-центрах.

Автоматизація в майбутньому

Згідно з даними зі свіжої доповіді Cisco Cloud Index Report, «річний обсяг минаючі через дата-центри глобального IP-трафіку досягне колосальних 7.7 зеттабайта до кінця 2020 року, при цьому глобальний трафік ЦОД досягне 644 екзабайт на місяць (в 2015 році середньомісячний показник досягав лише 214 екзабайт). У доповіді також говориться, що «до 2021 року на частку хмарних платформ буде доводитися 69 відсотків сукупного минаючого через ЦОД трафіку... Розширення хмарних ЦОД буде стимулювати розвиток технологій і автоматизації, а також стандартизацію цих і суміжних технологій. Це приведе до збільшення продуктивності хмарних дата-центрів, а також до росту ємності СЗД і пропускної здатності мережної інфраструктури».

Майбутнє автоматизації дата-центрів і оркестровки припускає ще більш тісну інтеграцію між логічним і фізичним рівнем. Апаратура усередині ЦОД зможе ще більш продуктивно взаємодіяти з IT-Навантаженнями, які з її допомогою обробляються. Крім того,

робототехніка й інші технології автоматизації допоможуть усунути або мінімізувати проблеми, пов'язані з відключеннями ЦОД, масштабуванням обчислювальної інфраструктури й керуванням ЦОД у цілому. Дата-Центри продовжать розвиватися й еволюціонувати, точно також будуть розвиватися й всі технології, які допомагають підтримувати їхню працездатність.

Робототехніка вже використовується на складах, у промисловому виробництві, у фармації й багатьох інших сегментах. Інтенсифікація впровадження технологій автоматизація й використання робототехніки для забезпечення нормального функціонування дата-центрів – усього лише справа часу. Уже зараз у даній роботі спостерігаємо створення великих розподілених ЦОД, появі й розвитку яких сприяє ріст пропускної здатності мережної інфраструктури. Багато компаній останнім часом усе активніше розміщають елементи своїх розподілених серверних ферм у північних країнах начебто Ісландії, де є швидкий інтернет, дешева й екологична електрика з ГеоЕС і можливість створення високоефективних систем природного охолодження серверів (фрикулінг).

Можливість обробки великого обсягу трафіку в таких ЦОД змушує керівників організації з, приміром, південній частині Європи або Азії всерйоз розглядати можливість створення нового об'єкта або оренди вже існуючого ЦОД у регіоні зі сприятливим кліматом і розвитий телекомунікаційною інфраструктурою – нехай і розташованому на відстані багатьох тисяч кілометрів. Ці дата-центри буде рости, оскільки усе більше користувачів будуть використовувати сервери, що перебувають у їхніх стінах, і СЗД. При цьому процеси їхнього моніторингу й контролю необхідно буде змінити: традиційні підходи у випадку гіпермасштабних ЦОД банально втрачають свою ефективність.

Розробка структурної схеми

Безліч протоколів і застосунків беруть участь у забезпеченні безперебійної роботи центра обробки даних: SSL, HTTP, балансувальники навантаження, черги проміжного програмного забезпечення, бази даних і протоколи зберігання. Продуктивність, обмірювана на вхідних дверях, буде характеризувати загальне обслуговування, але для ізоляції проблем потрібна видимість всього ланцюга. Перебої в роботі або відключення критично важливих застосунків можуть вплинути на продуктивність центра обробки даних.

Моніторинг ЦОД і керування стало основою нашої економіки. У результаті робота й захист Центра обробки даних мають вирішальне значення. Для надійного й безпечного моніторингу ЦОД прозорість має першорядне значення. Це саме те, що забезпечує програмне забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu своїм інтегрованим і уніфікованим підходом до моніторингу й керування IT-інфраструктурою, що розуміє наскрізні операційні процеси.

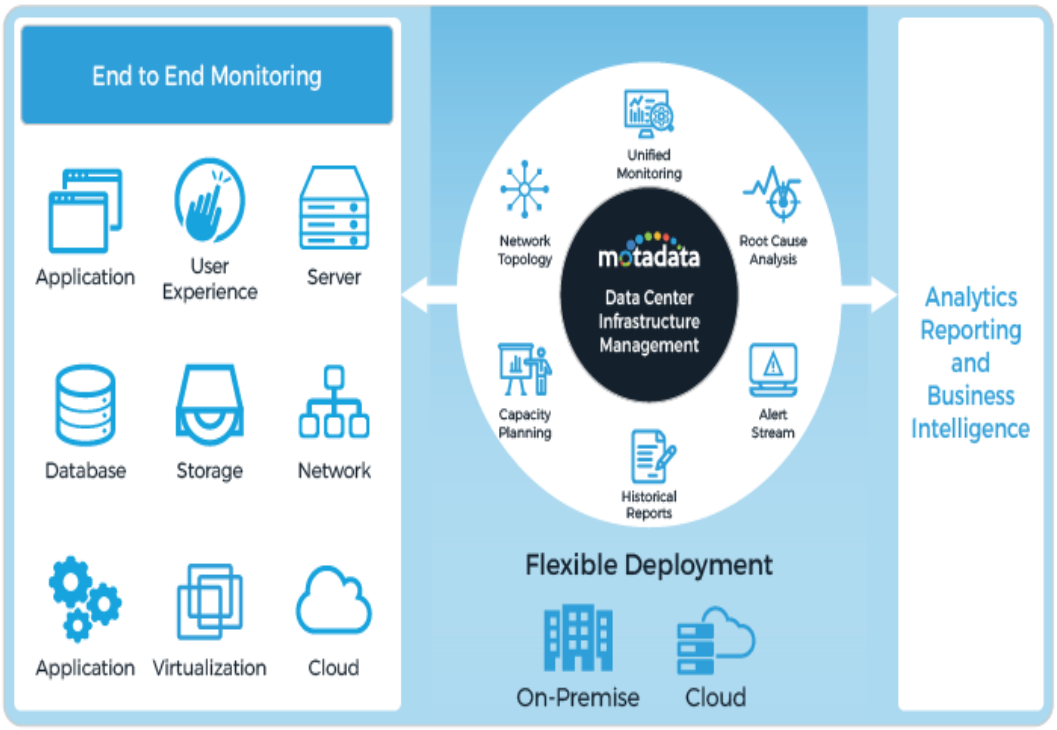


Рисунок 1 – Структурна схема системи

Моніторинг і оптимізація центрів обробки даних у фізичних, віртуальних і хмарних середовищах

Універсальне рішення, без схованих витрат і надбудов

Досвід єдиного моніторингу з непередбаченою простотою. За допомогою програмного забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu ви можете одночасно управляти IT-інфраструктурою, середовищем центра обробки даних і критично важливими бізнес-додатками й контролювати їх у рамках однієї консолі, що налаштовується, або панелі моніторингу. Моніторинг продуктивності ЦОД включає синергизм продуктивності застосунків, продуктивності фізичних і віртуальних серверів і достатню пропускну здатність, що іноді може бути проблематичним. Проблема виникає щораз, коли існують розрізнені інструменти моніторингу. Програмне забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu вирішує всі проблеми керування ЦОД за допомогою єдиного рішення.

Будьте проактивно доступності & уникайте простоїв

Контролюйте свій центр обробки даних у режимі реального часу, залишіть всі свої турботи про вузькі місця, коливання або використання смуги пропущення. Усе, що вам потрібно зробити – це встановити граничні значення, і потужний механізм оповіщення програмне забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu буде попереджати вас щораз, коли щось працює не так, як очікувалося. Завдяки сторонній інтеграції програмне забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu з додатками для спільної роботи, такими як SMS, електронна пошта й т. Д., Можна уникнути незвичайних простоїв. Виявлення, виявлення, аналіз і усунення неполадок у мережі за допомогою попереджень, що попереджають, і усунення неполадок. Розуміти тенденції, моделі й поводження, щоб приймати більше обґрунтовані рішення.

Платформа росте в міру росту

Продуктивність і доступність ЦОД важливі для будь-якої організації. Через технологічний розвиток складність і розмір інфраструктури центра обробки даних продовжують рости, і у випадку невдачі підприємства страдають. Програмне забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu має відкриту архітектуру, і

платформа готова до майбутнього. Платформа може бути масштабована відповідно до вимог, а також може відслідковувати поширення розподіленого середовища в різних місцях.

Моніторинг продуктивності в режимі реального часу

Забезпечте 24×7 моніторинг всіх ваших пристроїв і ефективно використовуйте ресурси в інфраструктурі ЦОД з моніторингом продуктивності й доступності в режимі реального часу. Стежите за тим, як ваша інфраструктура працює в режимі реального часу, і запобігайте дорогим збоям. Програмне забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu – «Мережа / доступ / постачальник», має можливості моніторингу на основі агентів і без агентів. Одержати повну видимість у цілому продуктивність мережі центрів обробки даних з більш ніж визначеними звітами 100.

Заощаджувати час доступності & ресурси

Щораз, коли користувачі повідомляють про повільний доступ до якого-небудь застосунки, основною причиною може бути несправність сервера, вичерпання смуги пропущення або неприступність самого застосунки. Щоб з'ясувати точну причину, IT-командам доводиться шукати на декількох моніторах і інформаційних панелях від вузьких місць пропускної здатності до сервера або застосунку. У цьому підході відсутня кореляція між даними, наданими декількома різнорідними інструментами моніторингу. На той час, коли ви зберете інформацію з даних і вистежите першопричину, застосунок уже буде закрито. Отже, аналіз кореневих причин програмне забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu вступає в гру. Знайдіть основну причину проблеми одним клацанням миші, як на багатофункціональній платформі, вона може корелювати дані метрики, потоку й журналу й видає коррелюванні метрики.

Ключові моменти

Вимір, моніторинг, керування й контроль ресурсів центра обробки даних і енергоспоживання компонентів інфраструктури об'єкта (наприклад, блоку розподілу живлення) і пристроїв IT-інфраструктури (наприклад, серверів, комутаторів і т. Д.)

Наскрізна видимість

Вимір, моніторинг, керування й контроль ресурсів ЦОД як компонентів інфраструктури об'єкта (наприклад, блоку розподілу живлення), так і пристроїв IT-інфраструктури (наприклад, серверів, комутаторів) і т. д.

Приймайте більше обґрунтованих рішень

Одержите повну прозорість всієї інфраструктури інфраструктури центра обробки даних, що дозволяє IT-адміністраторам приймати більше обґрунтовані рішення на основі важелів поліпшення роботи.

Масштаб як вам потрібно

Рішення готове до майбутнього й масштабовано. Центри обробки даних постійно ростуть, як і потреби моніторингу. Дані можуть масштабуватися й рости з вашим успіхом.

Корелювати дані

Нездатність розпізнати взаємодія або взаємозалежність різних елементів може привести до незапланованих відключень. Переконаєтеся, що ви запобігаєте це за допомогою механізму кореляції програмного забезпечення системи програмно визначаємого ЦОД на базі технологій Fujitsu.

Автоматизувати процеси

Різко зменшити складність і людські помилки. Краще використовувати робочу силу за допомогою автоматизованого рішення для моніторингу й керування ЦОД.

Смарт усунення неполадок

Знайдіть і усунете основну причину проблеми в один клік, перш ніж вона вплине на ваших кінцевих користувачів. Активізуйте дії по усуненню неполадок.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів програмно визначаємого ЦОД на базі технологій Fujitsu. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем програмно визначаємого ЦОД на базі технологій Fujitsu. Досліджена система

програмно визначаємого ЦОД на базі технологій Fujitsu. На основі отриманих результатів досліджень створена програмна реалізація системи програмно визначаємого ЦОД на базі технологій Fujitsu. Розроблені алгоритми дозволяють успішно вирішувати завдання програмно визначаємого ЦОД на базі технологій Fujitsu. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Разработка методики оценки среднего времени обслуживания информационных пакетов в телекоммуникационной сети / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
2. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
3. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011. – 193-195 с.
4. Современные телекоммуникации. Технологии и экономика / [В.Л. Банкет, О.В. Бондаренко, П.П. Воробьенко и др.]; под ред. С.А. Довгого. – М.: Эко-Трендз, 2003. – 320 с.
5. Столлингс В. Современные компьютерные сети / Вильям Столлингс.– СПб.: Питер, 2003. – 778 с.
6. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – М.: Техносфера, 2004. – 368 с.
7. Таненбаум Э. Компьютерные сети / Эндрю Таненбаум; пер. с англ. А. Леонтьев. – СПб.: Питер, 2002. – 848 с.
8. Телекоммуникационные системы и сети: учебное пособие. В 3 томах / [В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев]; под ред. В.П. Шувалова. – М.: Горячая линия-Телеком, 2005, т. 3 – 592 с.
9. Уолрэнд Дж. Телекоммуникационные и компьютерные сети / Дж. Уолрэнд. – М.: Постмаркет, 2001. – 480 с.
10. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.:Вильямс, 2006. – 1103 с.

УДК 004

Б. Фролов, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ LEGRAND CABLING SYSTEM 3 ДЛЯ ЦОД

У статті розроблено програмне забезпечення, яке призначено для системи Legrand Cabling System 3 для ЦОД. Метою розробки є дослідження та програмна реалізація системи Legrand Cabling System 3 для ЦОД. Об'єктом дослідження є процес Legrand Cabling System 3 для ЦОД. Предметом дослідження є методи Legrand Cabling System 3 для ЦОД. Методи дослідження базуються на методах теорії побудови комп'ютерних систем та мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи Legrand Cabling System 3 для ЦОД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, Legrand Cabling System 3, ЦОД

Постановка проблеми. Legrand представила третє покоління своєї кабельної системи (Legrand Cabling System 3, LCS3) своїм українським партнерам. Нова, радикально оновлена

система, крім кабельних компонентів, включає шафи й PDU і розрахована на застосування як у локальних мережах, так і в ЦОД. Крім мідних і оптичних кабельних компонентів до складу системи ввійшли також серверні й телекомунікаційні шафи й розеточні блоки. За допомогою нової системи Legrand розраховує розширити свою присутність у центрах обробки даних.

LCS3 – усього лише третє покоління СКС за ті 35 років, які компанія працює на цьому ринку. Окремі компоненти (роз'єми RJ-45 і комутаційні панелі) компанія початку пропонувати ще в 1993 році, однак перша закінчена система з'явилася в неї лише десять років через, в 2003 році, а наступне друге покоління – в 2009 році. Нова, радикально оновлена система розрахована на більше широку область застосування, чим її попередниця – від малих офісів до ЦОД.

LCS3 покликана задовольнити потребу ринку в продуктивних, масштабованих і (економічно) ефективних рішеннях. Мідна кабельна підсистема LCS3 Категорії 8 може підтримувати швидкості до 40 Гбіт/с, а оптична – до 100 Гбіт/с. Полки високої щільності дозволяють заощадити місце в шафах і ефективно масштабувати рішення, а без інструментальне закладення коннекторів і інші інновації в дизайні компонентів спрощують експлуатацію й обслуговування.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи Legrand Cabling System 3 для ЦОД

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи Legrand Cabling System 3 для ЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

Огляд існуючих систем Legrand Cabling System 3 для ЦОД.

Дослідження системи Legrand Cabling System 3 для ЦОД.

Програмна реалізація системи Legrand Cabling System 3 для ЦОД.

Об'єктом дослідження є процес Legrand Cabling System 3 для ЦОД.

Предметом дослідження є методи Legrand Cabling System 3 для ЦОД.

Методи дослідження базуються на методах теорії побудови комп'ютерних систем та мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Організації стандартизації й базові стандарти СКС

Абревіатура СКС – структуровані кабельні системи – уже настільки поширена, що не вимагає пояснень для більшості користувачів персональних комп'ютерів. Під цим терміном розуміють телекомунікаційну інфраструктуру будівель або, інакше кажучи, середовище передачі будь-яких слабкострумових сигналів у межах (комплексу) житлових, офісних і промислових будівель.

Ця стандартизована основа локальних комп'ютерних і офісних телефонних мереж завойовує все більше визнання завдяки ряду переваг – універсальності, зручності експлуатації й надійності. Успіх даної технології залежить у чималому ступені від організацій, що розвивають, що впроваджують і використовують СКС, і, у тому числі, від організацій стандартизації.

Розробку загальновизнаних стандартів СКС ведуть у США, у Європейській і Міжнародній організаціях стандартизації.

США

У середині 80-х років ряд компаній, що представляють телекомунікаційну й комп'ютерну індустрію США, виступили з ініціативою розробки стандартів кабельної інфраструктури будівель. У рамках Асоціації електронної промисловості (EIA) було створено кілька робочих груп. Проект Інженерного комітету TR-41, одержав назву TR-41.8. Комітет заснував кілька робочих груп по наступних напрямках стандартизації:

TR-41.8.1 Робоча група кабельної проводки комерційних і промислових будівель.

TR-41.8.2 Робоча група кабельної проводки житлових будівель і малих офісів.

TR-41.8.3 Робоча група телекомунікаційних каналів і приміщень / Адміністрування.

TR-41.8.4 Робоча група магістралей житлових будівель і малих офісів.

TR-41.8.5 Робоча група визначень.

TR-41.7.2 Робоча група по заземленню й електричним з'єднанням.

TR-41.7.2 Робоча група по рекомендаціях електромагнітної сумісності.

Технічні комітети Асоціації електронної промисловості (EIA) і координаційні комітети Правління EIA розробляють стандарти спільно. Члени комітетів працюють добровільно без якої-небудь компенсації. Компанії, які вони представляють, не обов'язково є членами Асоціації. Таким чином, прийняті документи є результатом домовленості зацікавлених фахівців і відбивають їхній різнобічний досвід, у даній області, наявний до моменту твердження стандартів.

В 1998 році Сектор телекомунікацій Асоціації електронної промисловості був перетворений в Асоціацію телекомунікаційної промисловості (TIA), що підкоряється Технічній раді. Ставши незалежною організацією, Асоціація продовжує здійснювати діяльність по стандартизації разом з Асоціацією електронної промисловості (EIA). Ці організації представлені в назвах стандартів як ANSI / TIA / EIA.

ANSI / TIA / EIA переглядає більшість стандартів кожні п'ять років. У результаті стандарти можуть бути підтверджені, доповнені або змінені. Зміни, які передбачається внести, направляються Голові комітету або в секретаріат ANSI / TIA / EIA.

Міжнародні організації стандартизації

Міжнародна організація стандартизації (ISO) і Міжнародна електротехнічна комісія (IEC) утворять орган стандартизації, визнаний в усьому світі. Національні організації – члени ISO і IEC беруть участь у розробці стандартів у складі Технічних комітетів. Комітети, створені галузевими організаціями, взаємодіють один з одним у суміжних областях. У спільній роботі беруть участь інші міжнародні, урядові й неурядові організації.

Міжнародна організація стандартизації й Міжнародна електротехнічна комісія заснували Об'єднаний технічний комітет ISO / IEC JTC 1, що спеціалізується в області інформаційних технологій. Проекти міжнародного стандарту, схвалені Об'єднаним технічним комітетом, передаються в національні організації стандартизації для голосування. Для прийняття стандарту потрібно не менш 75% голосів.

Європейські організації стандартизації

Європейський комітет стандартизації електротехніки (CENELEC) діє регіонально в тісній координації з Міжнародною організацією стандартизації. Країни, що входять в CENELEC, приймають європейські стандарти в якості національних без яких-небудь виправлень. Європейські стандарти публікуються на трьох офіційних мовах – англійській, французькій й німецькій. Переклади на інші мови, зроблені членами CENELEC, і завірені в Центральному секретаріаті, одержують статус офіційних версій.

Базові стандарти СКС

Базовими стандартами структурованих кабельних систем є: ANSI / TIA / EIA-568-A. Стандарт телекомунікаційних кабельних систем комерційних будівель. Жовтень 1995 року; ISO / IEC 11801. Інформаційні технології. Структурована кабельна система для приміщень замовників. Липень 1995 року; EN 50173:1995. Інформаційні технології. Структуровані кабельні системи. Липень 1995 року.

Стандарти покликані служити суспільним інтересам, усуваючи непорозуміння між виробниками й споживачами, забезпечуючи взаємозамінність і універсальну якість продукції поряд з її доступністю й грамотним використанням. Стандарти телекомунікаційної інфраструктури будівель повинні забезпечити роботу різнотипного встаткування будь-яких виробників, створення кабельні системи на етапі будівництва будівель і їхню тривалу експлуатацію.

Стандарт ANSI / TIA / EIA-568-A замінив ANSI / TIA / EIA-568, що діяв з липня 1991 року. У нову редакцію ввійшли доповнення, прийняті у формі технічних бюлетенів: EIA / TIA TSB 36, TIA / EIA TSB 40 і TIA / EIA TSB 40a. Бюлетені містили параметри

категорій 3, 4 і 5 для кабелів типа незахищена кручена пари (UTP) і роз'ємів. У стандарт додані специфікації Проекту TSB 53 захищеної кабельної системи із хвильовим опором 150 ом, багатомодового оптоволокна 62,5 / 125 мкм, одномодового волокна, ОВ роз'ємів і обмежень для оптоволоконого середовища передачі. Системи категорії 1 і 2 виключені з даного стандарту.

Міжнародний стандарт ISO / IEC 1180 був підготовлений Підкомітетом 25 ISO / IEC JTC 1 "Підключення встаткування інформаційних технологій". Європейський стандарт EN 50173 був прийнятий Технічним комітетом 115 "Електротехнічні аспекти телекомунікаційного встаткування". На додаток до американського стандарту, що визначає як альтернативне середовище передачі захищені системи із хвильовим опором 150 ом (розробка IBM) визначені параметри незахищених чотирьохпарних систем із хвильовим опором 120 ом (розробка Alcatel). Характеристики універсальних 100-омних систем розрізняються незначно.

Базові міжнародні і європейські стандарти збігаються практично буквально. Однак ISO / IEC і CENELEC розробляють власні стандарти в суміжних областях. У Європі, наприклад, існує Директива EMC, визначені власні параметри екранованих і оптоволоконих кабелів. Міжнародна організація стандартизації веде розробку стандартів проектування, монтажу, адміністрування, вимірів і впровадження застосунків. Назви взаємозалежних діючих і розроблювальних стандартів приводяться в додатках до кожного документа.

Україна бере участь у роботі Міжнародної організації стандартизації (ISO), але не входить в CENELEC. Тому в даному огляді за основу взяті положення й термінологія міжнародних стандартів. У США діє ряд стандартів, які тільки розробляються в згаданих організаціях і широко застосовуються при створенні СКС у всіх країнах. Організації ISO / CENELEC використовують розробки ANSI / TIA / EIA як щабля для руху вперед. При цьому вони виправляють недоліки американських стандартів. В огляді наведені відмінності американських стандартів і відзначені виправлені недоліки.

Групи стандартів СКС

Організації стандартизації діють на міжнародному, регіональному й національному рівнях. Ініціатива розробки стандартів СКС належить США, які також лідирують у їхньому прийнятті. Ряд інших країн, наприклад, Канада, Німеччина, розробляють і використовують власні стандарти. Германія випереджає всіх у розробці й використанні нових категорій.

Стандарти Асоціації електронної й телекомунікаційної промисловості й Американського національного інституту стандартизації (ANSI) найбільше повно відбивають різні аспекти створення телекомунікаційної інфраструктури. Як видно з таблиці, наведеної нижче, міжнародні і європейські організації ще не опублікували свої варіанти стандартів, що діють у США з 1990 – 1995 року.

За змістом й областям застосування стандарти можна підрозділити на три групи – проектування, монтажу й експлуатації.

Стандарти проектування визначають середовище передачі, параметри роз'ємів, лінії й каналу, у тому числі гранично припустимі довжини, способи підключення провідників (послідовність), топологію й функціональні елементи СКС. Додатка доповнюють стандарти в суміжних областях і підрозділяються на нормативні (частина стандарту) і інформаційні (для відомості). До цієї групи можна віднести також документи, що визначають параметри заземлення, особливості СКС малих офісів і житлових будівель, централізованих систем і рекомендації з побудови відкритих офісів.

Стандарти монтажу визначають у широкому змісті телекомунікаційні аспекти проектування й будівництва (комплексу) будівель. Облік телекомунікаційної інфраструктури має на увазі наявність каналів для прокладки кабелів і приміщень для їхньої комутації й розміщення встаткування. У вузькому змісті під монтажем розуміють роботи з установки кабельних систем. Другий підхід є більше дорогим. У дану групу включені також стандарти вимірів, оскільки на практиці якість монтажу СКС визначається за допомогою вимірів, які можуть завершувати процес створення систем.

Стандарти адміністрування визначають правила документування телекомунікаційної інфраструктури й створюються на базі стандартів проектування й монтажу.

Назви й час прийняття перерахованих стандартів наведено нижче.

Міжнародні стандарти

ISO / IEC 11801 Інформаційні технології – структуровані кабельні системи для приміщень замовника.

ISO / IEC 11801A1 / A2 Інформаційні технології – структуровані кабельні системи для приміщень замовника; Додатки 1/2.

Європейські стандарти

EN 50173:1995 Інформаційні технології – структуровані кабельні системи (1995 рік).

EN 50173 / A1:2000 Інформаційні технології – структуровані кабельні системи (2000 рік):

1 березня 2000 року – оголошення на національному рівні.

1 вересня 2000 року – публікація національного стандарту, ідентичного європейському.

1 вересня 2000 року – скасування діючих положень національних стандартів, що не відповідають європейському.

30 жовтня 2000 – коментарі національних комітетів стандартизації

Підготовлено до публікації друге видання EN 50173, що замінить EN 50173:1995 і EN 50173 / A1:2000.

Стандарти США

ANSI / TIA / EIA-568-A Телекомунікаційні стандарти кабельних систем комерційних будівель, (жовтень 1995).

Доповнення:

ANSI / TIA / 568-A-1. Специфікації затримки й фазового зрушення для 100-омних 4-парних кабельних систем, 1997.

ANSI / TIA / 568-A-2. Виправлення й доповнення до ANSI / TIA / EIA-568-A,1998.

ANSI / TIA / 568-A-4. Виробнича методика вимірів NEXT сполучних кабелів і вимоги до кабелів незахищена кручена пари, 1999.

ANSI / TIA / 568-A-5 Специфікації параметрів передачі 4-парних 100-омних кабельних систем категорії 5e, 1999.

EIA / TIA-569 Стандарти прокладки телекомунікаційних каналів комерційних будівель (жовтень 1990).

EIA / TIA-570 Стандарт телекомунікаційних кабельних систем житлових і малих комерційних будівель (червень 1991).

TIA / EIA-606 Стандарт адміністрування телекомунікаційної інфраструктури комерційних будівель (лютий 1993).

TIA / EIA-607 Вимоги по заземленню й електричним з'єднанням телекомунікаційних систем комерційних будівель (серпень 1994).

TIA / EIA TSB 72 Посібник із централізованих оптоволоконим кабельним системам (жовтень 1995).

TIA / EIA TSB 75 Додаткові вимоги побудови горизонтальних кабельних систем відкритих офісів (серпень 1996).

ISO / IEC 11801. Стандарт телекомунікаційної інфраструктури комерційних будівель

Стандарти визначають структуру й параметри слабкострумових кабельних систем, установлюваних в одному, декількох або комплексі будівель.

Універсальна телекомунікаційна інфраструктура будівель призначена для передачі сигналів всіх типів, включаючи мовні, інформаційні й відео. Системи сигналізації, які встановлюють у сучасних будинках, не висвітлюються в стандартах СКС (згадуються в ANSI / TIA / EIA-568-A. Вимоги по безпеці (електричному, пожежному й іншому видам) і електромагнітної сумісності (EMC) визначаються іншими стандартами й нормативами. Положення базових стандартів СКС погодяться з нормами безпеки й EMC.

Стандарти забезпечують:

користувачів – структурованої (добре організованої) кабельною системою, що не залежить від типу застосунків, і відкритий ринок – елементами для створення таких систем;

користувачів – гнучкою схемою прокладки кабелів, що дозволяє легко й економічно виконувати модифікацію системи;

будівельників-професіоналів (наприклад, архітекторів) інструкціями, що дозволяють проектувати й будувати кабельні системи ще до того, як стануть відомими конкретної вимоги користувачів, що забезпечує планування будівництва й ремонту;

промисловість і організації стандартизації – кабельною системою, що забезпечує роботу наявного мережного встаткування й базу для розробки нових видів продукції.

Стандарти дозволяють створювати середовище передачі з елементів різних виробників завдяки взаємодії організацій стандартизації один з одним.

Стандарти США визначають два рівні вимог – обов'язковий і що рекомендується. Обов'язковий рівень виражається словом «повинен», що рекомендується – словами – «треба», «може», «бажано». Обов'язковий рівень задає мінімум характеристик і параметри сумісності. Рівень, що рекомендується, використовується для більше повної відповідності параметрів СКС вимогам застосунків і різних умов експлуатації. У тому випадку, якщо для одного параметра задаються два рівні, що рекомендується рівень задає більше високу якість систем і являє собою верхню планку при створенні нових СКС.

Міжнародні і європейські стандарти не визначають рівні вимог, однак використовують ті ж слова, що припускають їх. Обов'язкові й нормативи, що рекомендуються, як правило, не розрізняють. У даному огляді рівні вимог точно позначені . Крім того, обов'язкові нормативи виділені жирним шрифтом.

1. Масштаб

Найважливіші принципи СКС – універсальність і довговічність. Вони дозволяють будівельниками створювати системи перш, ніж стануть відомі вимоги користувачів, і забезпечити термін служби телекомунікаційної інфраструктури будівель до 10 років і більше. Системи оптимізовані для будівель з офісною площею до 1,000,000 м2, числа користувачів 50 – 50,000 чоловік і відстаней між будинками до 3 км. Принципи побудови СКС рекомендується використовувати також для систем, число користувачів і розмір яких виходять за зазначені рамки.

2. Нормативні посилання

Після вступної частини, відбитої вище, у стандартах приводяться перелік стандартів, що доповнюють даний стандарт, що діють на момент прийняття стандартів.

3. Визначення й скорочення

Визначення й скорочення необхідні для точного розуміння категорій, без чого неможливо однозначне тлумачення положень стандартів.

Положення, викладені в стандартах, підлягають змінам, що відбивають прогрес мережних і кабельних технологій і термінального встаткування.

4. Відповідність

Кабельна система будується у відповідності з визначеними у стандартах вимогам і рекомендаціями.

5. Структура СКС

Під структурою СКС розуміють модель побудови системи з функціональних елементів і підсистем. Даний розділ визначає також інтерфейси крапки для підключення термінального встаткування до структурованої системи й самої СКС – до мережі загального користування. Групи функціональних елементів утворять підсистеми СКС.

5.1. Функціональні елементи СКС

Структурована кабельна система – середовище передачі електромагнітних сигналів – складається з елементів – кабелів і роз'ємів. Кабелі, оснащені роз'ємами й прокладені за певними правилами, утворять лінії й магістралі. Лінії, магістралі, точки підключення й комутації становлять функціональні елементи СКС.

В американському стандарті до функціональних елементів відносять два типи кабелів, три типи приміщень, елемент конструкції будівлі й документацію телекомунікаційної інфраструктури. Крім того, у даних групах стандартів використовується різна термінологія. Міжнародні / європейські стандарти підрозділяють СКС на вісім функціональних елементів, американський – на сім. Тільки два з них збігаються. У першому випадку функціональні елементи становлять середовище передачі, тобто властиво структуровану кабельну систему. Це дозволяє виділити підсистеми й провести точні границі між ними.

У другому до складу функціональних елементів не ввійшла магістраль комплексу й всі інтерфейси СКС і додані приміщення, елементи будівель і система документування. Це приведе до плутанини й змішування понять у технічній літературі, проспектах виробників і документації, створюваних по американській моделі – А.В.

5.2. Підсистеми СКС

Міжнародні / європейські стандарти підрозділяють СКС на три підсистеми: магістральна підсистема комплексу, магістральна підсистема будівлі, горизонтальна підсистема.

Розподільні пункти забезпечують можливість створення топології каналів типу «шина», «зірка» або «кільце».

5.2.1. Магістральна підсистема комплексу включає магістральні кабелі комплексу, механічне закінчення кабелів (роз'єми) у розподільчому пункті (РП) комплексу й РП будинки й комутаційні з'єднання в РП комплексу. Магістральні кабелі комплексу також можуть з'єднувати між собою розподільні пункти будівель.

5.2.2. Магістральна підсистема будівлі включає магістральні кабелі будівлі, механічне закінчення кабелів (роз'єми) у РП будинки й РП поверху, а також комутаційні з'єднання в РП будинки. Магістральні кабелі будівлі не повинні мати крапок переходу, електропровідні кабелі не слід з'єднувати сплайсами.

5.2.3. Горизонтальна підсистема включає горизонтальні кабелі, механічне закінчення кабелів (роз'єми) у РП поверху, комутаційні з'єднання в РП поверху й телекомунікаційні роз'єми. У горизонтальних кабелях не допускається розривів. При необхідності допускається одна крапка переходу. Усі пари й волокна телекомунікаційного роз'єму повинні бути підключені. Телекомунікаційні роз'єми не є крапками адміністрування. Не допускається включення активних елементів і адаптерів до складу СКС.

Абонентські кабелі для підключення термінального встаткування не є стаціонарними й перебувають за рамками СКС. Однак, стандарти визначають параметри каналу, до складу якого входять абонентські й мережні кабелі.

5.3. Топологія СКС

Топологія СКС – «ієрархічна зірка», що допускає додаткові з'єднання розподільних пунктів одного рівня. Однак такі з'єднання не повинні заміняти магістралі основної топології. Число й тип підсистем залежить від розмірів комплексу або будинки й стратегії використання системи. Наприклад, у СКС один будинки досить одного РП будівлі й двох підсистем – горизонтальної й магістральної. З іншого боку, великий будинок можна розглядати як комплекс, що включає всі три підсистеми, і в тому числі, трохи РП будівлі.

5.4. Розміщення розподільних пунктів

Розподільні пункти розміщаються в телекомунікаційних приміщеннях і апаратних. Телекомунікаційні приміщення призначені для установки панелей і шаф, мережного й серверного встаткування, що обслуговують весь або частина поверху. Апаратні виділяють для телекомунікаційного встаткування, щообслуговує користувачів усього будівлі (наприклад, УАТМ, мультиплексори, сервери) і розміщення РП будівлі / комплексу. Панелі / шафи й устаткування РП поверху, сполучені із РП будівлі / комплексу, також можуть перебувати в приміщенні апаратної.

5.5. Інтерфейси СКС

Інтерфейси СКС це закінчення підсистем, що забезпечують підключення встаткування й кабелів зовнішніх служб методом підключення або комутації.

Для підключення до СКС досить одного мережного кабелю. У варіанті комутації використовують мережний і комутаційний кабель і додаткову панель.

Підключення до мережі загального користування здійснюється за допомогою інтерфейсу мережі загального користування. Місце розташування інтерфейсу мережі загального користування визначається національними, регіональними й місцевими правилами. Якщо інтерфейси мережі загального користування й СКС не з'єднані комутаційним кабелем або за допомогою встаткування, необхідно враховувати параметри проміжного кабелю.

5.6. Конфігурація

5.6.1. Розподільний пункт поверху

Як мінімум один РП поверху рекомендується на кожні 1000 квадратних метрів офісної площі. На кожному поверсі повинен бути, принаймні, один РП поверху. Якщо число робочих місць на поверсі невелико, його можна обслуговувати за допомогою розподільного пункту на суміжному поверсі.

5.6.2. Рекомендовані типи кабелів

У таблиці 1 дані рекомендації застосування різних типів середовища передачі в кожній з підсистем.

Таблиця 1 – Рекомендоване середовище передачі підсистем СКС

Підсистема	Тип середовища передачі	Застосунки
Горизонтальна підсистема	Симетричні кабелі	Мовні й інформаційні
	Оптоволоконі кабелі	Інформаційні
Магістральна підсистема будівлі	Симетричні кабелі	Мовні й інформаційні класів А й В
	Оптоволоконі кабелі	Інформаційні класів В й вище
Магістральна підсистема комплексу	Оптоволоконі кабелі	Для всіх застосунків
	Симетричні кабелі	Для застосунків класу А (наприклад, лінії УАТМ)

Дані рекомендації застаріли – інформаційні додатки класів А (до 0,1 МГц) і В (до 1,0 МГц) у локальних мережах практично не застосовуються. Вибір середовища передачі для магістралі будівлі залежить від також від довжини каналів. Якщо довжина магістральної лінії не перевищує 90 метрів, симетричні кабелі відповідної категорії покликані забезпечити роботу всіх діючих застосунків – А.В.

З іншого боку, більшість багатомодових кабелів непридатні для роботи Gigabit Ethernet при довжині лінії більше 220 метрів (у відповідності зі стандартами максимальна довжина ОВ ММ магістралі – 2000 метрів) – А.В.

5.6.3. Телекомунікаційні роз’єми (ТР)

Телекомунікаційні роз’єми розташовують на стіні, підлозі або в іншій крапці робочої області. При проектуванні СКС варто забезпечити зручність доступу до всіх роз’ємів. Висока щільність роз’ємів підвищує гнучкість системи й полегшує зміни телекомунікаційних ресурсів робочих місць. У багатьох країнах на 10 м2 використовуваній площі повинні установлюватися два телекомунікаційних роз’єми.

Допускається установка роз’ємів поодиноко або групами, однак кожне робоче місце повинне мати не менш двох роз’ємів.

На кожному робочому місці повинен бути передбачений, принаймні, одне роз’єми, установлений на симетричному кабелі 100 ом або 120 ом (перевага віддається кабелям 100 ом). Інші ТР потрібно встановлювати або на симетричним, або на оптоволоконом кабелі.

Симетричний кабель повинен мати дві або чотири пари; усе пари повинні бути змонтовані на роз’єми. Якщо передбачено менш чотирьох пар, це потрібно відбити в маркуванні. Застосунки збалансованої передачі можуть мати обмеження по затримці

поширення сигналів по кожній з пар. Особливості специфікації ТР, що відповідають перерахованим вище типам кабелів, дані в розділі «Вимоги до роз'ємів».

Роз'єми повинні бути позначені постійним маркуванням, видної користувачеві. Варто звертати увагу на те, щоб реєструвалося первісне призначення пар, а також всі наступні зміни. Хвильові й інші адаптери, використовувані для узгодження різних передавальних середовищ, повинні перебувати із зовнішньої сторони роз'єму. Дозволяється міняти призначення пар за допомогою адаптерів.

У українськомовній літературі поняття «телекомунікаційне роз'єми» повсюдно підмінюють терміном «телекомунікаційна розетка». Роз'єми або закінчення кабелю, є частиною розетки, тобто складання роз'ємів, настановної й фіксуючої арматур. Розетка може поєднувати від одного до дванадцяти роз'ємів – А.В.

5.6.4. Телекомунікаційні приміщення й апаратні

Телекомунікаційне приміщення покликане забезпечувати наявність всіх засобів (простір, електроживлення, обігрів, вентиляція) для розташованих усередині нього пасивних елементів, активних пристроїв, а також інтерфейсів мережі загального користування. Для кожного телекомунікаційного приміщення варто передбачити прямий доступ до магістралі будівлі.

Апаратна – простір у межах будівлі, де розміщається телекомунікаційне встаткування й можуть перебувати або бути відсутніми розподільні пункти. До апаратного висувають інші вимоги, чим до телекомунікаційних приміщень, оскільки встаткування, установлюване в них, є більше складним (наприклад, УАТМ або сервери). В апаратній може перебувати більше одного розподільного пункту. Якщо телекомунікаційне приміщення служить для розміщення двох і більше розподільних пунктів, його варто вважати апаратною.

Термін «телекомунікаційне приміщення» часто переводять як «телекомунікаційна шафа». Ці поняття не збігаються. Якщо використовується кілька шаф /стійок, неправильний переклад приводить до непорозумінь. Особливо серйозні помилки виникають при проектуванні системи заземлення й тлумаченні стандартів, що також використовують даний термін – А.В.

5.6.5. Пункт вводу в будинок

Пункти вводу в будинок обладнаються у випадку, коли зовнішні кабелі магістралі комплексу, приватних мереж і мережі загального користування (включаючи антену) уводять у будинок і здійснюють перехід на внутрішні кабелі. Місцеві правила можуть вимагати спеціального комутаційного устаткування для оснащення зовнішніх кабелів роз'ємами. Це встаткування дозволяє перейти від зовнішніх до внутрішніх кабелів.

5.7. Електромагнітна сумісність

Міжнародні стандарти електромагнітних випромінювань і стійкості (наприклад, CISPR 22) і місцеві правила повинні бути прийняті в увагу. Кабельна система вважається пасивної й не може бути протестована на відповідність вимогам ЕМС індивідуально. Активне встаткування повинне відповідати вимогам відповідних стандартів ЕМС із урахуванням використовуваного середовища передачі.

5.8. Заземлення

Елементи системи заземлення повинні відповідати вимогам відповідних норм і правил. Інструкції й вимоги виробників устаткування варто виконувати, якщо вони сумісні з електричними нормативами.

Важливо відзначити, що відповідальність за відповідність СКС вимогам електромагнітної сумісності делегована виробникам активного встаткування. Такий підхід не вирішує проблеми. Строго говорячи, пункти 5.7. Електромагнітна сумісність і 5.8. Заземлення не ставляться до конфігурації СКС і висвітлюються в розділі 10, спеціально присвяченому даним проблемам. Крім того, вони не містять норм і правил, а тільки посилання на інші стандарти – А.В.

1) Коли бажана більша гнучкість системи, варто використовувати чотирьохпарні кабелі.

2) Установка двопарних кабелів обмежує роботу застосунків класу D.

6. Підсистеми СКС

Дана глава визначає модель горизонтальної й магістральної підсистем, максимальну довжину, кращі й рекомендовані типи кабелів. Рекомендується відповідність цим вимогам для більшості встановлених систем.

Загальна довжина абонентських (A), комутаційних (B) і мережних кабелів (E), що утворять канал горизонтальної підсистеми, – до 10 метрів.

Довжина комутаційних кабелів у РП будинки (C) і РП комплексу (D) – не більше 20 метрів.

Довжина мережних кабелів у РП будинки (F) і РП комплексу (G) – не більше 30 метрів.

Дотримання зазначених довжин строго рекомендується, однак не є вимогою, оскільки абонентські й мережні кабелі перебувають за рамками міжнародного, європейського й американського стандартів.

Вимоги до елементів системи – кабелям і роз'ємим – визначається в розділах «Вимоги до кабелів» і «Вимоги до роз'ємів». Симетричні кабелі із хвильовим опором 100 і 120 ом і роз'єми для них підрозділяються по категоріях. Параметри передачі категорій 3, 4 і 5 визначені в смузі частот 16, 20 і 100 Мгц відповідно.

Кабелі й роз'єми різних категорій можуть бути встановлені в межах підсистеми й / або кабельної лінії, але передавальні робітники характеристики лінії будуть визначатися категорією гіршого елемента.

Елементи з різним хвильовим опором не допускається встановлювати в одній лінії. Оптичні волокна з різними діаметрами серцевини не дозволяється з'єднувати в межах однієї кабельної лінії. Багаторазова поява того самого провідника або провідників (шунтовані відводи), не може бути частиною кабельної системи.

6.1. Горизонтальна підсистема

6.1.1. Довжина кабелів.

Максимальна довжина горизонтального кабелю повинна становити 90 м, незалежно від типу середовища. Вона виміряється від роз'єми (панелі) у РП поверху до телекомунікаційного роз'єму на робочому місці. Максимальна механічна довжина абонентських, комутаційних (перемичок) і мережних кабелів – не більше 10 метрів.

Для відповідності вимогам застосунків настійно рекомендується використання абонентських і мережних кабелів, робочі характеристики яких відповідають або перевищують параметри комутаційних кабелів. Довжина комутаційних кабелів і перемичок у РП поверху не повинна перевищувати 5 м.

Показана модель горизонтальної підсистеми, що забезпечує узгодження параметрів кабелів («Вимоги до кабелів») і ліній («Специфікація ліній»). Для цього фіксований кабель горизонтальної лінії обмежений довжиною 90 метрів і гнучкий – довжиною 5 метрів (що еквівалентно сумарній електричній довжині 97,5 метрів), а лінія включає три роз'єми однакової категорії. Крапка переходу є резервною й відсутній у даній моделі. Якщо використовується крапка переходу, параметри лінії повинні відповідати моделі із двома роз'ємами й довжиною кабелю не більше 90 метрів.

Абонентський і мережний кабелі не входять до складу структурованої кабельної системи, однак дозволяють створити канал з параметрами, що задаються стандартами. Передбачається, що загальна електрична довжина мережного й абонентського кабелів еквівалентна 7,5 метрам (відповідно до умов «Вимоги до кабелів»). Різниця механічної й електричної довжини для гнучких кабелів обумовлена вимогами до загасання.

Відмінності ANSI / TIA / EIA-568-A

Довжина комутаційних кабелів (або перемичок) і мережних кабелів не повинна перевищувати 6 метрів. Передбачається, що довжина абонентського кабелю (від TP до робочої станції) становить 3 метри, а загальна довжина сполучних кабелів обмежена 10 метрами.

Обмеження на рівні обов'язкової вимоги довжини комутаційних кабелів дозволяє встановити параметри горизонтальної підсистеми СКС. Для організації каналу діє рекомендація із сумарної довжини всіх гнучких кабелів – до 10 метрів. Гнучкі або сполучні кабелі відрізняються типом роз'ємів (штекерні , на відміну від гніздових у фіксованих кабелів) і конструкцією провідників – кожний провідник складається із семи мідних жил – А.В.

В американську модель лінії виявився включеним мережний кабель, що відповідно до положень того ж стандарту не входить до складу СКС. Це одне із протиріч, якого немає в міжнародних і європейських стандартах – А.В..

Модель оптоволоконих горизонтальних кабелів відрізняється можливою наявністю сплайсів на обох кінцях підсистеми й відсутністю комутаційних кабелів.

Деякі технології, зокрема моніторинг з'єднань СКС за допомогою системи LAN Sense, мають на увазі створення каналів з комутацією також і для оптоволоконих горизонтальних підсистем – А.В.

1) Специфікації комутаційних і інших гнучких кабелів дані в «Вимоги до гнучких симетричних кабелів 100, 120 і 150 ом»

6.1.2. Вибір типу кабелю.

Для використання в горизонтальній кабельній підсистемі рекомендуються кабелі двох типів:

Кращі: симетричний кабель 100 ом і багатомодове оптичне волокно 62,5/125 мкм.

Альтернативні: симетричний кабель 120 ом, симетричний кабель 150 ом, кабелі із багатомодовим оптичним волокном 50 / 125 мкм.

Параметри кабелів, роз'ємів наведені в «Вимоги до кабелів» і «Вимоги до роз'ємів». Для підключення декількох телекомунікаційних роз'ємів можливе застосування гібридного й композиційного кабелів. Якщо є екрановані або заземлені провідники, варто керуватися положеннями розділу «Практика екранування».

Відмінності ANSI / TIA / EIA-568-A

1. Відсутні симетричний кабель 120 ом і кабелі із багатомодовим оптичним волокном 50 / 125 мкм.

2. Як середовище передачі зізнається коаксіальний кабель 50 ом. Однак він не рекомендований для монтажу в знову встановлюваних СКС і повинен бути виключений з наступної редакції стандарту. Інші типи середовища передачі, також не включені в стандарт і доповнення, що допускаються до використання в якості, до мінімальної конфігурації, – екрановані кабелі 100 ом, багатопарні кабелі й коаксіальні кабелі 75 ом.

6.1.3. Конфігурація телекомунікаційних роз'ємів.

Два телекомунікаційних роз'єми, що забезпечують мінімальні ресурси робочої області відповідно до розділу «Структура СКС», можуть бути встановлені в такий спосіб:

а) один телекомунікаційний роз'єм повинен бути встановлений на симетричному кабелі категорії 3 або вище;

б) другий телекомунікаційний роз'єм повинен бути встановлений на симетричному кабелі категорії 5 (100 ом або 120 ом), на симетричному кабелі 150 ом або на багатомодовому оптоволоконому кабелі.

Вимоги по конфігурації ТР занижені з погляду сучасних вимог: кабелі категорії 3 практично не використовуються. Найбільше поширення одержали кабелі із хвильовим опором 100 ом, що забезпечують погоджене середовище передачі для переважної більшості зразків стандартного мережного встаткування – А.В.

6.2. Магістральна підсистема

6.2.1. Фізична топологія

У магістральній підсистемі повинне бути не більше двох рівнів комутації, що дозволяє обмежити деградацію сигналу в пасивних системах і спростити адміністрування. На шляху від РП поверху до РП комплексу повинен бути не більш ніж один розподільний пункт.

Єдиний розподільний пункт може забезпечити комутацію всієї магістральної підсистеми. Розподільні пункти магістральної кабельної системи можуть розташовуватися в телекомунікаційних приміщеннях або апаратних. У додатку D дані рекомендації зі створення логічної топології «кільце», «шина» і інших на основі фізичної топології «зірка».

Топологія «зірка» застосовна не тільки до кабелів, але й кабельним елементам передавального середовища, таким як індивідуальні волокна або пари Залежно від параметрів системи, кабельні елементи можуть перебувати в одному кабелі по всій довжині або тільки на частині довжини лінії. У магістральній підсистемі допускається використання гібридних і багатоелементних кабелів, що відповідають параметрам розділу 8Вимоги до кабелів.

6.2.2. Вибір типів кабелів

Стандарт визначає п'ять типів передавального середовища. У магістральній підсистемі можливе використання більше одного типу:

багатомодове й одномодове оптичне волокно (перевага віддається багатомодовому волокну 62,5 / 125 мкм).

симетричний кабель 100 0м, 120 0м або 150 0м (перевага віддається симетричному кабелю 100 0м). Відстані магістралі для всіх високошвидкісних застосунків, що використовують електропровідні кабелі повинні бути обмежені відповідно до розділу 6.1.1 Довжина кабелів.

Відмінності ANSI / TIA / EIA-568-A

1. Відсутні симетричний кабель 120 ом і багатомодові оптоволоконі кабелі 50 / 125 мкм.

2. Як середовище передачі зізнається коаксіальний кабель 50 ом. Однак він не рекомендований для монтажу в знову встановлюваних СКС і повинен бути виключений з наступної редакції стандарту. Інші типи середовища передачі, також не включені в стандарт і доповнення, що допускаються до використання в якості, до мінімальної конфігурації, – екрановані кабелі 100 ом, багатопарні кабелі й коаксіальні кабелі 75 ом.

6.2.3. Довжина кабелів магістралі

Максимальні відстані між розподільними пунктами повинні відповідати параметрам. У системах, розміри яких перевищують зазначені параметри, варто спроектувати додаткові РП, довжина магістралей яких не перевищує параметри даного розділу.

Обмеження довжини магістралі носять умовний характер. При використанні найпоширенішого багатомодового оптоволокна 62,5 / 125 зі смугою пропущення 160 МГц х км у вікні 850 нм канал довжиною 2000 метрів забезпечує роботу застосунків класу З (10 МГц) і нижче. Те ж волокно дозволяє передавати сигнали Fast Ethernet не більше ніж на 1300 метрів, а Gigabit Ethernet – 220 метрів. Інакше кажучи, при визначенні типу середовища й довжини каналів магістралей варто враховувати тип і вимоги протоколів – А.В.

Відстань між РП комплексу й РП поверху не повинне перевищувати 2000 м. Відстань між РП будівлі й РП поверху не повинне перевищувати 500 м. Максимальна відстань в 2000 між РП комплексу й РП поверху може бути збільшене при використанні одномодового волоконо-оптичного кабелю. Відстань між РП комплексу й РП поверху, що перевищує 3 км у випадку застосування одномодового оптичного волокна, виходить за рамки справжнього стандарту. Довжина перемичок і комутаційних кабелів у РП комплексу й РП будівлі не повинна перевищувати 20 м. Значення довжин, що перевищують 20 м, віднімаються з максимально припустимої довжини магістрального кабелю.

Відмінності ANSI / TIA / EIA-568-A

Відстань між РП поверху й РП комплексу при використанні електропровідних ліній не повинне перевищувати 800 метрів.

Дане положення американського стандарту суперечить обмеженню сумарної довжини магістралі в 2000 метрів для багатомодового оптоволокна. Якщо в магістралі комплексу є електропровідні й оптоволоконі кабелі, буде діяти обмеження по меншій відстані. Відповідно до міжнародного / європейськими стандартамиами довжина каналу залежить від

категорії середовища передачі й класу застосунків (наприклад, для кабелів категорії 5 і застосунків класу А припустима довжина каналу становить 3000 метрів) – А. В.

6.2.4. Зовнішні служби

Кабелі, по яких передаються сигнали зовнішніх мереж (наприклад, прийняті антеною) можуть входити в будинок у місцях, віддалених від розподільних пунктів. При визначенні максимальної довжини магістрального кабелю необхідно враховувати відстань між крапками вводу зовнішніх мереж і розподільним пунктом, до якого вони підключені. Місцеві нормативи й правила, що регулюють місце розташування інтерфейсів зовнішніх мереж, також впливають на їхнє видалення від розподільних пунктів. Довжину й параметри кабелів зовнішніх мереж варто документувати й надавати операторам послуг із запиту.

6.2.5. Підключення активного телекомунікаційного встаткування.

Передбачається, що довжина кабелів, що прямо з'єднують телекомунікаційне встаткування із РП комплексу й РП будівлі, не перевищує 30 м. Якщо використовуються кабелі більшої довжини, магістральні відстані повинні бути відповідно зменшені.

Відмінності ANSI / TIA / EIA-568-A

Стандарт містить додаткові рекомендації із планування магістралей. Як правило, практично неможливо або економічно недоцільно встановлювати магістраль на весь термін служби системи. Рекомендується передбачати один – три періоди тривалістю від трьох до десяти років. Для кожного з періодів проектується й установлюється максимальне число кабелів і роз'ємів у РП комплексу, будівель, поверхів і в крапках вводу.

Адміністрування є важливим аспектом створення й експлуатації структурованої кабельної системи. Гнучкість СКС може бути повністю реалізована тільки при правильному адмініструванні. Адміністрування включає точне позначення й облік всіх елементів, що становлять кабельну систему, а також кабельних трас, телекомунікаційних і інших приміщень, у яких монтується система. Всі зміни, внесені в кабельну систему, варто вчасно реєструвати – це необхідно для збереження гнучкості. Настійно рекомендується проводити адміністрування з використанням комп'ютерних програм.

Сфера дії адміністрування

Вимоги по адмініструванню, описані в даному розділі, застосовні до структурованої кабельної системи, а також до трас і приміщень, у яких вона монтується. Настійно рекомендується застосовувати описані нижче принципи адміністрування до будь-якої кабельної системи й до активного встаткування.

Ідентифікатори

Кожний елемент структурованої кабельної системи, а також траси й приміщення, у яких вона монтується, повинні бути легко ідентифікуємі. Кожному кабелю, панелі й розніманню повинен мати унікальне позначення (наприклад, назва, колір, номер або рядок символів).

Для кожного телекомунікаційного роз'єму варто вказати наступну інформацію, що відбиває вибір і застосування встановленої системи:

а) ТР: IEC 603-7 Хвильовий опір, категорія й розташування пар у ТР.

б) ТР: оптоволокно. Дизайн волокна (діаметр серцевини й оболонки – А.В.).

Підходящі ідентифікатори повинні бути також привласнені трасам і приміщенням, у яких монтується кабельна система. Елементи, яким привласнюються ідентифікатори, повинні бути чітко маркіровані. Кабелі варто позначати з обох кінців.

Записи

Адміністрування СКС потрібно вести за допомогою записів. Результати тестування системи, якщо таке проводилося, варто зберігати. Не потрібно даним стандартом, але рекомендується вести облік підтримуваних застосунків. Це полегшує виявлення джерел проблем.

Документування

Для процесу адміністрування необхідний належний контроль над веденням записів (схеми кабельних маршрутів, розташування й позначення ТР, розташування й состав РП,

результати тестування й схеми з'єднань). Важливо забезпечити реалізацію відповідних процедур своєчасного відновлення документації

Legrand Data Cabling Solutions LCS3

У цей час кабельні системи Legrand забезпечують високоякісний зв'язок більш ніж з 200 мільйонами пристроїв. Legrand є світовим лідером в області мереж зв'язку для передачі даних. Інвестиції в розробку й проектування структурованих кабельних систем і рішень дозволили розширити пропозиція й досягти найвищого рівня продуктивності. Ці рішення ідеально підходять для сучасних мультимедійних мереж, технологій і застосунків. Комплексні глобальні рішення Legrand для передачі даних ідеально вирішують ключові проблеми цифрових мереж: продуктивність, масштабованість і ефективність.

Зростаючі обсяги обміну даними, що ростуть число мереж, потреба в більше високих швидкостях і щільності встаткування – все це робить необхідним створення більше надійних, безпечних і високопродуктивних електричних і цифрових інфраструктур будівель. LCS3, нова структурована кабельна лінійка Legrand, спеціально розроблена для задоволення цих потреб.

Він пропонує безліч досягнень із погляду продуктивності, масштабованості й ефективності. Нові роз’єми можуть працювати в самих критичних середовищах з мідними рішеннями до категорії 8. LCS3 також містить у собі значно розширену оптоволокону пропозицію, що забезпечує швидкість до 100 Гбіт/с. А також інновації з погляду ергономіки: наші нові структуровані кабельні рішення є модульними, простими в установці в корпусах і оптимізовані для технічного обслуговування.

Більше ефективний, масштабований і високопродуктивний, LCS3 задовольняє останнім вимогам локальних мереж і центрів обробки даних!

Структурована кабельна система (Structured Cabling System, SCS) – це набір комутаційних елементів (кабелів, роз’ємів, коннекторів, кроссових панелей і шаф), а також методика їхнього спільного використання, що дозволяє створювати регулярні, легко розширювані структури зв'язків в обчислювальних мережах.

Структурована кабельна система це система, за допомогою якої проектувальник мережі будує потрібну йому конфігурацію зі стандартних кабелів, з'єднаних стандартними роз’ємами й комутируються на стандартних кроссових панелях. При необхідності конфігурацію зв'язків можна легко змінити – додати комп'ютер, сегмент, комутатор, вилучити непотрібне встаткування, а також поміняти з'єднання між комп'ютерами й концентраторами.

Структурована кабельна система планується й будується ієрархічно, з головною магістраллю й численними відгалуженнями від її.

Типова ієрархічна структура структурованої кабельної системи (рисунок 1) включає:

горизонтальні кабельні підсистеми (у межах поверху);

вертикальні кабельні підсистеми (усередині будівлі);

магістральну кабельну підсистему ЦОД (у межах однієї території з декількома будинками);

кабельну підсистему робочих місць;

центральні комутаційні вузли будівель.

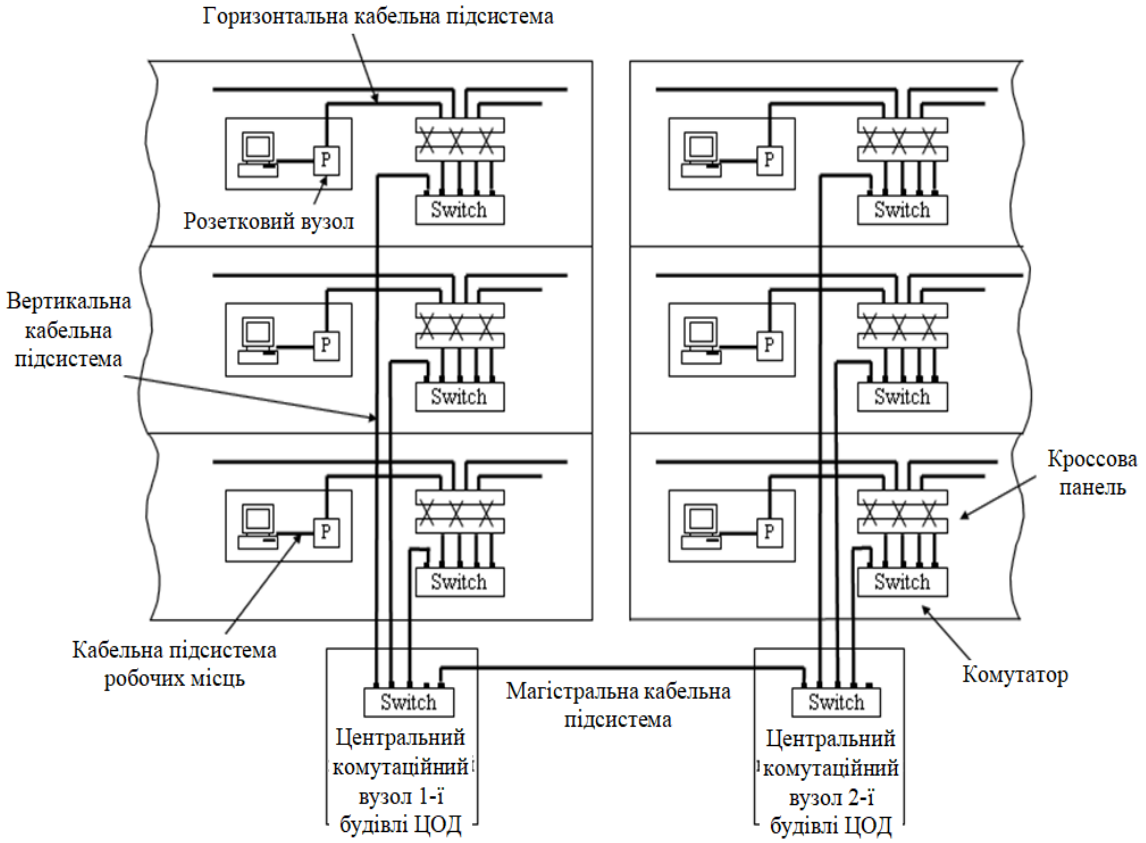


Рисунок 1 – Структурна схема системи

Горизонтальна підсистема

Горизонтальна кабельна система являє собою кабельне розведення, що йде від настінної розетки до місця підключення в комутаційній шафі. Ця ділянка включає наступні елементи:

Адаптер (якщо необхідно) для перетворення інтерфейсу встаткування в модульний інтерфейс.

Лінійні корди від комп'ютера до користувальницького інтерфейсу.

Користувальницький інтерфейс до кабельної мережі.

Кабелі від користувальницького інтерфейсу до комутаційної шафи.

Неекранована кручена пари (UTP).

Патч-кабелі й кроссове сполучне проведення, використовуваний у комутаційній шафі.

Вертикальна підсистема з'єднує кроссові шафи кожного поверху із центральної апаратної будівлі.

Підсистема ЦОД з'єднує кілька будівель з головною апаратною всього ЦОД. Ця частина кабельної системи звичайно називається магістраллю (backbone).

Комутаційний вузол

Комутаційний вузол містить необхідне встаткування для переходу між горизонтальними й вертикальними ділянками кабельної мережі й / або приєднання до якого-небудь активного встаткування (головній комп'ютерній системі, мережній апаратурі й т.д.). Інші назви комутаційного вузла включають комутаційну шафу, телекомунікаційну шафу, апаратну шафу, а також шафу для магістральної кабельної мережі.

Комутаційний вузол може бути:

центральним – центр структурованої кабельної системи одного будівлі.

поверховим – крапка переходу між вертикальною й горизонтальною кабельною системою.

Переваги використання структурованої кабельної системи:

Системонезалежність.

Легкість переміщення персоналу й устаткування без зміни проводки.

Зручність росту й зміни структури системи.

Реконфигуруємість.

Модульний дизайн, що забезпечує гнучкість системи.

Спрощується керування й обслуговування кабельного господарства.

Легкість виявлення й локалізації несправностей.

Підтримка широкого кола завдань.

Зниження експлуатаційних витрат.

Загальні принципи побудови СКС передбачають:

Універсальність СКС – сумісність із устаткуванням будь-яких виробників.

Надмірність – забезпечення таких параметрів передачі сигналів і даних, які дозволять перейти до використання нових технологій або збільшити число користувачів СКС із мінімальними змінами в кабельній проводці.

Модульність – можливість розвитку й зміни систем (модифікацій) з мінімальними матеріальними, трудовими й фінансовими витратами.

Кабельна система будується у відповідності міжнародним стандартам на прокладку кабелів по будинках EIA / TIA 568A – Commercial Building Telecommunication Wiring Standard і ANSI / EIA / TIA 569 – "Commercial Building Standard for Telecommunications Pathways and Spaces".

Вибір типу кабелю для горизонтальних підсистем

Більшість проектувальників починає розробку структурованої кабельної системи з горизонтальних підсистем, тому що саме до них підключаються кінцеві користувачі. При цьому вони можуть вибирати між екранованою кручений парою, неекранованою крученою парою, коаксіальним кабелем і волоконо-оптичним кабелем. Можливі використання й бездротові лінії зв'язку.

Горизонтальна підсистема характеризується дуже більшою кількістю відгалужень кабелю, тому що його потрібно провести до кожної користувальницької розетки, причому й у тих кімнатах, де поки комп'ютери в мережу не поєднуються. Тому до кабелю, використовуваному в горизонтальній проводці, пред'являються підвищені вимоги до зручності виконання відгалужень, а також зручності його прокладки в приміщеннях. На поверсі звичайно встановлюється кроссова панель, що дозволяє за допомогою коротких відрізків кабелю, оснащеного роз’ємами, провести перекомутацію з'єднань між користувальницьким устаткуванням і концентраторами / комутаторами. При виборі кабелю приймаються в увагу наступні характеристики:

– смуга пропущення,

– відстань,

– фізична захищеність,

– електромагнітна перешкодозахищеність,

– вартість.

Крім того, при виборі кабелю потрібно враховувати, яка кабельна система вже встановлена на підприємстві, а також які тенденції й перспективи існують на ринку в цей момент.

Екранована кручена пари STP дозволяє передавати дані на більшу відстань і підтримувати більше вузлів, чим неекранована. Наявність екрана робить її більше дорогою й не дає можливості передавати голос. Екранована кручена пари використовується в основному в мережах, що базуються на продуктах IBM і Token Ring, і рідко підходить до іншому встаткуванню локальних мереж.

Неекранована кручена пари UTP по характеристиках смуги пропущення й підтримуваних відстаней також підходить для створення горизонтальних підсистем. Але тому що вона може передавати дані й голос, вона використовується частіше.

Коаксіальний кабель усе ще залишається одним з можливих варіантів кабелю для горизонтальних підсистем. Особливо у випадках, коли високий рівень електромагнітних

перешкод не дозволяє використовувати кручену пару або ж невеликі розміри мережі не створюють більших проблем з експлуатацією кабельної системи.

Товстий Ethernet володіє в порівнянні з тонким більшою смугою пропущення, він більше стійок до ушкоджень і передає дані на більші відстані, однак до нього складніше приєднатися й він менш гнучкий. З товстим Ethernet складніше працювати, і він мало підходить для горизонтальних підсистем. Однак його можна використовувати у вертикальній підсистемі як магістраль, якщо оптоволоконий кабель із якихось причин не підходить.

Тонкий Ethernet – це кабель, що повинен був вирішити проблеми, пов'язані із застосуванням товстого Ethernet. До появи стандарту 10 Base-T тонкий Ethernet був основним кабелем для горизонтальних підсистем. Тонкий Ethernet простіше монтувати, чим товстий. Мережі на тонкому Ethernet можна швидко зібрати, тому що комп'ютери з'єднуються один з одним безпосередньо. Головний недолік тонкого Ethernet – складність його обслуговування. Кожний кінець кабелю повинен завершуватися термінатором 50 Ом. При відсутності термінатора або втраті їм своїх робочих властивостей (наприклад, через відсутність контакту) перестає працювати весь сегмент мережі, підключений до цього кабелю. Аналогічні наслідки має погане з'єднання будь-якої робочої станції (здійснюване через Т-коннектор). Несправності в мережах на тонкому Ethernet складно локалізувати. Часто доводиться від'єднувати Т-коннектор від мережного адаптера, тестувати кабельний сегмент і потім послідовно повторювати цю процедуру для всіх приєднаних вузлів. Тому вартість експлуатації мережі на тонкому Ethernet звичайно значно перевершує вартість експлуатації аналогічної мережі на кручений парі, хоча капітальні витрати на кабельну систему для тонкого звичайно нижче.

Основні області застосування оптоволоконого кабелю – вертикальна підсистема й підсистеми ЦОД. Однак, якщо потрібна високий ступінь захищеності даних, висока пропускна здатність або стійкість до електромагнітних перешкод, волоконо-оптичний кабель може використовуватися й у горизонтальних підсистемах. З волоконо-оптичним кабелем працюють протоколи AppleTalk, Token Ring, а також нові протоколи 100 VG-AnyLAN, Fast Ethernet, ATM.

Переважним кабелем для горизонтальної підсистеми є неекранована кручена пари категорії 5. Її позиції ще більше зміцняться із прийняттям специфікації 802.3 ab для застосування на цьому виді кабелю технології Gigabit Ethernet.

Вибір типу кабелю для вертикальних підсистем

Кабель вертикальної (або магістральної) підсистеми, що з'єднує поверхи будівлі, повинен передавати дані на більші відстані й з більшою швидкістю у порівнянні з кабелем горизонтальної підсистеми. Найчастіше для вертикальних підсистем використовується оптоволоконий кабель.

Для вертикальної підсистеми вибір кабелю в цей час обмежується трьома варіантами.

Оптоволокно – відмінні характеристики пропускної здатності, відстані й захисти даних; стійкість до електромагнітних перешкод; може передавати голос, відеозображення й дані. Але порівняно дорого, складно виконувати відгалуження.

Товстий коаксіал – гарні характеристики пропускної здатності, відстані й захисти даних; може передавати дані, але з ним складно працювати.

Широкополосний кабель, використовуваний у кабельному телебаченні, – гарні показники пропускної здатності й відстані; може передавати голос, відео й дані. Але дуже складно працювати й потрібні більші витрати під час експлуатації.

Застосування волоконо-оптичного кабелю у вертикальній підсистемі має ряд переваг:

– Передає дані на значно більші відстані без необхідності регенерації сигналу.

– Має сердечник меншого діаметра, тому може бути прокладений у більше вузьких місцях.

– Передані по ньому сигнали є світловими, а не електричними, тому оптоволоконий кабель не чутливий до електромагнітних і радіочастотних перешкод, на відміну від мідного

коаксіального кабелю. Це робить оптоволоконий кабель ідеальним середовищем передачі даних для промислових мереж.

– Оптоволоконому кабелю не страшна блискавка, тому він гарний для зовнішньої прокладки.

– Забезпечує більше високий ступінь захисту від несанкціонованого доступу, тому що відгалуження набагато легше виявити, чим у випадку мідного кабелю (при відгалуженні різко зменшується інтенсивність світла).

Оптоволоконий кабель має й недоліки:

– Дорожче чим мідний кабель, дорожче обходиться і його прокладка.

– Оптоволоконий кабель менш міцний, чим коаксіальний.

– Інструменти, застосовувані при прокладці й тестуванні оптоволоконого кабелю, мають високу вартість і складні в роботі.

Вибір типу кабелю для підсистеми ЦОД

Як і для вертикальних підсистем, оптоволоконий кабель є найкращим вибором для підсистем декількох будівель, розташованих у радіусі декількох кілометрів. Для цих підсистем також підходить товстий коаксіальний кабель.

При виборі кабелю для ЦОД потрібно враховувати вплив середовища на кабель поза приміщенням. Для запобігання поразки блискавкою краще вибрати для зовнішньої проводки неметалічний оптоволоконий кабель. З багатьох причин зовнішній кабель виробляється в поліетиленовій захисній оболонці високої щільності. При підземній прокладці кабель повинен мати спеціальну вологозахистну оболонку (від дощу й підземної вологи), а також металевий захисний шар від гризунів і вандалів. вологозахистний кабель має прошарок з інертного газу між діелектриком, екраном і зовнішньою оболонкою. Кабель для зовнішньої прокладки не підходить для прокладки усередині будівель, тому що він виділяє при згорянні велика кількість диму.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів Legrand Cabling System 3 для ЦОД. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем Legrand Cabling System 3 для ЦОД. Досліджена система Legrand Cabling System 3 для ЦОД. На основі отриманих результатів досліджень створена програмна реалізація системи Legrand Cabling System 3 для ЦОД. Розроблені алгоритми дозволяють успішно вирішувати завдання Legrand Cabling System 3 для ЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Мохамад Гани Абу Таам Разработка математической gert-модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / А.А.Смирнов, Мохамад Гани Абу Таам // Информационные системы в управлении, образовании, промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 498 с.
2. Мохамад Гани Абу Таам метод управления доступом в интеллектуальных узлах коммутации / Мохамад Гани Абу Таам, А.А.Смирнов // Информационные технологии и защита информации в информационно-коммуникационных системах: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – 486 с.
3. Мохамад Гани Абу Таам Математическая gert-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.
4. Мохамад Гани Абу Таам структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Системи управління, навігації та зв'язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120-125.
5. Мохамад Гани Абу Таам Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Гани Абу Таам, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 9(125). – Х.: ХУПС – 2014. – С. 105-110.

6. Мохамад Гани Абу Таам Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 4 (41). – Харків: ХУПС. – 2014. – С. 48-52.
7. Мохамад Гани Абу Таам Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Харків: ХУПС. – 2014. – С.90-95.
8. Мохамад Гани Абу Таам Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-153.
9. Мохамад Гани Абу Таам Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – Випуск 3(43) – Х.: ХУПС – 2015. – С. 100-107.
10. Мохамад Гани Абу Таам Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 3(19). – Х.: ХУПС. – 2015. – С. 134-141.

УДК 004

Е. Філіпов, магістр гр. КН-20М3
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АВ-ОБЛАДНАННЯ ДЛЯ ВІДОБРАЖЕННЯ ВІДЕО НА БАЗІ LG BUSINESS SOLUTIONS

У статті розроблено програмне забезпечення, яке призначено для системи АВ-обладнання для відображення відео на базі LG Business Solutions. Метою розробки є дослідження та програмна реалізація системи АВ-обладнання для відображення відео на базі LG Business Solutions. Об’єктом дослідження є процес АВ-обладнання для відображення відео на базі LG Business Solutions. Предметом дослідження є методи АВ-обладнання для відображення відео на базі LG Business Solutions. Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи АВ-обладнання для відображення відео на базі LG Business Solutions. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерні науки, АВ-обладнання, LG Business Solutions

Постановка проблеми. Для активно зростаючого ринку Digital Signage пропонується широка лінійка устаткування LG Business Solutions. Понад 44% всіх поставок доводиться на професійні дисплеї. За перші два квартали 2021 року їхні продажі виросли на 42% у порівнянні з аналогічним періодом попереднього року. З цілого ряду інших напрямків продажі збільшилися ще більше: так, наприклад, з комутаційного устаткування – у три рази. Продажі професійних дисплеїв ростуть в усьому світі. В 2019 році вони виросли на 20% і досягли 2320 тис. штук (до категорії професійного устаткування ставляться дисплеї з діагоналлю понад 30”). На ринок України доводиться всього близько 0,5% від світового, зате він росте навіть більше швидкими темпами – в 2019 було поставлено 34 тис. дисплеїв, що на 29% більше, ніж в 2018 році. Ринок і далі буде рости. Замовники розуміють, що для повідомлення інформацію до споживачів простіше і якісніше використовувати професійні дисплейні рішення, ніж, наприклад, паперову продукцію.

Потужним драйвером ринку Digital Signage служить ріст популярності цифрової зовнішньої реклами. Як відзначають експерти, поряд з рекламою на мобільних пристроях, вона є найбільш ефективним способом повідомлень інформації до споживача, причому дозволяє зробити це в потрібнім місці й у потрібний час. В Україні виділяється п'ять цільових ринків для професійних дисплеїв. Насамперед це ресторани швидкого харчування, де широко застосовуються інтерактивні дисплеї для прийому замовлень. Слідом за ними йде роздрібна торгівля, комерційні й державні організації. Традиційним замовником є транспортна галузь, де дисплеї використовуються для інформування пасажирів. Значні поставки в попередні роки були здійснені для стадіонів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи АВ-обладнання для відображення відео на базі LG Business Solutions

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи АВ-обладнання для відображення відео на базі LG Business Solutions.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем АВ-обладнання для відображення відео на базі LG Business Solutions.

– Дослідження системи АВ-обладнання для відображення відео на базі LG Business Solutions.

– Програмна реалізація системи АВ-обладнання для відображення відео на базі LG Business Solutions.

Об'єктом дослідження є процес АВ-обладнання для відображення відео на базі LG Business Solutions.

Предметом дослідження є методи АВ-обладнання для відображення відео на базі LG Business Solutions.

Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Відеостіна являє собою особливий екран великого розміру, що складається з окремих модулів. Сьогодні відеостіни можна зустріти в великих конференц-залах, диспетчерських і ситуаційних центрах, торговельних і бізнес-центрах, банках, на вокзалах, в аеропортах або просто на площах і вулицях міст. У кожному із цих місць відеостіна вирішує своє конкретне завдання. Типи модулів відеостін охоплюють великий спектр рішень з розміру, розв'язної, технології відображення інформації й часу безперервної роботи. Класичний варіант відеостіни будується на проекційних модулях – відеокубах. Але, при побудові відеостіни використання тільки відеокубів не завжди фінансово виправдано, часто їх можна замінити на LCD панелі, або навіть побудувати відеостіну за допомогою відеопроекторів, а спеціалізоване програмне забезпечення гарантує максимальний ефект від використання всіх переваг відеостіни.

Відеостіна на відеокубах.

По своєму технічному виконанню відеокуб – це складна проекційна система зворотної проекції. У конструкцію модуля убудовані відеопроектор і система дзеркал, що забезпечує переломлення проекційного променя й проекцію зображення на лінзу Френеля. Відеокуби є найпоширенішим і одночасно найдорожчим рішенням для побудови відеостін.

Відеокуби володіють рядом важливих переваг. Головне з них – це можливість роботи 24/7 і 365 днів у році. Ця особливість украй важлива для диспетчерських і ситуаційних центрів, де моніторинг ситуації цілодобовий.

У відеокубах перебувають DLP проектори, у яких виробники встановлюють різні джерела світла. Ще донедавна, єдиним джерелом світла була UHP лампа. У багатьох моделях відеокубів установлювали відразу трохи UHP ламп, які могли працювати одночасно для більшої яскравості зображення або з резервом один одного. Але сучасні відеокуби оснащують світлодіодним і лазерним джерелами світла. При використанні світлодіоду й

лазера, яскравість зображення зростає в 2 рази, у порівнянні зі звичайної UHP лампою, а термін служби, у безперервному режимі, перевищує 10 років.

Нові пристрої вставного типу (LED Engine), призначені для заміни лампових блоків, мають однакову з ними архітектуру, що забезпечує повну сумісність із діючими системами. Ці пристрої можуть використовуватися для більшості брендів і моделей DLP-кубів для відеостін, зроблених за останні 15 років. Така модернізація дисплеїв від компанії Mitsubishi Electric дозволяє не тільки скористатися технічними перевагами новітньої світлодіодної технології, такими як висока яскравість і, у деяких випадках, підвищена розв'язна здатність, але також істотно знизити загальну вартість володіння існуючим устаткуванням і збільшити строк його служби більш ніж на десять років.

Максимальна розв'язна здатність відеокуба Full HD – 1920x1080 крапок і WUXGA – 1920x1200 крапок. Цей параметр дуже важливий, якщо необхідно виводити на відеостіну складне високодеталізоване зображення.

Переваги й недоліки відеокубів

Переваги:

- Можливість побудови відеостін великої діагоналі й складної геометричної форми.
- Безшовна технологія складання.
- Можливість роботи в режимі 24/7 і 365 днів у році.
- Автоматичне підстроювання яскравості й кольоровості.
- Наявність моделей із фронтальним доступом.

Недоліки:

- Вимагають технологічного простору за відеостіною (у випадку тильного обслуговування).
- Більша глибина в порівнянні з LCD панелями.
- Складність інсталяції й налаштування.
- Яскравість залежить від діагоналі й джерела світла відеокуба.

Відеостіна на LCD панелях

Альтернативним відеокубам варіантом побудови відеостіни, що знаходить своє застосування у багатьох інсталяціях, є відеостіна на LCD панелях. Вартість такої відеостіни небагато дешевше, ніж вартість відеостіни на відеокубах і має ряд особливостей. Для побудови відеостін використовують тільки професійні LCD панелі. Звичайні LCD панелі (побутового застосування) мають безліч недоліків (широка рамка, малий час безперервної роботи, вигоряння, передача кольору…),які вирішені в професійних LCD панелях. Вигідна перевага відеостін на LCD панелях – це їхня глибина, що дозволяє монтувати їх максимально близько, що істотно заощаджує місце й ідеально підходить для невеликих приміщень або для гарних інсталяцій. Яскраве зображення із чудовою передачею кольору досягається за рахунок використання світлодіодного підсвічування матриці панелі.

Технологічно, в LCD панелей, з яких складається відеостіна, є присутнім рамка. Але виробники панелей прагнуть до її мінімізації й у сучасних моделях панелей товщина рамки досягає всього двох міліметрів і практично не видна на зібраній відеостіні. Але оскільки вона все-таки є, в LCD панелях застосовують спеціальну систему компенсацій зазорів між LCD модулями, щоб відображуваний текст був добре читаем на стиках відеостіни.

У професійних LCD панелях присутня функція автоматичної корекції зображення й функція рівномірної яскравості. Після першого налаштування передачі кольору і яскравості відеостіни, автоматика сама буде відслідковувати роботу LCD модулів і підбудовувати яскравість, контрастність і колірну температуру для цільної й рівномірної картинки по всій площі відеостіни.

Переваги й недоліки LCD панелей

Переваги:

- Насичена передача кольору.
- Висока яскравість.

– Низьке енергоспоживання.
– Стійкість до вигоряння пікселів.
– Автоматичне калібрування яскравості й рівномірності зображення.

Недоліки:

– Наявність рамки.
– Складність при обслуговуванні, тому що конструкція кріплення повинна мати механізм для зняття панелі без розбирання відеостіни.
– Ні можливості працювати в режимі 24/7.

Відеостіна на LED модулях

Світлодіодні (LED) відеостіни – це завжди чудова яскравість, чудова передача кольору й висока надійність. Такі відеостіни можна встановлювати не тільки усередині приміщення. Спеціальні герметичні модулі відеостіни не бояться дощу, вітру й морозу й можуть працювати в будь-яку погоду. Завдяки високому розв'язної здатності й маленькій відстані між світлодіодними пікселями, LED відеостіну можна використовувати не тільки для інсталяції в сфері реклами, але й для диспетчерських і ситуаційних центрів, конференц-залів.

Енергоспоживання LED технології вважають одним з найнижчих. Один модуль відеостіни споживає всього близько 200 Вт.

Переваги й недоліки LED відеостін:

Переваги:

– Яскравість і колірна насиченість зображення.
– Низьке енергоспоживання.
– Широкі кути огляду.

Недоліки:

– Досить великий крок окремого пікселя, для перегляду необхідно стояти не ближче 6 метрів до відеостіни.

Відеостіни на відеопроекторах

Для формування екранів величезних розмірів і складних архітектурних форм застосовують професійні потужні відеопроектори. Такі проектори здатні створити зображення не тільки на рівній поверхні, але й на закругленій або навіть у вигляді півсфери. Зовнішній або убудований у проектор контролер формує цілісне безшовне зображення будь-яких розмірів.

Переваги й недоліки

Переваги:

– Можливість створити зображення величезного розміру з урахуванням складної геометрії.
– Прийнятна якість картинки.
– Мобільність і швидкість розгортання.

Недоліки:

– Складність інсталяції.
– Шум вентиляторів.
– Потрібне проекційна відстань для інсталяції.

У даній роботі для реалізації системи АВ-обладнання для відображення відео на базі LG Business Solutions, замість матричних комутаторів використовуються HDMI-over-IP подовжувачі. Подібні рішення використовуються у великих будинках, таких як аеропорти, вокзали, бізнес-центри або спортивні спорудження. Звичайно, перед замовником ставиться завдання сформувати велике табло з 4-9 сегментів і продублювати його вміст на екрани, розміщені в різних куточках об'єкта.

Переваги HDMI-over-IP подовжувачів:

1. Перша й сама головне – це відсутність обмежень, пов'язаних з відстанню. Ви можете розміщати джерело сигналу й приймачі в різних залах, у різних корпусах будинку,

тобто встановлювати передавальне устаткування не там, де потрібно, а там, де зручніше й дешевше.

2. Масштабованість і можливість зміни конфігурацій. Допустимо, ви почали з побудови відеостіни формату 2x2, і надалі зштовхнулися з необхідністю збільшити неї до 4x4: вам не потрібно міняти старе устаткування на нове – просто докупите приймачі й зміните конфігурацію стіни в налаштуваннях устаткування. Оскільки трансляція здійснюється за допомогою Multicast, ви можете з того самого джерела подавати сигнал на одну відеостіну формату 2x2 і на 8 телевізійних панелей, розміщених у залі.

Тому якщо поставлено завдання – зробити так, щоб у великій аудиторії, навіть на самих далеких рядах було видно зображення на екрані, можна збільшити площу загальної стіни, а можна встановити дублюючі монітори між рядами, і все це – на тому самому устаткуванні.

3. Розширення області трансляції. Якщо в замовника споконвічно було поставлене завдання – показувати рекламу зі знижками на моніторі біля кас, а надалі він вирішив продублювати її ж на екранах у торговельних рядах, ви просто додаєте до кожного нового екрана по приймачі, підключаєте Ethernet-кабель, указуєте в web-інтерфейсі розширення трансляції на нові панелі – і все. Топологія Ethernet не знає обмежень, і з однаковою легкістю можна розміщати відеопанелі й в аеропортах, і в торгових центрах, і в державних установах.

Конструкція HDMI-over-IP подовжувачів Aten VE8950 для LG Business Solutions

Звичайно HDMI-подовжувач, що передає сигнал через IP-мережу складається із приймача (Aten VE8950R) і передавача (Aten VE8950T).

Фізично це невеликі залізні коробочки з VESA-кріпленням, які встановлюються з тильної сторони відеопанелі або на кронштейні проектора. Керування пристроями здійснюється через web-інтерфейс, тому з органів керування й індикації на Aten VE8950 для LG Business Solutions є тільки дві кнопочки для перемикання ID-номера пристрою, невелике віконце, у якому пробігає IP-Адресу й стандартні індикатори Link/Power.

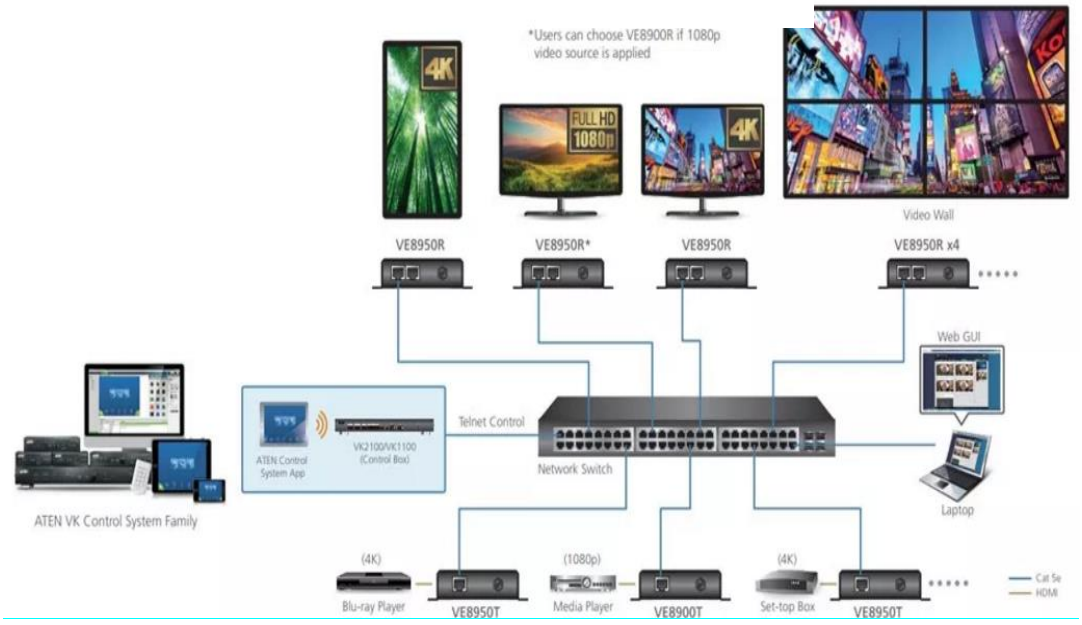


Рисунок 1 – Структурна схема системи

Приймачі Aten VE8950R мають по два LAN-порти для організації наскрізного підключення за принципом Daisy Chain, завдяки чому відпадає необхідність у використанні мережних комутаторів при передачі сигналу на відстань до 600 метрів, або при побудові відеостіни. На схемі нижче саме показані переваги наскрізного підключення приймачів: для 27 приймачів Aten VE8950R задіяні лише 4 порти мережного комутатора.

На схемі вище саме показані переваги наскрізного підключення приймачів: для 27 приймачів Aten VE8950R задіяні лише 4 порти мережного комутатора.

Налаштування відеостіни – процес досить пересічний: в Web-Інтерфейсі Aten VE8950T вибираємо тип віщання:

– "розгалужувач", якщо нам потрібно просто дублювати відеосигнал на яку-небудь панель

– "відеостіна" – те, що нам потрібно.

Хочеться звернути увагу, що передавач Aten VE8950T може як транслювати EDID підключеної відеопанелі до джерела сигналу, так і передавати свої ідентифікаційні дані. Останнє потрібно, наприклад, щоб примусово виставити на комп'ютері або відеоплеєрі розв'язна здатність, не підтримувана ТБ-панелями.

Наприклад, ви можете для 4-х панелей з дозволом 1080p задати загальний розв'язна здатність на вході 4K, щоб одержати більше високу якість картинки на відеостіні.

Тест – розподіл трафіку

Взагалі, питання IP-трафіку в подібних пристроях чи є не основним, адже з однієї сторони виробникові потрібно забезпечити передачу відео без втрат, а з іншого боку – заощаджувати кожний біт, щоб замовник мав можливість використовувати існуючу гігабітну мережа підприємства без яких-небудь обмежень. Давайте подивимося, який витрата трафіку є присутнім в Aten VE8950 для LG Business Solutions.

Таблиця 1 – Витрата трафіку в Aten VE8950 для LG Business Solutions

Розв'язна здатність на вході	Тип контенту	Типовий трафік, Мбіт/с	Піковий трафік, Мбіт/с
1080p, 50Hz	Презентація, слайди	5	9
1080p, 50Hz	Відео	320	800
1080p, 60Hz	Відео	400	800
4K, 60Hz	Відео	300	400
4K, 30Hz	Відео	400	800

Із практичної точки зору, навіть у розв'язній здатності 1080p на одному гігабітном порту двом передавачам Aten VE8950 для LG Business Solutions може бути тісно, тому при використанні деревоподібної мережної топології, Aten рекомендує використовувати кореневі комутатори з 10-гігабітними Uplink-портами й не підключати 100-мегабитні пристрою у світчі, через які проходить Multicast-трафік.

Наші тести показують, що трафік з максимальним стиском у режимі 1080p 60Hz падає з 320 Мбіт/с до 160-180 Мбіт/с з піками до 500 Мбіт/с. На відеороликах розходження картинки не спостерігається, а от тест «Мерехтіння» з онлайн-сервісу Monteon для тестування моніторів, показує, що передавач не віджимає картинку, а вирізує з її ті області, які вважає непотрібними. У нашому випадку, частина курсору чомусь зависала на екрані на довгі 10 секунд, перш ніж обновилася, а от у відео таких проблем не було.

До мого подиву, при зміні розв'язної здатності на 4K, трафік не просто не виріс, а навіть знизився до 250 – 300 Мбіт/с із піками до 400 Мбіт/с. Справа в тому, що трансмітер Aten VE8950T підтримує розв'язної здатності 4096x2160 і 3840x2160 з наступними обмеженнями:

– При частоті 30 Гц підтримується колірний режим 4:4:4

– При частоті 60 Гц підтримується колірний режим 4:2:0

У той же час, приймач Aten VE8950R підтримує 4K розв'язної здатності тільки при частоті 30 Гц і в колірному режимі 4:4:4. Тому, якість відображення визначається тим, яка частота розгорнення встановлена на джерелі:

Як говориться, різниця видна неозброєним поглядом. Плюс, при установці розв'язної здатності 4K із частотою 60 Гц, зображення на екрані зменшується, як у режимі відеостіни, так і в режимі розгалуження, і з'являються досить великі чорні бордюрчики. При частоті відновлення 30 Гц картинка виглядає ідеально, але дивитися відео вже некомфортно через помітні посмикування.

Разом, для 4K рецепт досить простій: для трансляції текстів, схем і графіків – установлюйте частоту 30 Гц, для відображення відео – 60 Гц.

Можливості масштабування

Комплект Aten VE8950 для LG Business Solutions складається із приймача VE8950R і передавача VE8950T, що продаються окремо. До одному з передавачів можна підключити до 64 приймачів, що дозволяє створювати відеостіни розмірами до 8x8.

Разом з HDMI сигналом, транслюються USB 2.0 порти (один порт для підключення до ПК на передавачі й 2 порти для пристроїв на приймачі), аудио сигнал з лінійного входу, ІЧ-трансмітер і RS232 порт. Для керування через RS232 підтримуються не тільки Telnet, але й контролери керування Aten.

Типове енергоспоживання

Типове енергоспоживання передавача VE8950T становить 3.07 Вт, а приймача VE8950R – 4.5 Вт. При такому низькому енергоспоживанні, цілком логічн запитання – чому не підтримується Po? Видимо, виробник розсудив, що й приймач і передавач звичайно розміщаються біля електричних розеток, так що живлення по сигнальному кабелю зайво.

Ціна питання

Середня роздрібна вартість одного приймача Aten VE8950T або Aten VE8950R становить 1300$. При такій вартості, для побудови відеостін, HDMI-over-IP подовжувачі доцільно використовувати в асиметричних інсталяціях, де кількість приймачів перевищує кількість передавачів.

Давайте приведемо розрахунок вартості інсталяції, що складає з відеостіни формату 4x4 і 4 звичайних екранів відображення, на які буде подаватися зображення з 5 різних джерел. Мається на увазі, що використовуються професійні відеопанелі з убудованою функцією відеостіни. При використанні HDMI-over-IP подовжувачів, розрахунок досить простій: нам буде потрібно:

- 5 передавачів VE8950T.
- 5 приймачів VE8950R.

Разом – 11000$

Збираючи ту ж саму інсталяцію на матричних комутаторах, нам доведеться використовувати модульну модель Aten VM3200 наступної конфігурації:

- Шасі Aten VM3200 – 1 штука – 16460$.
- Плата відеоуведення Aten VM7814 – 2 штуки – 3160$.
- Плата відеовиходів Aten VM8814 – 5 штук – 15787$.
- Скалюючий приймач Aten VE816R – 18 штук – 24498$.
- Скалюючий передавач Aten VE801T – 5 штук – 4294$.

Разом – 64 199 $.

Aten VE8950 для LG Business Solutions дозволяє задіяти в одній інсталяції як 4K, так і 1080p панелі, використовуючи єдиний 4K сигнал на вході, причому конфігурація настроюється через сучасний HTML5 інтерфейс простими кличами мишкою. Практично ніяких мережних налаштувань пристрій не припускає, так що мається на увазі, що ви використовуєте керований комутатор 2-го рівні або старший. При виборі мережного устаткування, переконаєтеся, що комутатор підтримує функцію IGMP Snooping, має можливість пропускати невідомі Multicast-пакети й дозволяє знижувати затримки в мультикаст-трансляціях за рахунок функції Immediate Leave. На щастя, такі комутатори зараз досить доступні: у нашім тесті ми використовували китайський Netis ST3310GF вартістю менш 100$.

Що сподобалося: у тепличних умовах, коли не потрібно свердлити стіни й прокладати кабелю, на налаштування відеостіни пішло менш 40 мінут, тобто даний комплект цілком можна розглядати як Drop-in рішення в існуючу цифрову інфраструктуру будинку.

Що не сподобалося: повну відсутність якої-небудь діагностики з боку HDMI подовжувача. Хотілося б мати доступ до Log-файлу, щоб відслідковувати хоча б мережну активність, а так само моменти перезавантаження пристрою.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів АВ-обладнання для відображення відео на базі LG Business Solutions. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем АВ-обладнання для відображення відео на базі LG Business Solutions. Досліджена система АВ-обладнання для відображення відео на базі LG Business Solutions. На основі отриманих результатів досліджень створена програмна реалізація системи АВ-обладнання для відображення відео на базі LG Business Solutions. Розроблені алгоритми дозволяють успішно вирішувати завдання АВ-обладнання для відображення відео на базі LG Business Solutions. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Дреев А.Н. Использование неравномерного распределения единичных битов для дополнительного сжатия SPIHT кода / А.Н. Дреев, А.А. Смирнов // Информационные системы в управлении, образовании, промышленности: монография. Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – С. 498.
2. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
3. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
4. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
5. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
6. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58
7. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв // Матеріали науково-практичної конференції, присвяченої 80-річчю фізико-математичного факультету КДПУ ім. В. Винниченка 26 листопада 2010 р. – Кіровоград – С. 12
8. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19
9. Дреев А.Н. Повышение оперативности доставки данных повышенной востребованности в телекоммуникационных системах и сетях / А.Н. Дреев, А.А. Смирнов, Е.В. Мелешко // Проблеми і перспективи розвитку ІТ-індустрії 25-26 квітня 2013 р. Системи обробки інформації. – Випуск 3 (110). Том 2. – Харків: ХУПС. – 2013. С. – 199.
10. Дреев А.Н. Экстраполяция квазипериодических процессов с аддитивными помехами / А.Н. Дреев, А.А. Смирнов // П'ята Міжнародна науково-практична конференція "Інформаційні технології та моделювання в економіці" 15-16 травня 2014 р. – Черкаси – С. 59
11. Дреев А.Н. Статистическая модель передачи многопакетного сообщения в телекоммуникационной системе или сети / А.Н. Дреев, А.А. Смирнов // «Компьютерное моделирование в наукоемких технологиях (КМНТ-2014)» Харьков, 28-31 мая 2014 года – С. 137-140

УДК 004

Ю. Толмачов, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ WEB-ЗАСТОСУНКІВ

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки для виявлення вразливостей web-застосунків. Метою розробки є дослідження та програмна реалізація системи кібербезпеки для виявлення вразливостей web-застосунків. Об'єктом дослідження є процес кібербезпеки для виявлення вразливостей web-застосунків. Предметом дослідження є методи кібербезпеки для виявлення вразливостей web-застосунків. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи кібербезпеки для виявлення вразливостей web-застосунків. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, вразливості, web-застосунки

Постановка проблеми. Web-застосунки в сучасному світі знайшли своє місце практично у всіх сферах діяльності людини. Вони використовуються для найрізноманітніших цілей від навчання та розваг до проектування найскладніших систем.

Проте є і зворотна сторона такої широкої функціональності: їх компрометація може призвести до катастрофічних наслідків. Все нові й нові вектори атак ставлять під загрозу безпеку як власника бізнесу так і їх клієнтів.

Для звичайного користувача це може обернутись крадіжкою особистих даних. Щодо компаній – то це може призвести до того, що вона втратить репутацію, позбудеться важливих клієнтів, зазнає фінансових втрат. Несанкціонований доступ до веб-сайту зловмисником загрожує власнику блокуванням сайту в пошукових і рекламних мережах, відмовою в наданні послуг хостингової компанії, втратою клієнтської бази і зруйнованої діловою репутацією. Відвідувачі веб-сайту ризикують потрапити під контроль "хакерів" в разі розміщення ними шкідливого коду на його сторінках. Зловмисники можуть отримати ваші приватні дані, зашифрувати всі файли на пристрої або ж проводити стеження за користувачами.

Постійно зростаючий функціонал, проведення платежів, передача персональних даних та інше, все це робить сайти все більше привабливими для різного роду порушників та крадіїв інформації, що обумовлює необхідність розробки і впровадження нових та вдосконалення існуючих засобів захисту.

Саме тому, виявлення вразливостей безпеки web-застосунку не менш важлива, ніж реалізація його основних функцій. Виявлення вразливостей на етапі проектування та розробки web-застосунку дозволяє значно полегшити роботу над його системою захисту.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи кібербезпеки для виявлення вразливостей web-застосунків

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи кібербезпеки для виявлення вразливостей web-застосунків.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

Огляд існуючих систем кібербезпеки для виявлення вразливостей web-застосунків.

Дослідження системи кібербезпеки для виявлення вразливостей web-застосунків.

Програмна реалізація системи кібербезпеки для виявлення вразливостей web-застосунків.

Об’єктом дослідження є процес кібербезпеки для виявлення вразливостей web-застосунків.

Предметом дослідження є методи кібербезпеки для виявлення вразливостей web-застосунків.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. На високому рівні безпека веб-застосунків базується на принципах безпеки прикладних програм які мають доступ до інтернету. Більшість атак на веб-застосунки реалізуються шляхом міжсайтового скриптингу (XSS) і SQL-ін’єкцій які зазвичай можливі через недостатню професійність кодера і помилками зв’язаними з обробкою застосунком вхідних і вихідних даних. Зазвичай ці дві загрози стоять на початку усіх чартів які надають інформацію про найчастіші загрози які є наслідком погано написаного коду (табл. 1).

OWASP в межах проекту Top Ten Vulnerabilities – склав список найбільш десяти найчастіших частих загроз веб-застосунків, зазвичай список оновлюється з періодом 3 роки.

1. Ін'єкції – Injections. Додатки використовують SQL-запити для того, щоб отримувати, додавати, змінювати або видаляти дані, наприклад при редагуванні користувачем своїх особистих даних або заповненні анкети на сайті. При недостатній перевірці даних від користувача, зловмисник може впровадити в форму Web-інтерфейсу додатку спеціальний код, що містить шматок SQL-запиту.

2. Недоліки системи аутентифікації і зберігання сесій (Broken Authentication and Session Management)

У разі, якщо ваш ідентифікатор вкраде зловмисник, а в системі не були реалізовані перевірки, скажімо IP-адреси сесії, або перевірки наявності більш одного з'єднання в одній сесії, зловмисник зможе отримати доступ до системи з правами вашого облікового запису. А якщо це інтернет-банк або кабінет платіжної системи, про наслідки такого несанкціонованого доступу легко здогадатися.

3. Міжсайтовий скриптинг – XSS (Cross Site Scripting). Міжсайтовий скриптинг – ще одна помилка валідації призначених для користувача даних, яка дозволяє передати JavaScript код на виконання в браузер користувача. Атаки такого роду часто також називають HTML-ін'єкціями, адже механізм їх впровадження дуже схожий з SQL-ін'єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері користувача.

4. Небезпечні прямі посилання на об'єкти (Insecure Direct Object References)

Даний вид уразливості є також наслідком недостатньої перевірки призначених для користувача даних. Суть її полягає в тому, що при виведенні будь-яких конфіденційних даних, наприклад особистих повідомлень або облікових карток клієнтів, для доступу до об'єкта використовується ідентифікатор, який передається у відкритому вигляді в адресному рядку браузера, і не реалізована перевірка прав доступу до об'єктів.

5. Небезпечна конфігурація (Security Misconfiguration).

Безпека Web-додатків вимагає наявності безпечної конфігурації всіх компонентів інфраструктури: компонентів програми (таких як фреймворки – frameworks), веб-сервера, сервера баз даних і самої платформи. Налаштування компонентів сервера за замовчуванням найчастіше небезпечні і відкривають можливості до атак. Наприклад, крадіжка сесійного cookie через JavaScript під час XSS-атаки стає можливою завдяки виключеним за замовчуванням налаштуванням cookie_http only.

6. Незахищеність критичних даних (Sensitive Data Exposure)

Багато web-додатків не захищають конфіденційні дані, такі як кредитні карти і облікові дані для автентифікації. Зловмисники можуть вкрасти або модифікувати такі слабо захищені дані для використання в своїх корисливих цілях.

7. Відсутність рівнів функцій контролю доступу (Missing Function Level Access Control)

Суть уразливості, як випливає з назви, полягає у відсутності перевірки наявності належного доступу до запитуваного об'єкту.

8. Міжсайтова підробка запиту (Cross-Site Request Forgery, CSRF/XSRF)

Вектор атаки CSRF, також відомий як XSRF, дозволяє зловмиснику виконувати від імені жертви дії на сервері, де не реалізовані додаткові перевірки.

9. Використання компонентів з відомими уразливими (Using Components with Known Vulnerabilities)

Найчастіше web-додатки написані з використанням спеціальних бібліотек або «фреймворків» (англ – framework), які поставляються сторонніми компаніями. У більшості випадків ці компоненти мають відкритий вихідний код, а це означає, що вони є не тільки у вас, але і у мільйонів людей у всьому світі, які студіюють їх вихідний код, в тому числі, і на предмет вразливостей. І потрібно відзначити, що роблять вони це аж ніяк не безуспішно.

10. Невалідовані переадресації та пересилання (Unvalidated Redirects and Forwards)

Web-додатки часто переадресовують користувача з однієї сторінки на іншу. В процесі можуть використовуватися неналежним чином перевіряються параметри із зазначенням сторінки кінцевого призначення переадресації.

Таблиця 1. – Топ загроз web-застосунків від Cenzic за 2021 р.

Відносна частота загрози	Назва загрози
37%	Міжсайтовий скриптинг
16%	SQL ін'єкції
5%	Розкриття повного шляху у get запитах
5%	Data breach (information disclosure)
4%	Виконання довільного коду
4%	Пошкодження пам'яті
4%	Cross-site request forgery
3%	Розкриття конфіденційної інформації
3%	Довільне виконання файлів
2%	Виконання локальних файлів серверу
1%	Віддалене виконання файлів
1%	Переповнення буферу
15%	Інші, включаючи ін'єкції JS-коду

До основних причин появи вразливостей web-застосунків та web-систем відносяться:

Повна відсутність перевірки вхідних даних (у web-формах будь-яких систем) або тільки часткова перевірка даних.

Некоректна обробка вхідних даних (нульовий байт, символи рівня директорій).

Переповнення буферу.

Необережна робота програми з файлами, у випадку коли ім’я файлу передається програмі ззовні (GET або POST).

Не врахування особливостей GET та POST запитів.

Некоректна робота з паролями (під час зберігання, передачі та обробки).

Неправильні права доступу.

Неправильні права програм на сервері.

Не врахування особливостей роботи програм завантаження файлів на сервер.

Некоректна логіка роботи веб-програми, яка при деяких допустимих вхідних даних приводить до непередбачуваних наслідків.

Виведення інформації при помилках програми або доступу до Бази Даних, коли виводиться додаткова службова інформація, не призначена для сторонніх очей.

Некоректна робота з Базами Даних (паролі, виведення службової інформації, завелика кількість запитів до БД).

Вразливості недостатньої обробки вхідних даних при роботі з БД (SQL-injections).

Неоптимізований програмний код, котрий приводить до значних навантажень на веб-сервер (при своїй звичайній роботі та особливо у випадку збою при передачі некоректних вхідних даних).

Вразливість web-застосувань та систем до DoS та DDoS атак.

Після розгляду вразливостей web-застосунків та причин їх появи перейдемо до етапу проектування системи, а саме розробки структури та функціональності системи.

Розробка структурної схеми

На структурній схемі (рис. 1) представлено основні структурні особливості архітектури системи та відображено її головні структурні блоки:

а) Інтерфейсний модуль;

б) Модуль налаштування інтерфейсу та тестів;

в) Модуль підключення та запуску тестових модулів;

г) Модуль тестування вразливості операцій рівня адміністратора;

д) Модуль тестування вразливості операцій рівня менеджменту;

е) Модуль тестування вразливості операцій рівня користувача;

ж) Модуль тестування безпеки фінансових операцій.

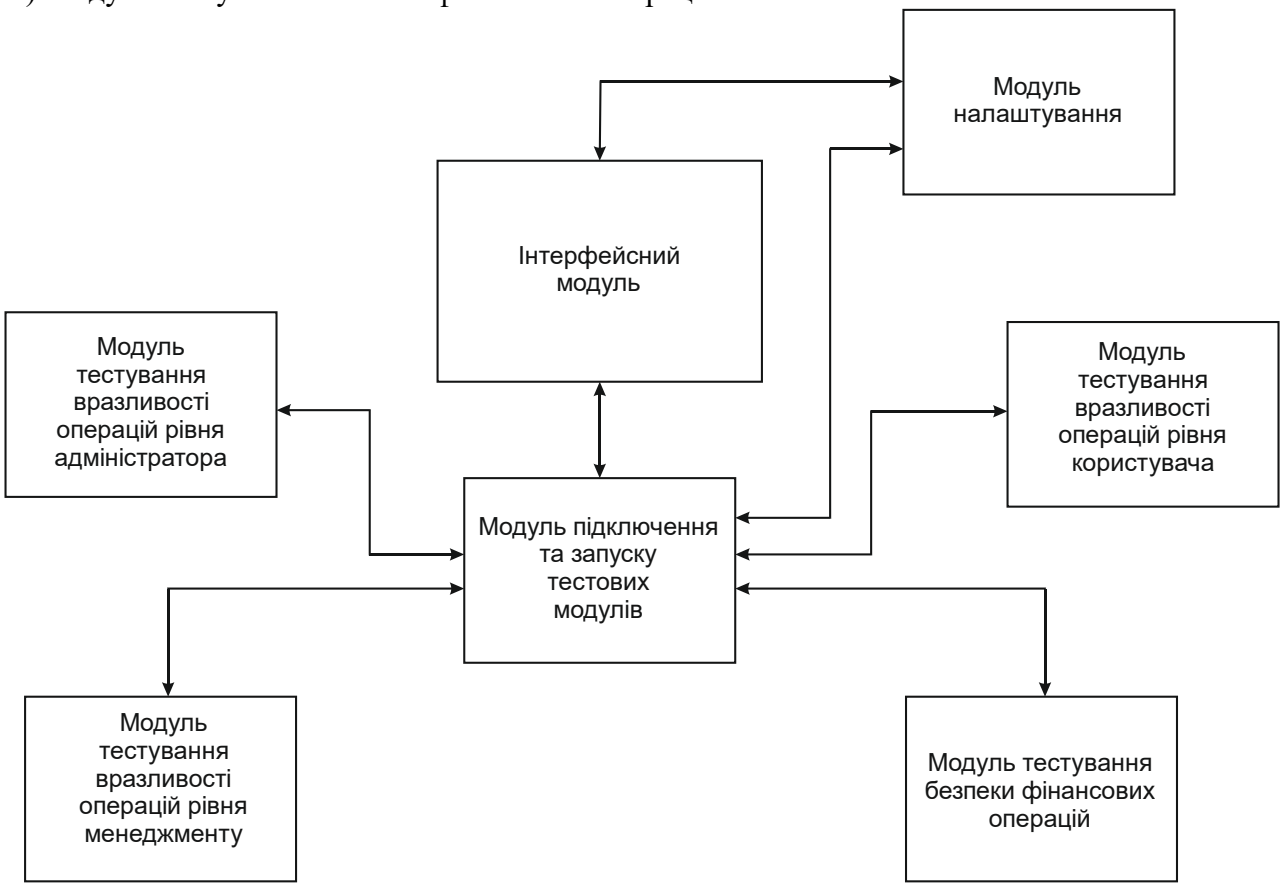


Рисунок 1 - Структурна схема роботи системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки для виявлення вразливостей web-застосунків. Рішення

даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем кібербезпеки для виявлення вразливостей web-застосунків. Досліджена система кібербезпеки для виявлення вразливостей web-застосунків. На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для виявлення вразливостей web-застосунків. Розроблені алгоритми дозволяють успішно вирішувати завдання кібербезпеки для виявлення вразливостей web-застосунків. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

С. Тесля, магістр гр. КІ-20М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ КОМУНАЛЬНИХ ТЕПЛОВИХ МЕРЕЖ

У статті розроблено програмне забезпечення, яке призначено для системи керування комунальних теплових мереж. Метою розробки є дослідження та програмна реалізація системи керування комунальних теплових мереж. Об’єктом дослідження є процес керування комунальних теплових мереж. Предметом дослідження є методи керування комунальних теплових мереж. Методи дослідження базуються на методах теорії автоматизованого управління , методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи керування комунальних теплових мереж. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення
комп’ютерна інженерія, автоматизоване керування

Постановка проблеми. Розвиток сучасної обчислювальної техніки, електроніки й радіотехніки дозволяє створювати складні системи, призначені для виконання різних наукових, виробничих, технологічних завдань [1-5]. Використання таких систем покликано поліпшити якість, ефективність тих або інших виробничих цілей. Існує кілька наукових напрямків, в основі яких лежить об'єднання обчислювальної техніки й електроніки з технологічними процесами, радіоапаратурою [3-8]. Якщо раніше об'єднання різних високонаукових технологій і засобів обчислювальної техніки використовувалося в основному в рішенні різних наукових проблем, таких як освоєння космосу, вивчення надр землі й багатьох інших, то зараз такі високонаукові технології використовуються й у повсякденному житті. Одним з напрямків використання мікропроцесорної техніки, є її застосування для реалізації контролю параметрів різних комунальних мереж та управління ними. В даному проекті за основу взята тепломережа. Особливістю проекту є його розробка на основі діючої системи теплопостачання міста Кропивницького. У цей час передбачено технічне оснащення більше 100 пунктів обліку теплової енергії, розташованих у Кіровограді. Апаратно-програмний комплекс призначений для передачі й контролю вимірюваних параметрів з пунктів обліку теплової енергії, розосереджених по території міста Кропивницького, на диспетчерський пункт. Застосування апаратно-програмного комплексу дозволить підвищити ефективність роботи системи теплопостачання міста, поліпшить оперативність виконання тих або інших відбудовних робіт, так як комплекс буде стежити за роботою системи теплопостачання цілодобово.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування комунальних теплових мереж

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи керування комунальних теплових мереж.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем керування комунальних теплових мереж.
- Дослідження системи керування комунальних теплових мереж.
- Програмна реалізація системи керування комунальних теплових мереж.

Об'єктом дослідження є процес керування комунальних теплових мереж.

Предметом дослідження є методи керування комунальних теплових мереж.

Методи дослідження базуються на методах теорії автоматизованого управління , методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У цей час стрімко розвивається мікроелектроніка й мікропроцесорні системи. У цих областях, як ні в яких інших, знаходять своє широке застосування високі технології, швидше всього впроваджуються нові технічні рішення, нові технології, росте потужність обчислювальних елементів з одночасним зменшенням їхніх розмірів. Для даного проекту було обрано одне з таких рішень – мікроконтролер AT90S1200, фірми Atmel. Atmel сьогодні – це прогресивна компанія, що випускає складні вироби сучасної мікроелектроніки; це один з визнаних світових лідерів у виробництві широкого спектра пристроїв енергонезалежної пам'яті високої швидкодії й мінімального питомого енергоспоживання, мікроконтролерів загального призначення й мікросхем програмувальної логіки від найпростіших пристроїв PAL і GAL до мікросхем ЗВІС CPLD і FPGA. Досить сказати, що практично всі базові кристали промислового стандарту MCS51 фірми Intel успішно замінені прямими аналогами сімейства AT89 фірми Atmel. Ці швидкісні, повністю статичні 8-розрядні КМОП мікроконтролери з модифікованою багаторазово Flash-пам'яттю програм, низьким енергоспоживанням і широким діапазоном допустимих напружень живлення, апаратно й програмно сумісні з відповідними мікроконтролерами Intel і користуються заслуженою популярністю в розроблювачів і виробників електронної апаратури.

Однак, хочеться докладніше познайомитися із ще одним украй цікавим напрямком сучасної мікроелектроніки, розвиваємим активно фірмою Atmel. Це нове сімейство високопродуктивних 8-розрядних RISC (Reduced Instruction Set Computers) мікроконтролерів загального призначення, об'єднаних загальною маркою AVR [7]. Задум створення AVR народився в дослідницькому центрі Atmel у Норвегії. Група розроблювачів запропонувала ряд ідей, які лягли в основу концепції AVR – мікроконтролерів:

1) використовувати новітню, найбільш швидкісну й економічну КМОП технологію фірми Atmel у сполученні з RISC архітектурою для розробки й виробництва швидких 8-розрядних мікроконтролерів, порівнянних з 16-розрядними мікропроцесорами й мікроконтролерами по продуктивності й переважаючих мікросхемах стандартної КМОП логіки по швидкості. Очікувана продуктивність – до 20 MIPS на частоті 20 Мгц, що всього на 30% менше, ніж в Intel KU80386 EXTC-25 при операціях типу "регістр – регістр". Час виконання короткої команди на такій тактовій частоті становить 50 нс;

2) розробляти архітектуру й систему команд AVR у найтіснішій згоді із принципами мови С так, щоб апаратна частина нового мікроконтролера і його система команд були невід'ємними частинами одного цілого й використовувалися з максимальним к.п.д. Істотно скорочується час розробки проектів і, відповідно, знижується їхня вартість, а також полегшується створення універсальних засобів підтримки розробок. Недалеким від істини буде й твердження, що мова С є найбільш популярним і ефективним засобом для програмування мікроконтролерів;

3) функціонально розширити мікроконтролер можливістю програмування в системі (ISP) шляхом об'єднання Flash-Технології фірми Atmel зі стандартним швидкісним послідовним інтерфейсом (SPI). Це дозволяє багаторазово модифікувати програму не тільки за допомогою звичайного програматора, але й безпосередньо в системі, у кінцевому пристрої користувача. При цьому не потрібно вводити ніяких додаткових апаратних вузлів і допоміжних джерел живлення.

Результатом з'явилася поява нового, дуже дешевого, швидкісного, легкого в освоєнні й використанні сімейства AT90S 8-розрядних мікроконтролерів марки AVR. Вони являють собою потужний інструмент, базу для створення сучасних високопродуктивних і економічних контролерів багатоцільового призначення. Так, наприклад, AVR використовуються у виробах класу Smart Card для персональних комп'ютерів, у

супутникових навігаційних системах для визначення місця розташування автомобілів на трасі, у мініатюрних автомобільних пультах дистанційного керування, у мережних картах і на материнських платах ЕОМ, у стільникових телефонах нового покоління й т.д.

Апаратні можливості:

– діапазон напруг живлення, В – 2,7 – 6,0;
– тактова частота, Мгц – 0-16;
– кількість ліній вводу/виводу (max) – 15;
– кількість інструкцій – 89;
– обсяг Flash ROM, байт – 1ДО;
– обсяг EEPROM, байт – 64;
– кількість таймерів/лічильників – 1;
– аналоговий компаратор – є;
– SPI (завантаження ROM і EEPROM) – є;
– сторожовий таймер – є;
– кількість біт захисту – 2;
– число режимів енергозбереження – 2;
– число джерел переривання: внутрішніх/зовнішніх – 2/1;
– тип корпуса – DIP28, SOIC28, SSOP28.

AT90S1200 мають Flash-пам'ять програм ROM обсягом 1K, що може бути завантажена як за допомогою звичайного програматора, так і за допомогою SPI інтерфейсу. Число циклів перезапису ROM – не менш 1000. Два програмувальних біти таємності дозволяють захистити пам'ять програм від несанкціонованого зчитування. AT90S1200 мають також блок енергонезалежної пам'яті даних EEPROM обсягом 64 байта, що стирається електрично. Цей тип пам'яті, доступний програмі мікроконтролера безпосередньо в ході її виконання, зручний для зберігання проміжних даних, різних констант, таблиць перекодувань, каліброваних коефіцієнтів і т.п. EEPROM може бути завантажена ззовні як через SPI інтерфейс, так і за допомогою звичайного програматора. Число циклів перезапису – не менш 100000.

Перелічимо периферійні пристрої AVR:

– таймер/лічильник, розрядність 8 біт;
– швидкісний послідовний інтерфейс SPI;
– убудована система скидання мікроконтролера;
– асинхронний дуплексний послідовний порт UART;
– контролер переривань;
– внутрішній тактовий генератор;
– сторожовий (WATCHDOG) таймер.

Внутрішній тактовий генератор може запускатися від зовнішнього джерела опорної частоти, від зовнішнього кварцового резонатора або від внутрішньої RC-ланцюжка.

Оскільки всі AVR повністю статичні, мінімальна припустима частота нічим не обмежена (аж до покрокового режиму). Максимальна робоча частота визначається конкретним типом мікроконтролера. Обмеження верхньої границі частотного діапазону пов'язані з технологічними проблемами при виробництві мікросхем і будуть усунуті в наступних версіях кристалів. У цей час контролер AT90S1200 версії "F" може працювати на частоті 16 Мгц при кімнатній температурі, а обмеження 12 Мгц діє у всьому температурному діапазоні [7].

Якщо часозадаючим елементом для тактового генератора AVR є внутрішній RC-ланцюжок, то частота, на якій працює мікроконтролер, фіксована й становить 1 Мгц. Це значення наближене й змінюється залежно від величини напруги живлення й температури корпуса. Вибір джерела тактової частоти (внутрішня/зовнішня) програмується, правда тільки за допомогою зовнішнього програматора. Як правило, AVR поставляються з фабрики вже "спеченими" для роботи від зовнішнього джерела опорної частоти, але можна замовити й інші. При цьому в абревіатурі мікроконтролера з'являється літера "A", що вказує на те, що

тактовий генератор даного кристала функціонує від убудованого RC-ланцюжка, наприклад, AT90S1200 A-12PC. Запрограмувати мікроконтролер AT90S1200 на роботу від внутрішнього RC-генератора через послідовний порт SPI неможливо. Сторожовий таймер призначений для захисту мікроконтролера від збоїв у процесі роботи. Він має свій власний RC-генератор, що працює на частоті 1 Мгц. Як і для основного внутрішнього RC-генератора, значення 1 Мгц є наближеним і залежить насамперед від величини напруги живлення мікроконтролера й від температури.

Порти вводу/виводу AVR мають число незалежних ліній "Вхід/Вихід" від 5 до 32. Кожний розряд будь-якого порту може бути запрограмований на вводу або на вивід інформації. Потужні вихідні драйвери забезпечують типову струмову навантажувальну здатність 20 мА на лінію порту (струм, який втікає) при максимальному значенні 40 мА, що дозволяє, наприклад, безпосередньо підключати до мікроконтролера світлодіоди й біполярні транзистори. Загальне струмове навантаження на всі лінії одного порту не повинна перевищувати 80 мА. Всі значення наведені для напруги живлення 5В.

AVR працюють у широкому діапазоні живлячих напруг від 2,7В до 6,0В. Струм споживання в активному режимі залежить від величини напруги живлення й частоти, на якій працює мікроконтролер, і становить менш 1мА для 500 кГц, 5...6 мА для 5Мгц і 8...9 мА для частоти 12 Мгц. AVR також можуть бути переведені програмним шляхом в один із двох режимів зниженого енергоспоживання. Перший – режим холостого ходу (IDLE), коли припиняє роботу тільки процесор і фіксується вміст пам'яті даних, а внутрішній генератор синхросигналів, таймери, система переривань і сторожовий таймер продовжують функціонувати. Струм споживання тут не перевищує 2,5 мА на частоті 12 Мгц. Другий – режим мікроспоживання (SLEEP), коли зберігається вміст регістрового файлу, але зупиняється внутрішній генератор синхросигналів. Вихід з режиму SLEEP можливий або по сигналі скидання, або від зовнішнього джерела переривання. При включеному сторожовому таймері струм споживання в цьому режимі становить близько 80 мкА, а при виключеному – менш 1мкА. (Всі вищенаведені значення справедливі для напруги живлення 5В).

Температурні діапазони роботи мікроконтролерів AVR – комерційний (0...70ºС) і індустріальний (-40...+85ºС).

З погляду програміста AVR являє собою 8-розрядний RISC мікроконтролер, що має швидкий Гарвардський процесор, пам'ять програм, пам'ять даних, порти вводу/виводу й интерфейсні схеми. Гарвардська архітектура AVR реалізує повний логічний і фізичний поділ не тільки адресних просторів, але й інформаційних шин для звертання до пам'яті програм і до пам'яті даних. Способи адресації й доступу до них також різні. Така побудова вже ближче до структури швидкісних цифрових сигнальних процесорів і забезпечує істотне підвищення продуктивності за рахунок:

а) одночасної роботи центрального процесора як з пам'яттю програм, так і з пам'яттю даних;

б) розширення до 16 біт розрядної сітки шини дані пам'яті програм. Наступним кроком на шляху збільшення швидкодії AVR є використання технології конвеєризації, внаслідок чого цикл "вибірка – виконання" команди може бути помітно скорочений, підвищуючи тим самим продуктивність процесора. Наприклад, у мікроконтролерів сімейства MCS51 коротка команда виконується за 12 тактів генератора (1 машинний цикл), протягом якого процесор послідовно зчитує код операції й виконує її. В PIC-контролерах фірми Microchip уже реалізована конвеєрна обробка. Коротка команда виконується в них протягом 8 періодів тактової частоти (2 машинних цикли). За цей час послідовно дешифрирується й зчитується код операції, виконується команда, фіксується результат і одночасно зчитується код наступної операції (конвеєр). Тому одна коротка команда в загальному потоці реалізується за 4 періоди тактової частоти або за один машинний цикл. У мікроконтролерах AVR теж використовується однорівневий конвеєр при звертанні до пам'яті програм і коротка команда в загальному потоці виконується, як і в PIC-контролерах, за один машинний цикл.

Головна ж відмінність полягає в тому, що цей цикл в AVR триває всього один період тактової частоти в порівнянні із чотирма в PIC.

Наступна відмітна риса архітектури мікроконтролерів AVR – регістровий файл швидкого доступу. Кожний з 32-х регістрів загального призначення довжиною 1 байт безпосередньо з'єднаний з арифметико-логічним пристроєм (ALU) процесора. Це означає, що в AVR існує 32 регістра-акумулятора. Це дозволяє в сполученні з конвеєрною обробкою виконувати одну операцію в ALU за один машинний цикл. Наприклад, два операнда витягають із регістрового файлу, виконується команда й результат записується назад у регістровий файл протягом тільки одного машинного циклу. Шість із 32-х регістрів файлу можуть використовуватися як три 16-розрядних покажчики адреси при непрямій адресації даних. Один із цих покажчиків застосовується також для доступу до таблиць перекодувань, записаних у пам'яті програм мікроконтролера. Використання трьох 16-бітних покажчиків істотно підвищує швидкість пересилання даних при роботі прикладної програми.

Під час переходів до виконання процедур обробки переривань або підпрограм поточний стан програмного лічильника зберігається в стеці. Тільки в AT90S1200 стек реалізований апаратно із глибиною вкладень, рівної 3. У всіх інших типах AVR мікроконтролерів стек формується програмно й розташовується в загальному адресному просторі оперативної пам'яті даних. 16-розрядний покажчик стека перебуває в загальному адресному просторі оперативної пам'яті й доступний для читання й запису.

Система команд AVR досить розвинена й нараховує 89 різних інструкцій. Майже всі команди мають фіксовану довжину в одне слово (16 біт), що дозволяє в більшості випадків поєднувати в одній команді й код операції, і операнд(и). Розрізняють п'ять груп команд AVR: умовного розгалуження, безумовного розгалуження, арифметичні й логічні операції, команди пересилання даних, команди роботи з бітами. По розмаїтості й кількості реалізованих інструкцій AVR більше схожі на CISC, чим на RISC процесори. Наприклад, в PIC-контролерів система команд нараховує від 33 до 58 різних інструкцій, а в MCS51 вона становить 111.

У цілому, архітектура AVR у сполученні з регістровим файлом і розширеною системою команд дозволяє в короткий термін створювати програми з дуже ефективним кодом як по швидкості його виконання, так і по компактності.

Програмні й апаратні засоби для нової платформи розроблялися паралельно із самими мікроконтролерами й містять у собі компілятори, внутрісхемні емулятори, відладчики, програматори, найпростіші відладочні плати-конструктори практично на будь-який смак.

Таким чином приведено переконливі доводи на користь обраної елементної бази. По достоїнству оцінено високу швидкість роботи й потужну систему команд AVR, наявність двох типів енергонезалежної пам'яті на одному кристалі й периферію, що розвивається. Немаловажну роль у цьому зіграла й відкрита політика Atmel у питанні розвитку різноманітних, доступних засобів підтримки розробок. Це дозволяє розроблювачам і виробникам електронної техніки сподіватися на збереження повноцінної підтримки для перспективної лінії AVR і в майбутньому, закладаючи мікроконтролери сімейства AT90S у свої нові вироби. У сполученні з усіма апаратними й програмними достоїнствами низька ціна на мікроконтролер з'явилася вирішальним фактором у виборі його.

Проектування друкованої плати контролера

Визначення загальних вимог до друкованої плати

По конструкції друковані плати (ДрП) діляться на наступні типи: однобічні (ОДрП), двосторонні (ДДрП) і багатошарові (БДрП). При виборі типу ДрП для розроблювальної конструкції варто враховувати техніко-економічні показники.

ОДрП являють собою діелектричну підставуз отворами, пазами, вирізами й т.п., на одній стороні якого виконаний провідний малюнок, а на іншій при складанні розміщають інтегральні мікросхеми (ІМС) і електрорадіоелементи (ЕР-Е).У зв'язку з обмеженою площею для трасування малюнка схеми такі ДрП застосовують для простих електронних пристроїв побутового й допоміжного призначення. Найбільш прості по конструкції й дешеві у

виготовленні ОДрП без металізованих отворів. Більше складні, але й більше надійні в експлуатації плати з металізованими за допомогою пістонів отворами.

ДДрП мають провідний малюнок на обох сторонах діелектричної підстави. Необхідні з'єднання друкованих провідників різних сторін ДДрП виконують за допомогою дротових перемичок, металізованих отворів, контактних площадок. Такі плати дозволяють реалізувати більш складні схеми й мають найбільш широке застосування при виготовленні вузлів електронних схем. Менш розповсюджені ДДрП на металевій підставі з нанесеним на нього електроізоляційним покриттям мають кращий тепловідвод, що істотно при великій потужності навісних елементів.

БДрП складаються із шарів, що чергуються, ізоляційного матеріалу й провідного малюнка. Між провідними шарами в структурі плат можуть бути або відсутствовати міжшарові з'єднання. Існує досить велика розмаїтість конструктивно-технологічних різновидів БДрП залежно від наявності й характеру міжшарових з'єднань. Найбільше поширення серед них одержали БДрП із металізацією наскрізних отворів, які не мають обмеження на число шарів (оптимальне число до 12) і придатні для установки елементів як зі штировими, так і із планарными виводами. Перевага використання БДрП цього типу обумовлена порівняно високою щільністю монтажу, гарною якістю міжшарових з'єднань, задовільною ремонтоздатністю, можливістю автоматизації й механізації як процесів виготовлення самих плат, так і складання на них вузлів.

Залежно від складності реалізованої електричної схеми й застосовуваної елементної бази вибирають конструктивне виконання плати, число шарів і щільність провідного малюнка схеми. При виборі числа шарів плати варто мати на увазі, що найменш трудомісткі й прості у виготовленні ОДрП без металізованих отворів і приблизно рівні по витратах ОДрП і ДДрП про металізованими отворами. Найбільш складні й трудомісткі у виготовленні БДрП, число шарів яких обмежено гранично припустимим співвідношенням між діаметром металізованих отворів і товщиною плати (не менш 0,33). Орієнтовно співвідношення трудомісткості виготовлення ОДрП без металізованих отворів, ДДрП і БДрП становить 1:4:20.

По точності виконання елементів (відповідно до ДСТ 23751 – 86) конструкції ДрП діляться на п'ять класів. Клас точності вказують на кресленні ДрП. Під елементами конструкції ДрП маються на увазі елементи провідного малюнка. Друковані плати 1-го й 2-го класів точності найбільш прості у виконанні, надійні в експлуатації й мають мінімальну вартість. Друковані плати 3-го, 4-го й 5-го класів точності вимагають використання високоякісних матеріалів, інструмента й устаткування, обмеження габаритних розміряний, а в окремих випадках і особливих умовах при виготовленні.

Габаритні розміри ДрП повинні відповідати ДСТ 10317 – 79. Розміри кожної сторони ДрП повинні бути кратними:

– 2,5 мм – при довжині до 100 мм;

– 5,0 мм – при довжині до 350 мм;

– 10,0 мм – при довжині більше 350 мм.

Рекомендується розробляти ДрП простої прямокутної форми. Конфігурацію, відмінну від прямокутної, варто застосовувати тільки в технічно обґрунтованих випадках. Співвідношення лінійних розмірів сторін ДрП повинне бути не більше 3:1. Допускається збільшення цього співвідношення за узгодженням із замовником. Згідно ОСТ 25.931 – 80 рекомендуються розміри ДрП на знову розроблювальні й модернизуємі вироби. Максимальні розміри ДрП і (або) робочого поля групової установки повинні бути не більше 470 мм. Допуски на лінійні розміри сторін ДрП повинні відповідати ДСТ 25346 – 82 і ДСТ 25347 – 82. Розміри контуру, що сполучаються, ДрП повинні мати граничні відхилення по 12 квалітету. Розміри контуру, що не сполучаються – по 14 квалітету відповідно до ДСТ 25347 – 82 (СТ СЕВ 145 – 75).

Товщина друкованої плати визначається товщиною вихідного матеріалу й вибирається залежно від використовуваної елементної бази й діючих механічних

навантажень. Кращими значеннями номінальних толщин одне- і двосторонніх друкованих плат є 0,8; 1,0; 1,5; 2,0 мм.

Фольговані матеріали являють собою шаруваті пресовані пластинки, виготовлені на основі папери (гетинакс) або тканини зі скляного волокна (стеклотекстоліт), просочені термореактивними сполучних і облицьовані з однієї або двох сторін мідною електролітичною фольгою, що оксидована із внутрішньої сторони для матеріалів звичайного виконання або покрита плівкою хрому для гальваностойких матеріалів.

Матеріал для друкованої плати вибирають за ДСТ 10316 – 78 або технічним умовам. Позначення марок, наприклад, СФ-1(2)-35 означають, що промисловістю випускаються як однобічні СФ- 1-35, так і двосторонні СФ- 2-35 фольговані матеріали із зазначеними толщинами фольги й матеріалу з фольгою. Букви Н и Г у позначенні марки матеріалу свідчать про підвищений нагревостійкости (до +100°С) і гальваностійкости.

Фольговані матеріали призначені для роботи в наступних умовах:

– гетинакс без додаткового вологозахисту призначений для виготовлення ДрП, на які в процесі роботи може впливати навколишнє середовище, що характеризується відносною вологістю повітря 45 – 75% при температурі 15 – 35°С;

– гетинакс із додатковим вологозахистом і стеклотекстоліт всіх марок призначені для виготовлення ДрП, на які в процесі роботи може впливати навколишнє середовище, що характеризується відносною вологістю повітря до 98% при температурі не вище 40°С;

– фольговані матеріали у вигляді ДрП повинні допускати вплив температури до 60°С. Фольговані матеріали виготовляються аркушами наступних номінальних розмірів:

– гетинакс всіх марок і толщин – 2440х1040; 1190х1040, 800х900 мм;

– стеклотекстоліт всіх марок і толщин – 1190х1010, 1010х890, 1010х840, 910х890, 640х490.

Умовні позначки фольгованих матеріалів – за ДСТ 26246 – 84. Для матеріалів вищого й першого сортів додатково повинне бути зазначене “в.с.” або “1с.”. Приклад умовної позначки фольгованого стеклотекстоліта вищого сорту товщиною 1,5 мм, облицьованого із двох сторін мідної електролітичної гальваностійкою фольгою товщиною 35 мкм: СФ- 2-35Г-1,5 в. с. ДСТ 10316-78.

Для ДрП, призначених для експлуатації в умовах першої групи твердості по ОСТ 4.077.000 (табл. 6), рекомендується застосовувати матеріали на основі паперу, для другої, третьої й четвертої груп твердості – на основі стеклоткани.

Методи виготовлення друкованих плат

Відома велика кількість технологічних варіантів виготовлення друкованих плат. Найбільш широке поширення одержали наступні методи:

– хімічний метод. Полягає в тому, що на мідну фольгу, приклеєну до діелектрика з однієї або із двох сторін, наносять кислотостійкою фарбою малюнок розташування друкованих провідників. Наступним травленням віддаляється мідь із незахищених ділянок і на діелектрику залишається схема провідників. Найпоширенішими варіантами цього способу є фотохімічний, сітчасто-хімічний, офсетно-хімічний, які розрізняються способом нанесення захисного шару. Достоїнства цього методу: достатня простота, легко піддається автоматизації. Недоліки: необхідність застосування металевих втулок при двосторонньому монтажі й непродуктивна витрата міді.

– електрохімічний метод. Полягає в нанесенні на плату кислостійкою фарбою негативного малюнка провідників. Нанесення малюнка відбувається з наступним нарощуванням шаруючи міді. Основна перевага електрохімічного методу полягає в можливості металізації отворів одночасно з одержанням провідників. Недоліком є низька здатність, що розсіює (0,5 ¸ 0,8 мм) і низька міцність зчеплення провідників з підставою. Електрохімічний метод знаходить застосування головним чином у досвідченому й дрібносерійному виробництві при виготовленні двосторонніх плат з більшим числом переходів.

– комбінований метод. Полягає в одержанні провідників шляхом травлення фольгованого діелектрика й металізацією отворів електрохімічним способом. Сутність методу травлення фольгованого матеріалу з наступним втравлюванням фольги з окремих ділянок плати. Цей метод забезпечує одержання чітких ліній провідників друкованої схеми. Він характеризується меншою трудомісткістю в порівнянні з електрохімічним методом. Друковані плати більш надійні, тому що при цьому діелектрик перебуває в більше сприятливій умові, тому що фольга охороняє її від дії електроліту. Комбінований метод широко застосовується при виготовленні двосторонніх друкованих плат.

Після механічної обробки плата перевіряється на наявність тріщин на краях плати й в отворах, відшарування друкованих провідників у зоні отворів. Друковані провідники повинні бути чіткими. Цілісність електричних кіл установлюється методом прозвонки.

Деталі на плату встановлюють вручну, пайку монтажних з'єднань виконують паяльником потужністю 35Вт приспіваємо ПЗС – 60. Застосовують тільки безкислотні флюси. Якість пайки перевіряють зовнішнім оглядом.

Для захисту провідників і поверхні підстави плати від впливу припою використовують резистивні маски на основі епоксидної смоли, сухого плівкового резисту.

Опис конструкції друкованої плати

Конструкція розробленого контролера одноплатна. Через велику кількість пересічних провідників плата двостороння. Основний крок координатної сітки приймаємо 2,5 мм. Центри всіх отворів розташовуються на друкованій платі у вузлах координатної сітки. Діаметр монтажних і перехідних отворів – 0,8 мм.

Друковані провідники зображуються у вигляді відрізків ліній, що збігаються з лініями координатної сітки або під кутом кратним 15°. Друковані провідники виконані однакової ширини – 0,5 мм із допуском 0,03 мм. Провідники покрити сплавом “Розі”. Маркування на платі виконувати травленням шрифтом 2.5 ПЗ ІО.010.007, у вузьких місцях шрифтом 2.

Обґрунтування щодо вибору мови програмування

Програма AVR-мікроконтролера – це розміщена в пам'яті програм послідовність команд, кожна з яких складається із двійкових кодів операцій і двійкових адрес операндів.

Система команд AVR-мікроконтролерів включає команди арифметичних і логічних операцій, команди передачі даних, команди, що управляють послідовністю виконання програми, і команди операцій з бітами. Для зручності написання й аналізу програм всім операціям із системи команд, крім двійкового коду, зіставлені мнемокоди асемблера (символічні позначення операцій), які використовуються при створенні вихідного тексту програми.

Спеціальні програми-транслятори потім переводять символічні позначення у двійкові коди.

По вихідному тексті програми, написаної мовою асемблера, можна визначити час її виконання й обсяг програмної пам'яті, необхідний для її зберігання. Програмування мовою асемблера є прекрасним засобом для того, щоб відчути архітектуру мікроконтролера й логікові його роботи. Цьому також сприяє та обставина, що транслятори з мови асемблера поширюються фірмою Атмел безкоштовно й доступні всім бажаючої.

Крім мови асемблера, для програмування мікропроцесорів, що вбудовуються, широке поширення одержали мови програмування високого рівня: C и BASIC, Delphi. Вони надають програмістові такий же легкий доступ до всіх ресурсів мікроконтролера, як і асемблер, але, разом з тим, дають можливість створювати добре структуровані програми, знімають із програміста турботу про розподіл пам'яті даних і містять великий набір бібліотечних функцій для виконання стандартних операцій.

Вся енергонезалежна пам'ять AVR-мікроконтролерів розміщається всередині кристала й складається з електрично програмувальних FLASH-пам'яті програм і EEPROM-пам'яті даних.

Так як всі команди AVR являють собою 16-розрядні слова, FLASH- пам'ять організована як послідовність 16-розрядних осередків і має ємність від 512 слів до 64K слів

залежно від типу кристала. В FLASH-пам'ять, крім програми, можуть бути записані постійні дані, які не змінюються під час функціонування мікропроцесорної системи. Це різні константи, таблиці знакогенераторів, таблиці лінеаризації датчиків і т.і. Достоїнством технології FLASH є високий ступінь упакування, а недоліком те, що вона не дозволяє стирати окремі осередки. Тому завжди виконується повне очищення всієї пам'яті програм. При цьому гарантується, як мінімум 1000 циклів перезапису FLASH-пам'яті AVR.

EEPROM блок пам'яті, що стирається електрично, AVR призначений для зберігання енергонезалежних даних, які можуть змінюватися безпосередньо на об'єкті. Це калібровані коефіцієнти, різні установки, конфігураційні параметри системи. EEPROM-пам'ять має меншу ємність (від 64 байт до 4К байт), але має можливість побайтного перезапису осередків, що може відбуватися як під керуванням зовнішнього процесора, так і під керуванням властиво AVR-мікроконтролера під час його роботи із програми.

В енергонезалежній пам'яті AVR є декілька спеціалізованих біт [7].

LOCK-біти (LB1, LB2) призначені для захисту програмної інформації, що втримується в FLASH-пам'яті. Можливі режими захисту перераховані в таблиці 3.1. Запрограмувавши біти захисту, стерти їх можна лише під час очищення FLASH -пам'яті, що знищує й всю програму. FUSE-біти дозволяють задавати деякі конфігураційні особливості мікроконтролера (див. таблицю 3.2).

Мікроконтролери AT90S1200 мають FUSE-біти SPIEN і RCEN. Всі інші типи classicAVR конфігуруються за допомогою FUSE-біт SPIEN і FSTRT. MegaAVR мають чотири FUSE-біти: SPIEN, SUT0, SUT1 і EESAVE. Три енергонезалежних Signature-байти служать для ідентифікації типу кристала, програмуються на фабриці й доступні тільки для читання.

Таблиця 1 – Режими захисту програми

Режим	Стан Lock-біт		Тип захисту
	LB1	LB2	
1	1	1	Захист відсутній
2	0	1	Заборона програмування Flash
3	0	0	Заборона як програмування, так і читання Flash

Таблиця 2 – Призначення FUSE-біт

Fuse-біт (значення за замовчуванням)	Значення	Режим роботи AVR
0		AVR тактується внутрішнім RC-генератором. (робота AVR без зовнішніх елементів)
RCEN (1)	1	Тактування за допомогою зовнішнього кварцового резонатора або генератора
	0	Дозвіл послідовного програмування через SPI інтерфейс
SPIEN (0)	1	Заборона послідовного програмування через SPI інтерфейс
	0	Затримка старту AVR після скидання ~ 0.25мс
FSTRT (1)	1	Затримка старту AVR після скидання ~ 16 мс
	00	Затримка старту AVR після скидання ~ 5 мс
	01	Затримка старту AVR після скидання ~ 0.5 мс
SUT 0/1 (11)	10	Затримка старту AVR після скидання ~ 4.0мс
	11	Затримка старту AVR після скидання ~ 16 мс
EESAVE (1)	0	EEPROM не стирається під час циклу очищення енергонезалежної пам'яті
	1	EEPROM стирається під час циклу очищення

		енергонезалежної пам'яті

Різноманітні способи програмування AVR-мікроконтролерів забезпечують простий і зручний доступ до внутрішньої енергонезалежної пам'яті у всіх можливих ситуаціях програмування кристала.

Для енергонезалежних FLASH і EEPROM блоків AVR передбачені паралельний і послідовний способи програмування, які виконуються під керуванням зовнішнього процесора, а для EEPROM-пам'яті також можливий спосіб програмного перезапису під керуванням AVR. LOCK-біти можуть програмуватися як паралельно, так і послідовно. FUSE-біти в молодших моделей AVR можуть програмуватися тільки послідовно, а в старших – і паралельно, і послідовно.

Паралельне програмування енергонезалежної пам'яті використовує велику кількість виводів мікроконтролера й виконується на спеціальних програматорах. Таке програмування зручно, коли при масовому виробництві необхідно "прошивати" велику кількість кристалів.

Послідовне програмування може виконуватися прямо в мікропроцесорній системі (In System Programming) через послідовний SPI-інтерфейс, що використовує всього чотири виводи AVR-мікроконтролера. Ця нова можливість є дуже важливою, так як дозволяє обновляти програмне забезпечення у вже функціонуючій мікропроцесорній системі.

Розробка структурної схеми

В процесі практичної реалізації теоретичних принципів розробки системи, розглянутих вище, була розроблена структурна схема (рисунок 1) в якій були розглянуті аспекти побудови системи керування тепломережею.

Розглядаючи її можно побачити що система розбита на дві основних частини апаратна частина (винесена на плакат «Функціональна схема апаратної частини») та програмна частина (винесена на плакат «Функціональна схема програмної частини»), взаємозв’язок котрих відбувається за допомогою інтерфейсу RS-232 та інтерфейсу Windows.

Вхідні дані подають поточне значення спостерігаємих об`єктів (тепломереж). Спостерігання відбувається за допомогою датчиків тиску температури, вологості та інших датчиків.

Головним модулем апаратної частини являється мікроконтролер AT90S1200, якій керує вхідними потоками і подає дані на інтерфейс RS-232. Головним модулем у програмної частини є розроблене у магістерській роботі програмне забезпечення.

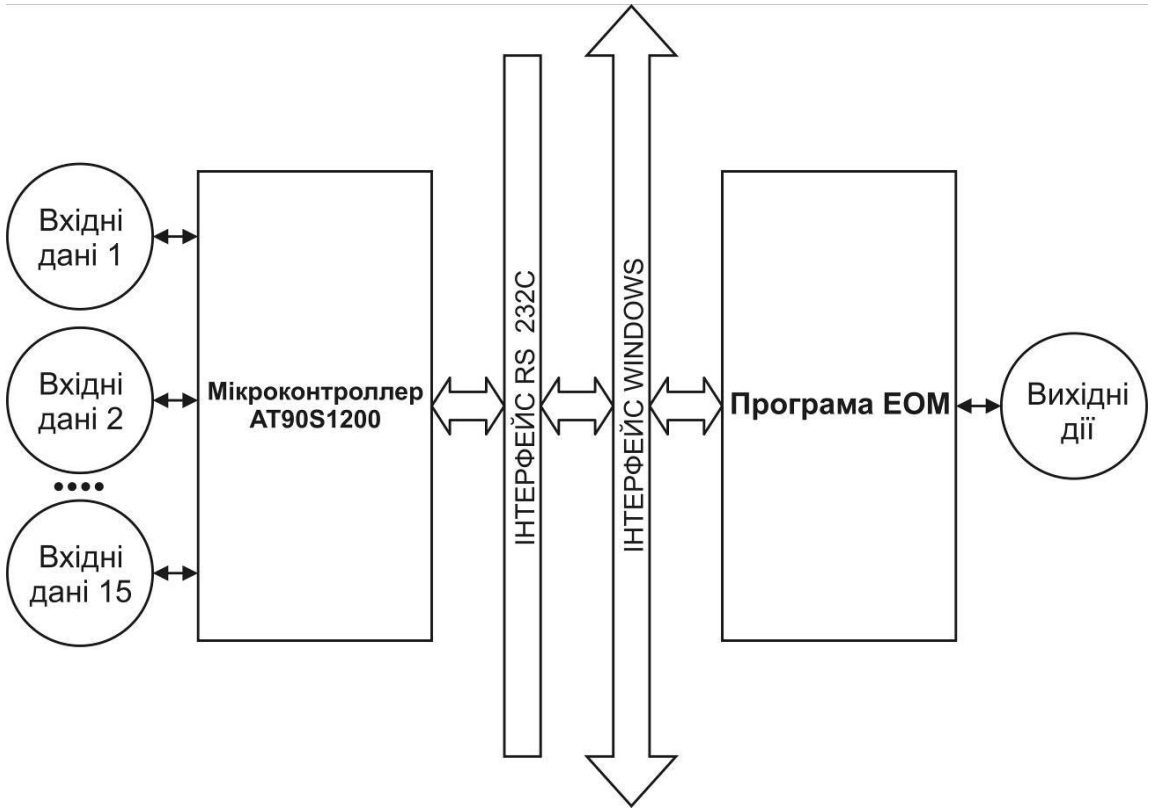


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування комунальних теплових мереж.

Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем керування комунальних теплових мереж. Досліджена система керування комунальних теплових мереж. На основі отриманих результатів досліджень створена програмна реалізація системи керування комунальних теплових мереж. Розроблені алгоритми дозволяють успішно вирішувати завдання керування комунальних теплових мереж. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
2. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
3. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
4. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
5. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем

/ А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
8. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
9. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
10. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.

УДК 004

Є. Теніченко, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ФЛЕШ-МАСИВІВ PURE STORAGE ДЛЯ ЗБЕРІГАННЯ ДАНИХ BIG DATA

У статті розроблено програмне забезпечення, яке призначено для системи флеш-масивів Pure Storage для зберігання даних Big Data. Метою розробки є дослідження та програмна реалізація системи флеш-масивів Pure Storage для зберігання даних Big Data. Об’єктом дослідження є процес флеш-масивів Pure Storage для зберігання даних Big Data. Предметом дослідження є методи флеш-масивів Pure Storage для зберігання даних Big Data. Методи дослідження базуються на методах теорії Big Data, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи флеш-масивів Pure Storage для зберігання даних Big Data. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, флеш-масиви, Pure Storage, Big Data

Постановка проблеми. Флеш-масиви стають основним носієм даних: продажі жорстких дисків падають, а флеш-накопичувачів ростуть. В 2020 році за даними IDC поставки гібридних масивів перевершили продажу дискових систем, а цього року, як очікується, їх обійдуть і «чисті» флеш-масиви (All-Flash Array, AFA). Серед законодавців мод на цьому ринку – компанія Pure Storage, що от уже протягом останніх п'яти років Gartner відносить до числа лідерів у цьому ключовому сегменті ринку систем зберігання даних.

Компанія Pure Storage, як заявляється, – самий швидко зростаючий єдиноріг в історії: рубіж в 1 млрд доларів компанія переборола через 8 років після свого створення. Ще більш швидкими темпами росту міг би похвастатися інший стартап в області флеш-масивів, ізраїльська компанія XtremeIO – їй удалося досягти обсягу продажів своєї продукції в 1 млрд доларів усього за 6 років, але на той момент компанія вже три роки як входила до складу EMC.

Pure Storage продовжує нарощувати продажі, причому навіть швидше, ніж раніше. За підсумками II кварталу 2021-го фінансового року її оберт виріс на 37% у порівнянні з аналогічним кварталом попереднього року. Тільки за останній рік число клієнтів збільшилося майже на 40% і перевищило 5000 компаній. У Європі продажу масивів щороку практично подвоюються (середньорічний ріст 98%). Як очікується, за результатами 2021 фінансового року продажу досягнуть 1, 35-1,38 млрд доларів.

Завдяки високому коефіцієнту стиску даних (3, 5-3,8:1) дані обсягом у кілька сотень терабайт удалося розмістити в системі висотою 5U. Це дозволяє відмовитися від необхідності розширення існуючого ЦОД.

Окремо потрібно відмітити те, що в Pure Storage технічна підтримка надається в тому числі й українською мовою, причому в компанії немає підтримки першого рівня – звернення відразу направляється інженерові. Це виявляється можливо завдяки високій надійності масивів. У середньому по мирі в 98% масивів 100-процентний показник безперервної експлуатації. Це досягається в тому числі за рахунок відновлення не тільки програмного, але й апаратного забезпечення, включаючи контролери, без зупинок. Поки всі поставлені в Україну системи працюють без простоїв (uptime 100%).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи флеш-масивів Pure Storage для зберігання даних Big Data

Мета й завдання дослідження Метою роботи є дослідження та програмна реалізація системи флеш-масивів Pure Storage для зберігання даних Big Data.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем флеш-масивів Pure Storage для зберігання даних Big Data.
– Дослідження системи флеш-масивів Pure Storage для зберігання даних Big Data.
– Програмна реалізація системи флеш-масивів Pure Storage для зберігання даних Big Data.

Об'єктом дослідження є процес флеш-масивів Pure Storage для зберігання даних Big Data.

Предметом дослідження є методи флеш-масивів Pure Storage для зберігання даних Big Data.

Методи дослідження базуються на методах теорії Big Data, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Визначальними характеристиками для Big Data є, крім їхнього фізичного обсягу, і інші, що підкреслюють складність завдання обробки й аналізу цих даних. Набір ознак VVV (volume, velocity, variety – фізичний обсяг, швидкість приросту даних і необхідності їхньої швидкої обробки, можливість одночасно обробляти дані різних типів) був вироблений компанією Meta Group в 2001 році з метою вказати на рівну значимість керування даними по всім трьох аспектах.

Надалі з'явилися інтерпретації із чотирма V (додавалася veracity – вірогідність), п'ятьома V (viability – життєздатність і value – цінність), родина V (variability – мінливість і visualization – візуалізація). Але компанія IDC, наприклад, інтерпретує саме четверте V як value (цінність), підкреслюючи економічну доцільність обробки більших обсягів даних у відповідних умовах.[5]

Виходячи з вищенаведених визначень, основні принципи роботи з Big Data такі:

1. **Горизонтальна масштабованість**. Це – базовий принцип обробки Big Data. Як уже говорилося, Big Data з кожним днем стає усе більше. Відповідно, необхідно збільшувати кількість обчислювальних вузлів, по яких розподіляються ці дані, причому обробка повинна відбуватися без погіршення продуктивності.

2. **Відказостійкість**. Цей принцип випливає з попередні. Оскільки обчислювальних вузлів у кластері може бути багато (іноді десятки тисяч) і їхня кількість, не виключена, буде збільшуватися, зростає й імовірність виходу машин з ладу. Методи роботи з Big Data повинні враховувати можливість таких ситуацій і передбачати превентивні міри.

3. **Локальність даних**. Так як дані розподілені по великій кількості обчислювальних вузлів, то, якщо вони фізично перебувають на одному сервері, а обробляються на іншому, витрати на передачу даних можуть стати невиправдано великими. Тому обробку даних бажано проводити на тій же машині, на якій вони зберігаються.

Ці принципи відрізняються від тих, які характерні для традиційних, централізованих, вертикальних моделей зберігання добре структурованих даних. Відповідно, для роботи з Big Data розробляють нові підходи й технології.

Технології й тенденції роботи з Big Data

Споконвічно в сукупність підходів і технологій включалися засоби масово-паралельної обробки невиразно структурованих даних, такі як СУБД NoSQL, алгоритми MapReduce і засобу проекту Hadoop. Надалі до технологій Big Data стали відносити й інші рішення, що забезпечують подібні по характеристиках можливості по обробці надвеликих масивів даних, а також деякі апаратні засоби.

– **MapReduce** – модель розподілених паралельних обчислень у комп'ютерних кластерах, представлена компанією Google. Відповідно до цієї моделі застосунок розділяється на велику кількість однакових елементарних завдань, виконуваних на вузлах кластера й потім зводяться природно в кінцевий результат.

– **NoSQL** (від англ. Not Only SQL, не тільки SQL) – загальний термін для різних нереляційних баз даних і сховищ, не позначає яку-небудь одну конкретну технологію або продукт. Звичайні реляційні бази даних добре підходять для досить швидких і однотипних запитів, а на складні й гнучко побудованих запитах, характерних для Big Data, навантаження перевищує розумні межі й використання СУБД стають неефективним.

– **Hadoop** – вільно розповсюджуваний набір утиліт, бібліотек і фреймворк для розробки й виконання розподілених програм, що працюють на кластерах із сотень і тисяч вузлів. Вважається однією з основних технологій Big Data.

– **R** – мова програмування для статистичної обробки даних і роботи із графікою. Широко використовується для аналізу даних і фактично став стандартом для статистичних програм.

– **Апаратні рішення**. Корпорації Teradata, EMC і інші пропонують апаратно-програмні комплекси, призначені для обробки Big Data. Ці комплекси поставляються як готові до установки телекомунікаційні шафи, що містять кластер серверів і керуюче програмне забезпечення для масово-паралельної обробки. Сюди також іноді відносять апаратні рішення для аналітичної обробки в оперативній пам'яті, зокрема, апаратно-програмні комплекси Hana компанії SAP і комплекс Exalytics компанії Oracle, незважаючи на те, що така обробка споконвічно не є масово-паралельної, а обсяги оперативної пам'яті одного вузла обмежуються декількома терабайтами.

Консалтингова компанія McKinsey, крім розглянутих більшістю аналітиків технологій NoSQL, MapReduce, Hadoop, R, включає в контекст застосовності для обробки Big Data також технології Business Intelligence і реляційні системи керування базами даних з підтримкою мови SQL.

Методи й техніки аналізу Big Data

Міжнародна консалтингова компанія McKinsey, що спеціалізується на рішенні завдань, зв'язаних зі стратегічним керуванням, виділяє 11 методів і технік аналізу, застосовних до Big Data.

– **Методи класу Data Mining** (видобуток даних, інтелектуальний аналіз даних, глибинний аналіз даних) – сукупність методів виявлення в даних раніше невідомих, нетривіальних, практично корисних знань, необхідних для прийняття рішень. До таких методів, зокрема, відносяться навчання асоціативним правилам (association rule learning), класифікація (розбивка на категорії), кластерний аналіз, регресійний аналіз, виявлення й аналіз відхилень і ін.

– **Краудсорсинг** – класифікація й збагачення даних силами широкого, невизначеного кола осіб, що виконують цю роботу без вступу в трудові відносини

– **Змішання й інтеграція даних** (data fusion and integration) – набір технік, що дозволяють інтегрувати різнорідні дані з різноманітних джерел з метою проведення глибинного аналізу (наприклад, цифрова обробка сигналів, обробка природної мови, включаючи тональний аналіз, і ін.)

– **Машинне навчання**, включаючи навчання із учителем і без учителя – використання моделей, побудованих на базі статистичного аналізу або машинного навчання для одержання комплексних прогнозів на основі базових моделей

– **Штучні нейронні мережі**, мережний аналіз, оптимізація, у тому числі генетичні алгоритми (genetic algorithm – евристичні алгоритми пошуку, використовувані для рішення завдань оптимізації й моделювання шляхом випадкового підбора, комбінування й варіації шуканих параметрів з використанням механізмів, аналогічних природному добору в природі)

– **Розпізнавання образів**.

– Прогнозна аналітика.

– Імітаційне моделювання (simulation) – метод, що дозволяє будувати моделі, що описують процеси так, як вони проходили б у дійсності. Імітаційне моделювання можна розглядати як різновид експериментальних випробувань

– **Просторовий аналіз** (spatial analysis) – клас методів, що використовують топологічну, геометричну й географічну інформацію, що витягається з даних

– **Статистичний аналіз** – аналіз тимчасових рядів, A/ B-Тестування (A/B testing, split testing – метод маркетингового дослідження; при його використанні контрольна група елементів рівняється з набором тестових груп, у яких один або кілька показників були змінені, для того щоб з'ясувати, які зі змін поліпшують цільовий показник)

– **Візуалізація аналітичних даних** – подання інформації у вигляді рисунків, діаграм, з використанням інтерактивних можливостей і анімації як для одержання результатів, так і для використання в якості вихідних даних для подальшого аналізу. Дуже важливий етап аналізу Big Data, що дозволяє представити найважливіші результати аналізу в найбільш зручному для сприйняття виді.

Big Data в промисловості

Відповідно до звіту компанії McKinsey «Global Institute, Big data: The next frontier for innovation, competition, and productivity», дані стали таким же важливим фактором виробництва, як трудові ресурси й виробничі активи. За рахунок використання більших дані компанії можуть одержувати відчутні конкурентні переваги. Технології Big Data можуть бути корисними при рішенні наступних завдань:

- прогнозування ринкової ситуації;
- маркетинг і оптимізація продажів;
- удосконалювання продукції;
- прийняття управлінських рішень;
- підвищення продуктивності праці;
- ефективна логістика;
- моніторинг стану основних фондів.

На виробничих підприємствах Big Data генеруються також внаслідок впровадження технологій Промислового інтернету речей. У ході цього процесу основні вузли й деталі верстатів і машин забезпечуються датчиками, виконавчими пристроями, контролерами й, іноді, недорогими процесорами, здатними робити граничні (мрячні) обчислення. У ході виробничого процесу здійснюється постійний збір даних і, можливо, їхня попередня обробка (наприклад, фільтрація). Аналітичні платформи обробляють ці масиви інформації в режимі реального часу, представляють результати в найбільш зручному для сприйняття виді й зберігають для подальшого використання. На основі аналізу отриманих даних робляться виводи про стан устаткування, ефективності його роботи, якості продукції, що випускається, необхідності внесення змін у технологічні процеси й т.д.

Завдяки моніторингу інформації в режимі реального часу персонал підприємства може:

- скорочувати кількість простоїв;
- підвищувати продуктивність устаткування;
- зменшувати витрати на експлуатацію устаткування;

– запобігати нещасні випадки.

Останній пункт особливо важливий. Наприклад, оператори, що працюють на підприємствах нафтохімічної промисловості, одержують у середньому близько 1500 аварійних повідомлень у день, тобто більше одного повідомлення в мінуту. Це приводить до підвищеної утоми операторів, яким доводиться постійно приймати миттєві рішення про те, як реагувати на той або інший сигнал. Але аналітична платформа може відфільтрувати другорядну інформацію, і тоді оператори одержують можливість зосередитися в першу чергу на критичних ситуаціях. Це дозволяє їм більш ефективно виявляти й запобігати аварії й, можливо, нещасні випадки. У результаті підвищуються рівні надійності виробництва, промислової безпеки, готовності технологічного устаткування, відповідності нормативним вимогам.

Крім того, за результатами аналізу Big Data можна розраховувати строки окупності устаткування, перспективи зміни технологічних режимів, скорочення або перерозподіли обслуговуючого персоналу – тобто приймати стратегічні рішення щодо подальшого розвитку підприємства.

Сучасне Big Data рішення складається з декількох блоків, що вимагають спільної роботи команд із різними компетенціями й інтеграції набору Open-source і пропрієтарних програмних компонентів:

1. Технічне рішення по збору, зберіганню й обробці більших обсягів даних, позначене на схемі як Big Data Tools. Таке рішення, як правило, будується на основі стека Hadoop, так як він представляє гарний баланс між вартістю, надійністю й функціональністю.

2. Просунутий аналіз даних з використанням методів науки про даний (Data Science) і алгоритмів машинного навчання

3. Візуалізація Big Data, а також створення інтерактивних звітів для керівництва компанії, співробітників і клієнтів (Business Intelligence). При цьому використовувана аналітична платформа повинна бути сумісна зі стеком Hadoop

Інтеграція платформи системи флеш-масивів Pure Storage для зберігання даних зі стеком Big Data

Big Data рішення будуються на базі open-source технологічного стека Hadoop. Для рішення завдань візуалізації, моделювання й інтерактивного аналізу даних у такі рішення інтегрується аналітична платформа системи флеш-масивів Pure Storage для зберігання даних. Також можлива інтеграція із уже існуючими системами Big Data.

Складання рішення Hadoop вимагають глибокої експертизи. Фахівці мають необхідні знання для побудови оптимальної архітектури аналітичного Big Data рішення й використовують наступні технології, що забезпечують роботу в реальному масштабі часу в умовах підприємства:

1. Багаторівнева сегментація даних. Наприклад, самий часто затребуваний, але щодо невеликий обсяг даних зберігається в базі даних у пам’яті, платформи системи флеш-масивів Pure Storage для зберігання даних, а повний обсяг даних – в розподіленому файловому сховищі.

2. Кешовані на різних рівнях системи.

3. λ-архітектура для забезпечення відновлення всіх рівнів даних у реальному часі.

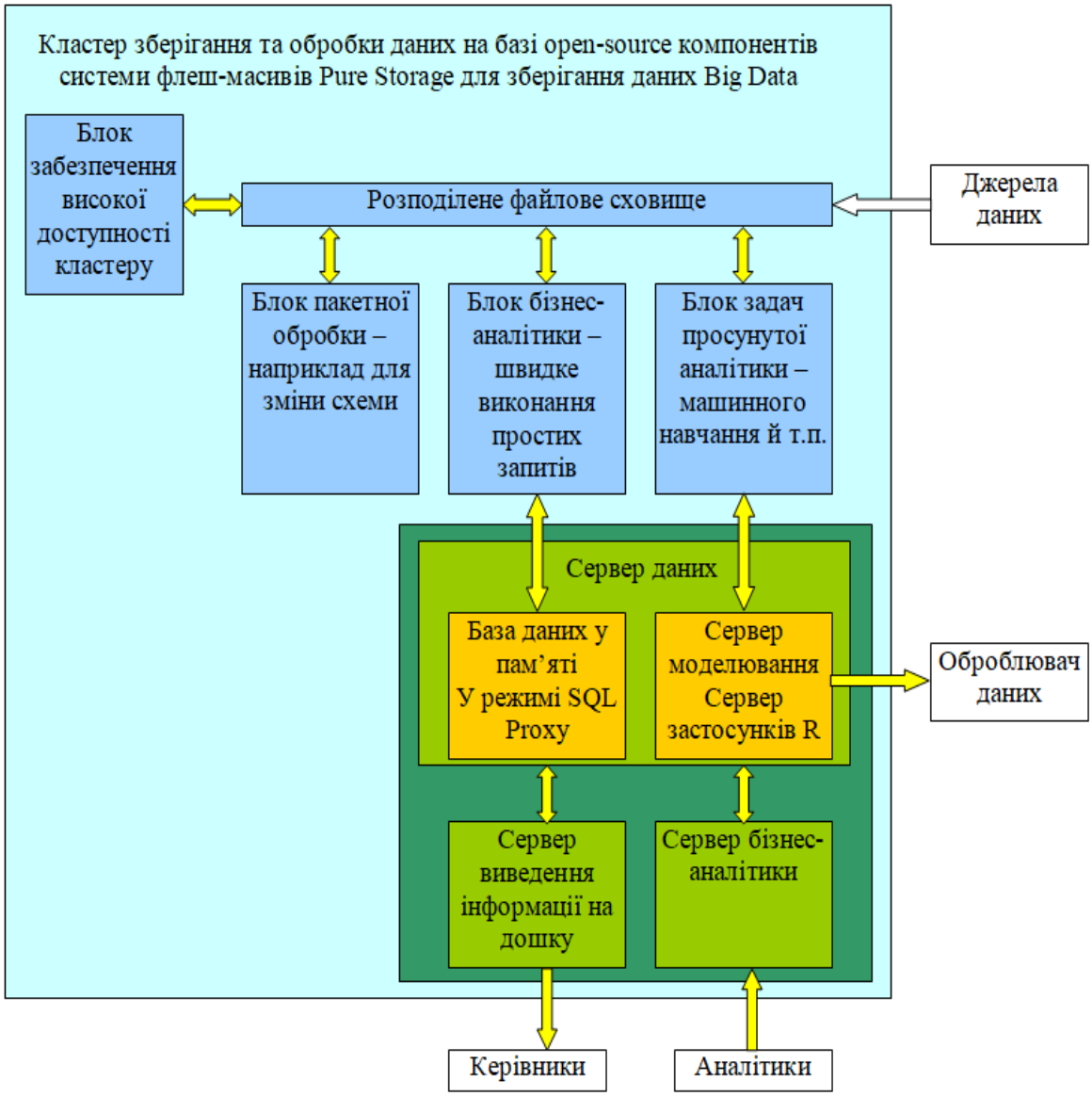


Рисунок 1 – Структурна схема системи

Просунутий аналіз даних і моделювання з використанням методів Data Science

Інструменти Data Science – це комп'ютерні методи й алгоритми, що дозволяють застосувати розділи математичної статистики, теорії ймовірностей, чисельних методів оптимізації дискретного аналізу для виділення знань із даних.

– Метричні методи класифікації й регресії.
– Логічні методи класифікації.
– Критерії вибору моделей і методи відбору ознак.
– Градієнтні методи навчання.
– Метод опорних векторів.
– Багатомірна лінійна регресія.
– Нелінійна регресія.
– Прогнозування тимчасових рядів.
– Байєсовська теорія класифікації.
– Логістична регресія. Поділ суміші розподілів.
– Кластеризація.
– Нейронні мережі.
– Лінійні композиції, бустинг.

– Евристичні, стохастичні, нелінійні композиції.
– Ранжирування.
– Пошук асоціативних правил.
– Завдання із частковим навчанням.
– Колаборативна фільтрація.
– Тематичне моделювання.
– Навчання з підкріпленням.

За допомогою методів Data Science можна оптимізувати виробничі процеси без значних капітальних витрат. Важливою особливістю проектів Data Science є дослідницький характер, до проведення серйозного аудита даних неможливо дати точний висновок про досяжність тих або інших бізнес-цілей. Для рішення цієї проблеми системи флеш-масивів Pure Storage для зберігання даних пропонує підхід, що дозволяє максимально знизити ризики клієнта, що сформований у відповідності з наступними принципами.

Висновки. У статті наведене теоретичне узагальнення й рішення наукового завдання дослідження методів флеш-масивів Pure Storage для зберігання даних Big Data. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем флеш-масивів Pure Storage для зберігання даних Big Data. Досліджена система флеш-масивів Pure Storage для зберігання даних Big Data. На основі отриманих результатів досліджень створена програмна реалізація системи флеш-масивів Pure Storage для зберігання даних Big Data. Розроблені алгоритми дозволяють успішно вирішувати завдання флеш-масивів Pure Storage для зберігання даних Big Data. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

11. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
12. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
13. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
14. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
15. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
16. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
17. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку ІТ-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
18. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
19. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.

20. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 004

О. Тарасов, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ В БІЗНЕС-ПРОЦЕСИ ПІДПРИЄМСТВА

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Метою розробки є дослідження та програмна реалізація системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Об'єктом дослідження є процес інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Предметом дослідження є методи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерні науки, хмарні технології, бізнес-процеси

Постановка проблеми. Традиційний проектний бізнес поступово міняється внаслідок поширення таких підходів як пропозиція інфраструктури у вигляді сервісу. У теж час конкуренція на ринку системної інтеграції посилюється в результаті прагнення великих вендорів працювати із замовниками прямо, пропозиції IT-послуг на базі власних ЦОД з боку телекомунікаційних операторів і інших факторів. На це накладаються нерадісні перспективи стагнації українського проектного ринку. Все це змушує системних інтеграторів мінятися самим і шукати нові джерела росту.

Всі замовники хочуть говорити про цифрову трансформацію, але мало хто представляє, що це в дійсності таке. Щоб задовольнити запит з боку замовників на зміни й самим відповідати вимогам ринку, у даній роботі покажемо, як системний інтегратор здійснив цифрову трансформацію власного бізнесу. За підсумками перетворень у компанії з'явилося два нових бізнес-підрозділи – консалтингу в області цифрової трансформації й хмарних сервісів.

Для здійснення трансформації з однієї сторони ми зберігаємо, підтримуємо, і плавно видозмінюємо поточний бізнес, з іншої сторони за допомогою інституту трансформації ми піддали ревізії практично всі аспекти нашого життя. Зміст транформації полягає в тому, що за допомогою простих методик удалося визволити інтелектуальний потенціал співробітників.

Одним з наслідків стала поява продуктового напрямку. Насамперед під продуктами в даному контексті розуміються різні види сервісів і готових рішень, які можуть бути тиражовані. Це дозволяє збільшити клієнтську базу за рахунок тих компаній, хто не готовий платити за повністю кастомізоване рішення.

Багато клієнтів зацікавлені в досвіді цифрової трансформації. Ми відразу надаємо їм цифрові інструменти, за допомогою яких вони могли б заробляти більше грошей.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства

Мета й завдання дослідження Метою роботи є дослідження та програмна реалізація системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства.

– Дослідження системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства.

– Програмна реалізація системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства.

Об'єктом дослідження є процес інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства.

Предметом дослідження є методи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства.

Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу Аналіз бізнес-процесів

Аналіз бізнес-процесів (Business Process Analysis) – це систематичне одержання даних з метою ідентифікації, визначення, оцінки й подання процесу як основи для його організації й поліпшення.

Приводом для проведення аналізу, як правило, є конкурентне положення компанії на ринку. Порівняння цін, витрат і продуктів/послуг може прояснити необхідні вимоги й підштовхнути до поліпшення. Індикаторами фактичної ситуації можуть служити:

тривалий час поставки продукції й виникаючих проблем зі строками виконання замовлень;

непрозорий хід процесу й недостатня його глибина;

надмірно широкий спектр продуктів і деталей;

часта зміна місць виникнення витрат при проходженні замовлення;

значні внутрифірмові транспортні й складські витрати, заморожування матеріалів і площ;

високі витрати на переустаткування при зміні продукту або технології;

низька частка часу обробки в загальному часі проходження замовлення;

високі витрати й високе завантаження потужностей; поява «вузьких місць» і ін.

Названі індикатори ставляться, переважно, до ключових процесів. Однак це не означає, що все дослідження повинне бути зосереджене винятково на них. Більший результат приносить аналіз всіх видів бізнес-процесів – ключових, управлінських, підтримуючих.

Структура процесу

Для ідентифікації процесу як необхідної умови його поліпшення, потрібне визначення його структури. Тут можуть використовуватися наступні дані:

вимоги (кількісні, якісні, економічні, екологічні, тимчасові);

технологічна послідовність подій і дій (трансформацій), що визначає будову й характеризує процес по виду й меті;

актуальна структура (послідовність виконуваної роботи), як просторово-логічна послідовність проходження замовлення через організаційні одиниці й робітники системи;

процесно-орієнтовані дані, такі як тривалість процесу (тривалість обробки замовлення), використання персоналу, площі, витрати на що створюють і не створюють вартість події (транспортування, зберігання й складування).

Для визначення даних необхідні наступні інструменти:

виробнича документація й регламент;

проведення аудита;

проведення інтерв'ю й самоопис працівників;

опис послідовності виконання робіт;

workshop з учасниками процесу.

При вивченні даних виходять відповіді на наступні питання:

який процес аналізується? які функціональні області або організаційні одиниці беруть участь? коли і які функції повинні виконуватися? Як виглядають результати цих функцій? Які наслідки повинні виходити із цих результатів?

щодо ходу роботи – які етапи і як вони повинні виконуватися? який час проходження замовлення? які витрати? за допомогою чого виконуються робочі етапи? Які існують вимоги до якості?

щодо матеріального потоку – які види ресурсів? яка потреба в потужностях? який обсяг потужностей у наявність? які потужності не задіяні? яка частота коливань у використанні потужностей? Яка матриця надходження – передачі матеріалів?

щодо інформаційного потоку – звідки надходить інформація (вхід)? які дані? по якому шляху надходять? Як обробляються дані? куди поставляється вихідна інформація (вихід)?

Показники, використовувані для аналізу бізнес-процесів

Аналіз означає в першу чергу оцінку результативності, що виходить за допомогою показників. Для безперервного процесу поліпшення також як і для ефективного керування необхідна побудова системи показників, що складається із двох і більше факторів. Розрізняють три види показників: структурні, відносні й вимірювані або індекси.

Структурний показник являє собою відношення частини до цілого, причому цифра в чисельнику є частиною цифри в знаменнику.

Відносні показники відбивають відношення різних даних друг до друга.

У коефіцієнтах і індексах співвідносяться цифри в рівних одиницях виміру, але з різних, здебільшого рівних по величині періодів або стосовні до різних моментів часу.

Якщо виразити показник А в відсотках від показника Б, тоді говорять про індекс:

Для оцінки інтегральної результативності впровадження бізнес-процесів підприємства існує європейська модель оцінки досконалості EFQM, що була заснована в 1988 році чотирнадцятьома провідними підприємствами Європи на паритетних засадах з метою розробки для поліпшення й спрощення виробничих процесів на підприємствах. Один раз у рік одне підприємство нагороджується Європейською нагородою якості (European Quality Award). Одержати її може одне з підприємств, що впровадили в себе модель EFQM і яке отримало найкращі результати.

Моделювання бізнес-процесів

Що таке моделювання бізнес-процесів? Моделювання бізнес-процесів (Business Process Modeling) – орієнтоване по цілям, розроблене по певній систематиці й формі подання відображення бізнес-процесу.

Структура моделі відбиває по суті логічну предметно-тимчасову послідовність функцій, розглянутих у рамках певного процесу. Загальні характеристики моделі є основою для документації, аналізу, організації, автоматизованої обробки й підтримки процесів, а також для їхнього сприяння й комунікації.

Цілі моделювання бізнес-процесів

1. Документування бізнес-процесів підприємства для того:

щоб вчасно одержувати дані;

щоб представляти дійсну ситуацію в організаційній одиниці підприємства;

щоб переміщати бізнес-процеси в інші підрозділи;

щоб регулювати робочі процеси й методи через механізм зовнішнього керування;

щоб виконувати обов'язки перед бізнес-партнерами або бізнесом-співтовариством (наприклад, по сертифікації підприємства);

щоб задовольняти діючим правовим нормам;

щоб навчати співробітників або уводити в суть справи;

щоб уникати втрат знань (наприклад, при звільненні співробітника);

щоб підтримувати менеджмент якості й керування охороною навколишнього середовища.

2. Підготовка / проведення оптимізації бізнес-процесів:

щоб уводити нові організаційні структури;

щоб змінювати при зміні ринкових умов завдання підприємства;

щоб перебудовувати або поліпшувати процеси підприємства.

3. Підготовка автоматизації й впровадження інформаційних технологій,

4. Установлення показників процесу й контролю результативності,

5. Проведення benchmarking між підрозділами підприємства, партнерами й конкурентами,

6. Знаходження Best Practice (кращого досвіду в компанії, регіоні, галузі),

7. Супровід організаційних змін

як продаж або частковий продаж;

як додаткова покупка й інтеграція підприємства або схилів підприємства;

як впровадження(вступ) або зміна(перемикання) систем IT або організаційних структур;

8. Участь у конкурсах (наприклад, конкурс EFQM, премія фонду Людвіга Ерхарда й ін.)

Загальною тенденцією сучасної організації й моделювання бізнес-процесів на підприємстві є перехід від функціонально-орієнтованої до процесно-орієнтованої моделі.

Моделювання бізнес-процесів припускає розгляд не тільки їхню типологію, але й облік рівня.

Подання бізнес-процесів припускає використання відповідних інструментів: символи, показники, графіки, діаграми, графи, бланки, а також таких рішень, як спеціальне програмне забезпечення.

Використання автоматизованих методів дозволяє знизити витрати, провести симуляцію й візуалізацію можливих процесних рішень, а також застосовувати й модифікувати раніше розроблені рішення. Існують різні програмні продукти для рішення завдань аналізу й організації процесів. Їх можна розділити на 3 групи:

Стандартні графічні пакети, для подання процесів в електронному виді (візуалізація). Наприклад: ABC-FlowCharter, CorelFlow, Visio.

Програмне забезпечення для аналізу процесів побудовано на базі графічних пакетів і дозволяє, поряд з візуалізацією, обробляти деякі дані процесів. Наприклад: Ablauf-Profi, Proplan, Vamos-BE.

Процесно-орієнтоване програмне забезпечення. Ця група пропонує широкі функціональні можливості. Звичайно в даних продуктах реалізовані модулі для аналізу, моделювання й візуалізації процесів, а також підтримуються оцінка й документація. Деякі системи дозволяють будувати анімаційні моделі. Наприклад: SYCAT, ARISToolset, AENEIS, AIBAS.

Опис бізнес-процесів

Опис бізнес-процесів (Business Process Description) – для опису процесу з якісно-кількісної, просторово-організаційної й технічно-технологічної точок зору використовуються характеристики (параметри), які задані стандартом ENISO 9001:2000. До таких параметрів ставляться:

Цілі процесу.

Об'єкт впливу (вид, кількість, розміри, ...)

Місце впливу (організаційна одиниця, робоча система).

Вид і послідовність подій, структура.

Застосовувані засоби виробництва (вид, кількість, продуктивність, ...).

Хід процесу (горизонтальний, вертикальний; просторово-тимчасовий).

Участь персоналу (кількість, кваліфікація, ...).

Витрати часу на події й загальний процес (тривалість процесу).

Робочі умови, вимоги й завдання.

Застосовувані технології, режими роботи.

Результати.

Невизначені стани й події.

Опис процесів вимагає визначення відповідної області розгляду, тобто вибору стартової й кінцевої крапки, що обмежують область, що цікавить.

Приклад

Для визначення типового шляху проходження замовлення в компанії область розгляду повинна охоплювати всі події від стартової крапки – «надходження замовлення» – до кінцевої крапки – «поставка замовлення клієнтові». Нехай, рівнем розгляду буде рівень структурного підрозділ і частина загального процесу. Необхідно визначити проходження замовлення в «Конструкторському бюро», тоді стартовою крапкою для опису й аналізу є «надходження замовлення в конструкторське бюро», а кінцевої – «передача замовлення на виробництво». Цей приклад показує, що процеси можуть мати різний ступінь складності, що визначає витрати на їхній аналіз і організацію. Тому при реалізації подібних проектів, насамперед, визначають ступінь деталізації.

Подання бізнес-процесів припускає використання відповідних інструментів: символи, показники, графіки, діаграми, графи, бланки, а також таких рішень, як спеціальне програмне забезпечення.

Розповсюдженою формою подання може бути графічна блок-схема.

Зв'язок організаційних одиниць, що беруть участь, відзначається лінією, що підвищує наочність подання, однак, не несе необхідної інформації про час проходження, витратах на обробку або перервах. Подібний вид опису є простим і низькозатратним, однак надає таку корисну інформацію, як проходження через організаційні одиниці, час проходження замовлення, витрати на обробку й ін.. Крім того, він дозволяє зробити виводи про високу частку часу проміжного зберігання, можливих «вузьких місцях» у виробництві, що повторюється зміні відповідальності під час обробки замовлення.

Оптимізація бізнес-процесів

Оптимізація бізнес-процесів (Business Process Optimization) – безпосередня розробка й реалізація заходів щодо вдосконалювання (реорганізації) бізнес-процесів компанії.

Дослідження їхнього фактичного стану дозволяє сформулювати цілі по вдосконалюванню (реорганізації). Наприклад, завоювання частки ринку, зниження часу проходження замовлення, зменшення матеріальних запасів і ін.

Приклад

Компанія А робить спортивні товари й товари для відпочинку. На основі дослідження поточного положення на ринку в компанії були сформульовані наступні цілі:

Зниження витрат до 25 Євро в середньому на виріб.

Виготовлення й поставка продукту за замовленням клієнта протягом 5 днів з моменту замовлення в магазині.

Підтримка номенклатури продукції в кількості 1300 штук.

Керівництво компанії прийняло пропозицію по дослідженню й поліпшенню процесів і, як результат проведеного дослідження, установило відповідні цілі. Для досягнення запланованих результатів було необхідно не тільки докорінно поліпшити процес проходження замовлення, але й внести зміни в розробки продуктів, організацію роботи на ділянці монтажу, змінити функції працівників і організувати роботу зі збуту.

Оптимізація направляється на реалізацію поставлених цілей і містить заходу, що усувають виявлені проблеми. До них можуть ставитися: питання сполучення змінених технологій, змінених робочих систем, занадто велике число рівнів керування, простої, невикористовувані потужності, дублювання робочих завдань, помилки в передачі інформації, втрата інформації, помилки в документації м ін.

При розробці заходів щодо оптимізації варто враховувати параметри впливу: логістичні, економічні, тимчасові, просторові, персональні.

Логічні – це кількість етапів процесу, технологічна реалізуємість, послідовність подій, організаційна взаємодія.

Економічні – низькі витрати, високе завантаження потужностей, низький рівень запасів, економічна глибина процесу, гнучкість, висока частка створення вартості.

Часові – короткий час проходження замовлення, низька частка допоміжного часу, низька частка часу переналагодження, гнучкість виробничого часу.

Просторові – можливість розташування необхідних робочих місць, можливість упорядкування робочих систем, мінімальні транспортні шляхи, можливість зміни порядку розташування робочих систем.

Персональні – обсяг роботи й потреба в персоналі, забезпечення необхідної кваліфікації, підвищення кваліфікації, гнучкий робочий час для персоналу.

Методи оптимізації бізнес-процесів

Методи оптимізації бізнес-процесів можуть бути різними, залежно від рішення виявлених проблем. Схема 2. показує можливі підходи по їхньому поліпшенню.

Метод виключати позначає зменшення рівнів процесу, ліквідацію причин перешкод, скорочення транспортних шляхів, виключення вхідного контролю.

Спрощувати припускає зменшення складності в проходженні замовлення, зниження комплексності структури продукту, організацію роботи, поділ робіт

Стандартизувати – програми, технології, методи, продукти, що комплектують, етапи.

Скорочувати – місця виникнення витрат, кількість і тривалість подій, деталей, виробничі витрати.

Прискорювати – паралельний інжиніринг, симуляцію, швидке проектування зразків, автоматизацію.

Змінювати – необхідні матеріали, технології, методи роботи, розташування, робочі системи, обсяг замовлення/партії, порядок обробки.

Забезпечувати взаємодія організаційних одиниць, робочих систем, працівників.

Виділяти й включати – необхідні процеси, що комплектують.

Організація бізнес-процесів

Організація бізнес-процесів (Business Process Organization) – поєднує заходу щодо встановлення їхньої внутрішньої структури (технологічної, тимчасовий, просторової, організаційної) з урахуванням конкретних умов компанії для певної області. Результатом є план, модель, опис процесів як основа для їхньої реалізації.

У заходи щодо організації входять: визначення ходу процесу й оргструктури, визначення ресурсів, установлення керівництва, формування процесних даних і документів, розробка інформаційного обслуговування й інші аспекти.

Шість кроків системного підходу

Системний підхід до організації процесів базується на шести кроках і припускає метод, що складається із шести пунктів.

1. Дослідження вихідної ситуації.
2. Аналіз і оцінка.
3. Розробка концепції.
4. Деталізація процесного рішення.
5. Впровадження.
6. Застосування.

У Кроці 1 проводиться дослідження фактичного стану процесів з використанням різних інструментів і методів, а також його аналіз. Фактичний стан можуть відбивати наступні дані: володіння процесом і результати, тривалість проходження замовлення (робочих днів, змін), витрати на обробку замовлення (годин/замовлення, хвилин/замовлення), кількість подій і робочих систем, що беруть участь, частка подій, що створюють і не створюють вартість, кількість організаційних рівнів, використання площ,

завантаження робочих систем/потужностей, затримки, час очікування, умови роботи; керування перешкодами й ін. На основі причин і стимулів виробляються необхідні цілі.

У Кроці 2 зібрані дані необхідно проаналізувати відповідним чином, підготувати, тобто впорядкувати, перевірити на повноту, обробити й оцінити.

З урахуванням виявлених причин неефективності починається розробка заходів щодо зміни. Як альтернативні варіанти змін виступають: повна (ре)організація процесу або його поступове поліпшення.

У Кроці 3 проробляються варіанти можливих рішень, уточнюються вимоги й необхідні переваги. Тут формуються заходи щодо організації процесів, насамперед, у формі загального планування можливих варіантів рішень. При цьому справедливо наступне основне правило: чим більше що змістовно відрізняються друг від друга варіантів буде знайдено, тим більша ймовірність досягнення поставленої цілі. Варіанти рішень рівняються по:

результатам, що досягаються;

вимогам до реалізації;

витратам і строкам реалізації;

необхідності навчання й перекваліфікації працівників і т.д.

Наприкінці кроку приймається остаточне рішення про впровадження одного із запропонованого варіанта. Тому що на попередньому вужі визначені вимоги й необхідні заходи, то далі переходять до Кроку 4 – деталізації процесного рішення. Детальне планування припускає: властиво деталізацію обраного рішення; організацію, переміщення й зміну робочих систем, іноді робочих місць; розробку необхідних заходів щодо реалізації (проведення перекваліфікації, організація робочого часу й системи винагороди, зміна кооперації, розробка процесних інструкцій і документації).

У Кроці 5 реалізуються необхідні підготовчі заходи й заходи щодо зміни:

розміщення процесу;

організація матеріального потоку;

перекваліфікація працівників;

зміна організації роботи, а також методів, засобів виробництва.

Далі виконується властиво впровадження на підприємство обраного рішення. Для виявлення можливих недоліків і слабких місць проводиться пілотний проект, що означає послідовний прогін процесу до досягнення запланованих результатів.

Бізнес-процес починає функціонувати по-новому в Кроці 6. Одержувані результати необхідно зіставляти із установленими цілями для виявлення можливих відхилень і визначення можливих коректувань. Отримані результати й досвід повинні оброблятися й зберігатися. У Кроці 6 необхідно здійснювати постійне поліпшення й удосконалювання, для чого використовуються методи в області планування, керування й організації процесів.

Схема бізнес-процесу

Схема бізнес-процесу (Business Process Diagram) – це подання покрокових процесів, де схеми звичайно створюються як блок-схеми, у яких фігури представляють етапи процесу, а послідовність етапів позначається стрілками.

Багато українських компаній використовують у своїй діяльності текстовий опис бізнес-процесів у документах, які є процесними регламентами. Але для цілей аналізу й оптимізації діяльності компанії даний варіант не ідеальний. Опис бізнес-процесу в текстовому виді складно представити й аналізувати системно. При сприйнятті й аналізі текстової інформації людський мозок розкладає її на ряд образів, на що йдуть додатковий час і розумові зусилля.

Види схем бізнес-процесів

Схеми розробляються за допомогою цілого ряду різних методик: без символів і діаграм; з використанням символів і діаграм; побудови залежно від пріоритетів; графічно-описове подання процесів.

Схеми можуть бути побудовані з використанням графів пріоритетів. Графи пріоритетів – це подання за допомогою мережного плану часткових завдань монтажу, причому часткові завдання представляються як вузли, а взаємини між ними як єднальні лінії.

Схеми на основі графічно-описового подання є більше зручним для реалізації.

Під цифровою трансформацією бізнесу звичайно розуміють впровадження нових технологій, які дозволять істотно поліпшити бізнес-процеси компанії. У даній роботі під цифровою трансформацією мається на увазі впровадження хмарних технологій у бізнес-процеси підприємства. При цьому IT-менеджери вважають, що реінжинірингом бізнес-процесів будуть займатися представники бізнесу. А бізнес-керівництво вважає, що співробітники IT впровадять новітні IT-технології, які самі поліпшать доходи бізнесу, скоротять витрати й знизять ризики.

Цифрова трансформація бізнесу доречна, якщо треба:

треба дуже сильно, у кілька разів, збільшити вигоди бізнесу від використання IT;

є й гроші, і час, і бажання бізнес-керівництва займатися реінжинірингом бізнес-процесів, створивши до цього ще і єдину цифрову IT-платформу (як мінімум, логічно єдині дані по вашій компанії).

Цифрова трансформація бізнесу: що це таке?

Загальноприйнятих визначень, що таке цифрова трансформація бізнесу, немає. Є різні точки зору на це, що сильно залежать від того, хто відповідає на це питання.

Цифрова трансформація бізнесу: як її бачать гендиректори українських компаній:

Істотне збільшення вигід, які інформаційні технології дають бізнесу при непідвищенні ризиків IT.

У деяких випадках є розуміння, що за IT прийде платити в кілька разів більше, але майже всі гендиректори намагаються прикинути «валянками» і спробувати провести цифрову трансформацію бізнесу без збільшення витрат на IT.

Конкретні IT-технології, які гендиректори українських компаній, звичайно асоціюють із цифровою трансформацією бізнесу:

Продажі через Інтернет.

Омніканальність (робота із замовниками через різні канали).

Мобільний доступ до корпоративних інформаційних систем.

Налаштування виробництва під конкретні замовлення.

Аналіз і прогноз поводження замовників.

Цифрове проектування й моделювання.

Соціальні мережі: продажу й робота із претензіями.

Автоматизація керування логістикою.

3D-друк.

Блокчейн.

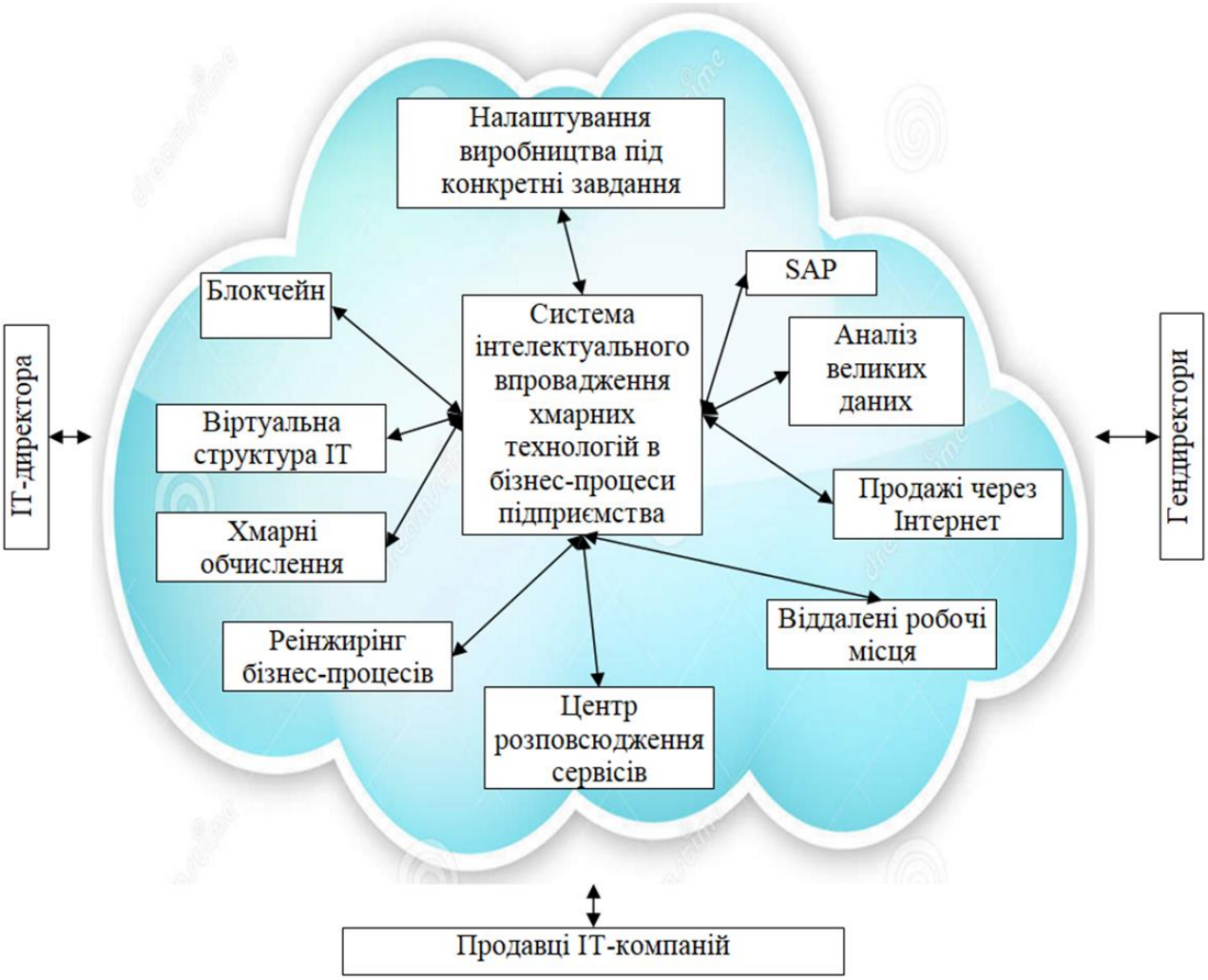


Рисунок 1 – Структурна схема системи

IT-керівники хочуть і далі продовжувати впровадження нових IT-технологій, уважаючи що цифрова трансформація бізнесу – це завдання бізнес-менеджерів по реінжинірингу бізнес-процесів на базі IT-технологій (особливо нових).

Цифрова трансформація бізнесу: як її бачать керівники IT-служб українських компаній:

«Хмарні обчислення».
Віртуальна інфраструктура IT.
Мобільний доступ.
Вилучені робочі місця.
SaaS, PaaS, IaaS.
Аналіз більших даних.
Омніканальність.
Реінжиніринг бізнес-процесів.
Автоматизація служби підтримки клієнтів компанії.
Майнинг криптовалют.
Продавці хочуть вигідно продати що те зараз, ну або через півроку.
Цифрова трансформація бізнесу: як її бачать продавці IT-компаній в Україні:
«Хмарні обчислення».
Впровадження продуктів SAP.
Впровадження продуктів IBM.
Впровадження продуктів Oracle.
Аналіз великих даних.

ЦОД.

Віртуальна інфраструктура IT.

Інтернет речей.

Штучний інтелект.

Shares Service Center.

Нові комп'ютерні технології часто виявляються старими розробками, але під новою рекламною оболонкою.

Проблеми, що виникають при цифровій трансформації бізнесу:

Нереально виконати вимоги багатьох українських гендиректорів (швидко, якісно, безкоштовно, з нульовими ризиками, а також не міняючи бізнес-процесів (і не задіючи співробітників бізнес-підрозділів);

Нереально виконати вимоги багатьох українських гендиректорів (швидко, якісно, безкоштовно, з нульовими ризиками, а також не міняючи бізнес-процесів (і не задіючи співробітників бізнес-підрозділів);

Продавці IT-компаній просто хочуть щось продати, не піклуючись про результати впровадження.

Етапи еволюції IT до цифрової трансформації бізнесу

На мій погляд можна виділити наступні етапи залежності бізнесу від IT:

до 1965 року: бізнес взагалі не залежав від IT, хіба що папір і рахівницю за IT уважати;

с 1965 року: IT виконують вимоги бізнесу до IT. Рішення по поліпшенню IT: оптимізація окремих елементів IT. Ефективність +5+10% вигід від IT;

с 2000 року: IT виконують вимоги бізнесу й дають нові можливості бізнесу. Рішення: IT-стратегія. Вигоди +10+20%;

с 2010 року: єдині цифрові платформи бізнесу. Рішення: інтегровані інформаційні системи, центри даних, обробки даних, єдині класифікатори інформації, централізовані служби підтримки IT. Вигоди: +15+30%;

с 2015 року: IT радикально трансформують бізнес. Рішення: цифрова трансформація бізнесу, +30+50% збільшення вигід від IT.

Вивід: Для планування цифрової трансформації бізнесу треба визначитися, чи готова ваша компанія не тільки до більших можливих вигід від цифрової трансформації бізнесу, але й більшим витратам і ризикам неуспіхів.

Краще на початку провести аудит готовності до цифрової трансформації бізнесу й/або розробити IT-стратегію або стратегію створення цифрової трансформації бізнесу.

Планування цифрової трансформації бізнесу

Роботи на етапі 1: Виявлення суті бізнесу й перспектив його розвитку, пріоритетів бізнесу, вимог бізнесу до IT:

Вибір доцільних нових IT-технологій. Аналіз можливостей нових IT-технологій.

Аналіз поточного стану IT (інформаційні системи, інфраструктура IT, керування IT).

Облік розміру компанії, галузі, інших особливостей.

Визначення відповідальних за цифрову трансформацію бізнесу.

Визначення рамок проекту по цифровій трансформації бізнесу: час, гроші, люди, методики, елементи IT і бізнесу.

Розробка стратегії цифрової трансформації бізнесу.

Оцінити впровадження нових IT-технологій треба з урахуванням їх вигід, витрат і можливих ризиків. На жаль ризики впровадження зовсім нових IT-технологій можуть бути дуже великі.

Відповідальні за цифрову трансформацію бізнесу

От типові варіанти відповідальних за цифрову трансформацію бізнесу (CDO):

0) Спеціальних відповідальних немає.

1) На одному рівні з IT-директором.

2) Новий керівник IT-директори.

3) Уже наявний куратор IT від бізнесу.

4) Новий менеджер, підлеглий IT-директорові.

5) Нова функція IT-директори.

6) Новий радник і/або робоча група по цифровій трансформації.

7) Новий IT-директор, що займеться й цифровою трансформацією.

Виводи:

Треба вибрати оптимальний саме для вашої компанії варіант відповідального (відповідальних) за цифрову трансформацію бізнесу (тому що це нова область і в багатьох компаніях поки немає відповідальних за неї).

Планувати цифрову трансформацію бізнесу треба з обліком того, хто буде за це відповідати (ну або враховувати при плануванні цифрової трансформації бізнесу що треба буде вибрати відповідального за цей напрямок).

Краще на початку провести аудит готовності до цифрової трансформації бізнесу й/або розробити IT-стратегію або стратегію створення цифрової платформи бізнесу.

Роботодавці й кадровики вже досліджували це питання й от відповідь. IT-директор, якого з руками відірвуть компанії, у яких вам хочеться працювати, це:

Цифровий і командний геній: харизматичний менеджер зі стратегічним мисленням, що провидить, як розвивати бізнес через цифрові технології. Проекти його команди повинні перегравати по ефективності, красі й безпеці все те, що можуть дати зовнішні IT-провайдери.

Джерело мегадоходи й економії: відрізняє тренд від хайпа, вчасно бачить і ощадливо забезпечує унікальні конкурентні технологічні переваги, впроваджує проривні рішення й мінімізує витрати бізнесу розумної й своєчасної цифровізацією.

Футуролог, продажник, політик: пророкує, які IT-інструменти знадобляться завтра всім іншим директорам і клієнтам, уміє оптимізувати цифрою спільні рішення й надихаюче «продавати» їхнім колегам, керівництву й клієнтам, на зрозумілому для них мові.

Чоловік мрії: win-win фахівець із безперервних змін, схильний до постійного апгрейду свого мислення й консервативному керуванню ризиками компанії, гнучкий менеджер талантів і геній комунікації зі складними клієнтами, терплячий як Будда й надійний як Бандера …

Загалом, ідеальний CIO для компанії – це оцифрованний від голови до ніг підприємець, продажник і політик, а також генерал, поет і трошки бог: «Юрій Гагарін цифрової епохи». Довідаєтеся в цьому портреті себе або?.. Не зовсім?.. Так ніхто не ідеальний! Ідеали потрібні, щоб постійно рости над собою.

Вибір за вами, шановні IT-директори 21 століття, тому що навіть поверхневий data analysis показує, що ви навіть не усвідомлюєте, що не володієте:

1. Ні стратегічним і футурологічним мисленням 21 вік.
2. Ні навичками політичного просування рішень цифрового розвитку бізнесу.
3. Ні технологією керування інноваційними змінами й ризиками.
4. Ні методами роботи з міждисциплінарними командами й наставництва.
5. Ні мистецтвом творчого мислення й дії в бізнесі.
6. Ні навичками продажів, переговорів, презентацій, сторителінгу.
7. Ні навичками емоційної компетентності й керування стресом.
8. Ні методикою розвитку власної кар'єри з CIO в GlobalCIO.

Від IT-стратегії до стратегії цифрової трансформації бізнесу

Можлива структура стратегії цифрової трансформації бізнесу:

Доцільна цифрова трансформація бізнес-процесів (вимоги й побажання з боку бізнесу).

IT-технології, доречні для цифрової трансформації бізнесу.

Інфраструктура IT (необхідне через 1-5 років стан).

Інформаційні системи й дані (необхідне через 1-5 років стан).

Керування IT (необхідне через 1-5 років стан).

План проектів по IT (на 1 рік і 2-5 років). Бюджет IT.

Сценарії розвитку ІТ (альтернативні варіанти розвитку ІТ і цифрової трансформації бізнесу).

Істотне питання, що цікавив передплатників мого сайту, якщо стратегія ІТ є, то, якщо бізнес вимагає стратегію цифрової трансформації, що робити. На мій погляд, потрібно з наявної ІТ-стратегії взяти як основу шматочки. Тобто зрозуміти, що бізнес хоче від цифрової трансформації, що він хоче через рік і два й постаратися зрозуміти й формалізувати. Нехай з боку бізнесу письмово це напишуть.

З боку ІТ і бізнесу вибрати нові ІТ-технології, доробити власну ІТ-стратегію: цілі ІТ, необхідний стан, інфраструктуру, інформаційні системи, керування, плани проектів. Ну й зрозуміло, що треба врахувати розмір компанії, галузі й інші фактори. І далі, на мій погляд, робити не стратегію цифрової трансформації, а стратегію створення єдиної цифрової платформи, що реально.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Досліджена система інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального впровадження хмарних технологій в бізнес-процеси підприємства. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
2. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
3. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
4. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
5. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
6. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.
7. Коваленко А.С. Експертна система технічного діагностування інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2015. – № 1(41). – С. 106-111.
8. Коваленко А.С. Удосконалення методу технічного обслуговування об’єктів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко, О.П. Доренський // Системи озброєння і військова техніка. – Х.: ХУПС, 2016. – № 2(46). – С. 109-114.
9. Коваленко А.С. Метод визначення оптимального комплексу робіт з відновлення працездатності інтегрованої системи технічної діагностики в умовах ресурсних обмежень / А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2016. – Вип. 3(140). – С. 69-72.
10. Kovalenko A.S. Information model and its element for displaying information on technical condition of objects of integrated information system / A.S. Kovalenko, A.A. Smirnov, A.V. Kovalenko, A.P. Dorensky // International

Journal of Computational Engineering Research (IJCER). – India: Delhi, 2016. – Volume 6, Issue 1. – P. 21-27.

УДК 004

Б. Тарасенко, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ FIBRE CHANNEL 6

У статті розроблено програмне забезпечення, яке призначено для системи зберігання даних з використанням технології Fibre Channel 6. Метою розробки є дослідження та програмна реалізація системи зберігання даних з використанням технології Fibre Channel 6. Об'єктом дослідження є процес зберігання даних з використанням технології Fibre Channel 6. Предметом дослідження є методи зберігання даних з використанням технології Fibre Channel 6. Методи дослідження базуються на методах теорії телекомунікації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи зберігання даних з використанням технології Fibre Channel 6. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, Fibre Channel 6

Постановка проблеми. Fibre Channel залишається кращою технологією для підключення систем зберігання. Згідно надаваним IDC даним за 2019 рік за допомогою FC здійснюється доступ до більш ніж 20 тис. Пбайт даних – більше ніж за допомогою який-небудь іншої. На ринку комутаторів FC залишилося фактично два гравці – Brocade і Cisco, причому, на відміну від мережевого ринку, Cisco аж ніяк не домінуючий гравець у цьому сегменті – Brocade належить левова частина ринку (понад 80% як по обсязі продажів, так і по кількості портів, що поставляються,).

Рік назад Brocade увійшла до складу Broadcom як підрозділ Brocade Storage Networking.Всі лінійки IP- і Ethernet-устаткування були розпродані, так що тепер Brocade, як і колись, спеціалізується виняткова на рішеннях Fibre Channel. В Україні все встаткування Brocade продається через OEM-партнерів – у компанії дотепер немає жодного дистриб'ютора або інтегратора, що був би авторизований на прямий продаж комутаторів під маркою Brocade.

Після різкого падіння продажів в 2015 році ринок в Україні нарешті відновився. Цього року ріст продажів триває, причому це досягається не тільки за рахунок окремих великих проектів, але й завдяки множині дрібних і середніх..

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи зберігання даних з використанням технології Fibre Channel 6.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи зберігання даних з використанням технології Fibre Channel 6.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем зберігання даних з використанням технології Fibre Channel 6.

– Дослідження системи зберігання даних з використанням технології Fibre Channel 6.

– Програмна реалізація системи зберігання даних з використанням технології Fibre Channel 6.

Об’єктом дослідження є процес зберігання даних з використанням технології Fibre Channel 6.

Предметом дослідження є методи зберігання даних з використанням технології Fibre Channel 6.

Методи дослідження базуються на методах теорії телекомунікації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Чому варто розглянути використання Fibre Channel? Fibre Channel як і раніше є найбільш безпечним, надійним, економічно ефективним і масштабованим протоколом для з'єднання серверів і сховищ, а також єдиним протоколом, спеціально призначеним для передачі трафіку сховища.

Всі ми знаємо, що обсяг даних продовжує рости в геометричній прогресії, і що самі дані є тією новою валютою, на яку розраховують підприємства. Здатність вчасно реагувати на ці дані може вплинути на конкурентоспроможність бізнесу на ринку. Тому швидкий і надійний доступ до даних має першорядне значення, а базова інфраструктура, що зв'язує користувача із системами зберігання даних, є більше важливої, ніж коли-або колись.

У сучасному центрі обробки даних архітектори можуть вибирати з безлічі різних варіантів підключення, але Fibre Channel був і залишиться джерелом життєвої сили для підключення до загальних сховищ. Це пов'язане з тим, що Fibre Channel є найбільш безпечним, надійним, економічно ефективним і масштабованим протоколом для з'єднання серверів і сховищ, а також єдиним протоколом, спеціально призначеним для передачі трафіку сховища.

Fibre Channel існує вже кілька десятиліть і як і раніше є основним вибором для підключення до загального сховища в центрі обробки даних. За допомогою Fibre Channel створюється виділена мережа зберігання, а команди зберігання SCSI направляються між сервером і пристроями зберігання із пропускною здатністю до 28,05 Гбіт/с (32GFC) і з IOPS, що перевищує один мільйон. Оскільки Fibre Channel споконвічно був розроблений для трафіку сховищ, він працює дуже надійно й забезпечує високопродуктивний зв'язок. Адаптери HPE StoreFabric 16GFC і 32GFC і інфраструктура комутації забезпечують пропускну здатність, кількість операцій вводу-виводу в секунду й низьку затримку, необхідні в центрах обробки даних сьогодні й на роки вперед.

Досягнення в технології Fibre Channel тримають його на випередження, коли справа доходить до підключення.

Наприклад, інфраструктура HPE StoreFabric 16GFC і 32GFC уже здатна підтримувати трафік зберігання NVMe, навіть до того, як власні масиви зберігання NVMe стануть масовими. Інші розширені можливості включають розширену діагностику, спрощене розгортання й оркестровку й підвищену надійність, таку як T-10 PI, двопортова ізоляція й багато чого іншого.

Інший популярний варіант підключення до сховища – iSCSI. З iSCSI, команди зберігання в стандартній мережі TCP / IP, і це відмінно підходить для систем низького й середнього рівня, де продуктивність і безпека не є основними вимогами. Розповсюджена омана про Fibre Channel полягає в тому, що, оскільки він використовує виділену мережу зберігання даних, він дорожче, ніж iSCSI. Хоча iSCSI може працювати в тій же мережі Ethernet, що й весь звичайний мережевий трафік, для забезпечення продуктивності, необхідної більшості клієнтів від своїх систем зберігання, iSCSI повинен працювати в сегментованій або виділеній мережі Ethernet, ізольованої від звичайного мережевого трафіку. Це означає складні конфігурації VLAN і політики безпеки або повністю виділену мережу Ethernet. Так само, як Fibre Channel.

Єдина реальна різниця у вартості між FC і iSCSI – це коли DAC – кабелі використовуються в реалізаціях iSCSI. Але з обмеженням відстані 5 метрів, використовуючи DAC – кабелі. Це може нормально працювати для клієнтів малого й середнього бізнесу, що

мають тільки один масив зберігання, але DAC – кабелі погано працюють у великомасштабному центрі обробки даних.

Коли ви дивитеся на топологію мережі зберігання даних, кращі практики ідентичні для iSCSI і Fibre Channel. Для забезпечення відказостійкості й усунення простоїв у проекті мережі зберігання даних (SAN) передбачено два ідентичних мережевих шляхи між серверами й сховищем.

Однак одна істотна відмінність полягає в тому, що мережі Fibre Channel не так піддані порушенням безпеки, як Ethernet. Коли ви востаннє чули про злом мережі Fibre Channel? Ніколи? Як щодо мережі Ethernet?

Безпека є однією з головних причин того, що Fibre Channel буде залишатися опорою в центрі обробки даних протягом багатьох років.

Як ми очікуємо, набір команд SCSI буде замінений командами Non-Volitile Memory Express або NVMe. NVMe – це оптимізований набір команд, розроблений для SSD і пам'яті класів зберігання, що набагато ефективніше, ніж SCSI. Крім того, NVMe являє собою багаторядну архітектуру із чергами вводу-виводу до 64 КБ, причому кожна черга вводу-виводу підтримує до 64 КБ команд. У порівнянні з SCSI з однією чергою й 64 командами, NVMe може забезпечити значно більше високу продуктивність.

Сучасна інфраструктура HPE StoreFabric 16GFC і 32GFC, що підтримує команди SCSI, також може запускати команди NVMe у мережі SAN або в структурі, як вона називається. При використанні Ethernet клієнтам буде потрібно впровадити RDMA з низькою затримкою в порівнянні з конвергентним Ethernet або RoCE, щоб повною мірою використовувати переваги NVMe. Однак цей підхід вимагає складної реалізації Ethernet без втрат з використанням мостів центрів обробки даних (DCB) і керування пріоритетними потоками (PFC). Складність мережі для NVMe через Ethernet буде величезним бар'єром для більшості клієнтів, особливо коли розгорнута сьогодні FC SAN прекрасно працює зі сховищем NVMe завтрашнього дня.

Fibre Channel – зверхшвидкістна (до 1 Гбіт/с і вище) схема повнодуплексної передачі даних. Технологія забезпечує передачу даних з малою затримкою (10-30 мкс) на відстані до 10 кілометрів.

У назві Fibre Channel (якщо переводити буквально, те 'волоконний канал') криється підступ, оскільки оптичне волокно зовсім не при чому. Середовищем передачі даних може бути крім оптоволокна й кручена пари, і коаксіал. Архітектура Fibre Channel являє собою суміш канальної й мережевої топології.

Варіанти топології Fibre Channel

Топологія Fibre Channel.

Усього в Fibre Channel існують три варіанти топології.

Найпростішою топологією є, мабуть, 'точка-точка'. У ній два пристрої Fibre Channel з'єднані прямим з'єднанням між собою. При цьому передавач одного пристрою з'єднується із приймачем другого, і, відповідно, навпаки. Пристрої, що з'єднуються, повинні працювати на одній швидкості, при цьому їм доступна вся пропускна здатність з'єднання.

Більше розповсюдженим варіантом топології є арбітражна петля (FC-AL). При цьому способі з'єднання можливе підключення до 127 пристроїв без використання комутаторів. Хоча топологія й називається петлею, по суті це ланцюжок пристроїв, що одним кінцем може бути підключена до комутатора (а може й не бути). При з'єднанні пристроїв арбітражною петлею пропускна здатність є поділюваної, тобто в один конкретний момент часу тільки два пристрої можуть взаємодіяти один з одним. Також зберігається вимога, відповідно до якого пристрої, що з'єднуються, повинні працювати на одній швидкості.

Третій варіант топології – з'єднання з комутуючою структурою. За рахунок каскадного застосування комутаторів можливе з'єднання дуже великої кількості пристроїв – понад 16 мільйонів. Обмежень на відповідність швидкостей пристроїв, що з'єднуються, у цьому випадку немає.

Позначення портів

Порти Fibre Channel діляться на кілька типів залежно від типу пристрою, його призначення й підтримуваної топології. Для зручності всі вони мають літерні позначення.

N (Node Port, N_Port) – порт Fibre Channel на кінцевому пристрої (сервері, дисковому масиві, принтері й т. П.). Node Port у перекладі означає 'вузловий порт'.

F (Fabric Port, F_Port) – порт на комутаторі (або 'комутуючий порт'), до якого підключається вузловий порт.

NL_Port і FL_Port . Якщо перераховані вище вузлові або комутуючі порти можуть підключатися до арбітражної петлі, то вони маркіруються додатково буквою L від англійського loop, тобто петля.

E (Expansion Port, E_Port) – порт на комутаторі для підключення одного комутатора до іншого.

G (Generic Port, G_Port) – універсальний порт, до якого може бути підключений не тільки інший комутатор, але й вузол.

GL – універсальний порт із підтримкою підключення арбітражної петлі.

Різновиди устаткування

Концентратори

У топологічної схеми «арбітражна петля» крім поділу пропускної здатності є й інші недоліки. Наприклад, при відмові адаптера на якому-небудь пристрої або розриві в з'єднуючому кабелі петля виявляється повністю непрацездатною. При зміні набору пристроїв у петлі (зокрема, при додаванні нового пристрою) вся петля повинна бути ініціалізована заново (щоб підключений пристрій міг одержати адресу), причому ця процедура може займати досить багато часу.

Для рішення цих і подібних проблем використовуються концентратори Fibre Channel. Одночасно із цим, їхнє застосування дозволяє використовувати більше зручну для підключення нових пристроїв фізичну топологію «зірка», хоча логічно топологія залишається кільцем. Звичайно концентратори мають не більше 10 портів. Однак це обмеження легко перебороти за рахунок каскадного підключення концентраторів.

Концентратори підвищують надійність використання арбітражної петлі за рахунок застосування схеми обходу портів (Port Bypass Circuit, PBC). PBC виконує дві функції: по-перше, автоматично виявляє наявність вузла й включає його в петлю, по-друге, виявляє відмова вузла й виключає його з петлі. Найбільш просунуті концентратори підтримують віддалене керування й інші розвинені функції.

Комутатори

Комутатори Fibre Channel є істотно більше дорогими пристроями, ніж концентратори Fibre Channel. На відміну від концентраторів, вони дозволяють надати вузлу виділену пропускну здатність і створювати топології з незрівнянно більшим числом вузлів (224). Крім того, комутатори можуть мати порти з підтримкою різних швидкостей і середовищ передачі.

Комутатори Fibre Channel прості в установці й використанні завдяки наявності функцій самоконфігурації й самоврядування. Всі операції конфігурування здійснюються автоматично. Наприклад, при підключенні вузла до комутатора він реєструється на комутаторі й погоджує з ним взаємоприйняті параметри. При підключенні комутатора до комутатора вони визначають конфігурацію й адреси. У випадку універсального порту (GL_Port) комутатор також сам установлює, до чого він підключений – до іншого комутатора, до петлі або до вузла. З огляду на цінові фактори, для організації взаємодії між пристроями в декількох петлях вигідніше використання комутуючих концентраторів замість більше дорогих комутаторів.

Маршрутизатори

Маршрутизатори Fibre Channel дозволяють підключити мережа Fibre Channel до іншого середовища передачі, наприклад до SCSI або Ethernet.

Адаптери Fibre Channel

Дотепер ми говорили про, так сказати, структуроутворюючих пристроях Fibre Channel. Однак найпоширенішими пристроями є, природно, адаптери Fibre Channel. Без них

ніякий вузол не зміг би взаємодіяти з комутуючою структурою Fibre Channel. Ті самі адаптери можуть служити для з'єднання як з локальною мережею (іншими вузлами), так і з периферією. Це дозволяє, зокрема, скоротити число необхідних слотів вводу/виводу. Більшість адаптерів випускається для шини PCI. Часто разом з адаптерами використовуються гігабітні перехідники (GigaBit Interface Converter). Вони служать для перетворення оптичних сигналів в електричні й назад.

Класи сервісу

Комутатори й вузли можуть підтримувати один або більше видів сервісу. Загальні підтримувані комутаторами й вузлами сервіси визначаються під час процедури реєстрації пристроїв. Ручне налаштування при цьому не потрібно.

Клас 1 відповідає сервісу із установленням з'єднання й гарантованою доставкою. Виділене з'єднання через комутуючу структуру (сукупність комутаторів) установлюється за кілька мікросекунд. Оскільки з'єднання є виділеним, ніяке інший пристрій не може зв'язатися з портами одержувача й відправника, до його завершення. Пристрій-Одержувач підтверджує одержання кожного кадру устрою-передавачу. У такий спосіб гарантується доставка кадрів. Цей клас сервісу підходить для обміну більшими обсягами даних, зокрема для резервного копіювання.

Клас 2 іноді називають мультиплексним. При його використанні комутація кадрів виробляється незалежно друг від друга, тому кадри можуть доставлятися не в тому порядку, у якому були відправлені. З'єднання між пристроями не встановлюється. Доставка кадрів гарантується шляхом використання підтверджень. Цей вид сервісу схожий на організацію трафіку в локальних мережах.

Клас 3 аналогічний Класу 2, за винятком того, що він не використовує підтвердження одержання, тому доставка кадрів не гарантується. За рахунок цього реальна пропускна здатність збільшується. Щонайкраще цей клас сервісу підходить для багатоадресного і широкомовного розсилання.

Інші класи часто не виділяються в самостійні, а вважаються підвидами перерахованих. Вони відрізняються від перерахованих вище, наприклад, використанням не повної, а часткової пропускної здатності каналу.

Характеристики Fibre Channel

Fibre Channel дозволяє підтримувати самі різні швидкості – від 133 Кбіт/с до 4,252 Мбіт/с і навіть більше. Одна із цілей розробки Fibre Channel складалася, зокрема, у підтримці HIPPI на 100 Мбайт/с. Тому основною швидкістю передачі даних – так званою повною швидкістю – є 100 Мбайт/с (інші швидкості вказуються часто в частках від основної швидкості – одна восьма, четверта, друга, подвійна, учетверена). Однак, з урахуванням накладних витрат на кодування 8B/10B, заголовки кадрів і т.д., швидкість передачі властиво бітів становить 1,063 Мбіт/с. Таким чином, виробники приводять, як правило, дві швидкості – 'корисну', у байтах за секунду, і 'чисту', у бітах за секунду.

Як і в інших мережевих технологіях, підтримувані відстані й швидкості передачі залежать від типу використовуваного середовища передачі й генераторів сигналу. Fibre Channel може функціонувати як по оптичної, так і по мідному середовищу передачі.

Найбільші швидкості (до 4 Гбіт/с) і відстані (до 10 км) досягаються у випадку застосування одномодового оптичного волокна й низькочастотних лазерів. Багатомодове волокно здатне підтримувати такої ж швидкості, але на набагато менших відстанях, зокрема 100 Мбайт/с на відстанях до 500 м у випадку багатомодового волокна 50/125 мкм із високочастотним лазером. Мідне середовище передачі дозволяє підтримувати швидкості не вище основний на невеликих відстанях (100 м і менш).

Розробка структурної схеми

Дуже утрированно ідею Fibre Channel можна викласти так – аналог SCSI інтерфейсу для роботи з послідовних високошвидкісних каналів з можливістю комутації й маршрутизації потоків даних подібно звичайним Ethernet мережам і роботою на більших відстанях (до десятків кілометрів). Повторюємо, це дуже спрощене формулювання, але

основну суть інтерфейсу Fibre Channel вона відбиває. Часто багато з людей плутають Fibre Channel з оптичною реалізацією Ethernet, уважаючи що раз це оптика з такими ж оптичними кабелями, те й призначення те саме. Зрозуміло, це далеко жодне й те ж. Fibre Channel по суті поєднує високу швидкість SCSI інтерфейсу й переваги мережевої топології.

Технічні характеристики:

Швидкість передачі даних – 1 Gbit/s, 2 Gbit/s, 4 Gbit/s і 8 Gbit/s. С обліком того, що для з'єднання пристроїв застосовуються два оптичних кабелі, кожний з яких працює в одному напрямку, при збалансованому наборі операцій запис/читання швидкість обміну даними подвоюється, тобто Fibre Channel працює в повнодуплексному режимі. У перерахуванні на мегабайтів паспортна швидкість Fibre Channel становить відповідно 100 MByte/s, 200 MByte/s, 400 MBytes/s, 800 Mbytes/s. Реально при 50% співвідношенні операцій запису/читання швидкість інтерфейсу досягає 200 MByte/s, 400 MByte/s і 800 MBytes/s. У майбутньому повинен з'явитися варіант на 16 Gbit/s або 1600 Mbyte/s. Найбільш популярні рішення Fibre Channel на 4 Gbit/s, оскільки вони мають краще співвідношення ціна/якість.

Як і в SCSI інтерфейсі, протоколи сумісні – пристрій з FC-AL на 4 Gbit/s буде працювати з контролером на 1 Gbit/s і навпаки. Зрозуміло, швидкість передачі даних у подібній парі буде визначатися по самому повільному із пристроїв.

Дальність роботи – до 300 метрів на оптичних багатомодових кабелях і повній швидкості інтерфейсу, до 10 кілометрів на одномодовом кабелі. Для переходу із багатомодового на одномодовий кабель потрібні спеціальні перетворювачі вартістю від $600 за пару.

Реалізація фізичного каналу – або мідь, але тільки на швидкостях не вище 1 Gbit/s, або оптоволокно багатомодове 50/125 мкм і 62,5/125 мкм із з'єднувачами типу SC або, що частіше зустрічається, LC.

Топологія

Топологія Fibre Channel. Незважаючи на те, що формально Fibre Channel не є мережевим інтерфейсом, його топологія має багато схожа з мережевою топологією. Отже, топологія Fibre Channel може бути:

Arbitrated Loop (Петля з арбітражем, скорочено AL)

Це послідовне з'єднання пристроїв у кільце. Вихід одного пристрою з'єднується із входом наступного, його вихід у свою чергу із входом наступні й т.д. Усього в такій петлі може брати участь до 127 пристроїв. На AL топологію на момент створення стандарту покладали більші надії. Оскільки в Fibre Channel використовується абсолютна адресація пристрою, те більших втрат і затримок у петлі не виникає, при цьому AL дозволяє уникнути покупки дорогого Fibre Channel комутатора. Але з ростом швидкостей обміну даними AL стала негативно позначатися на продуктивності систем. До того ж в AL є два істотних недоліки: вихід з ладу хоча б одного пристрою приводить до відмови всієї системи й додавання/ виключення пристрою вимагає зупинки роботи всієї системи хоча б на короткий час.

Point-To-Point (Точка – точка)

У цьому варіанті робота з Fibre Channel практично нічого не відрізняється від SCSI, хіба що відстані між пристроями можуть бути на порядки більше.

Switched Fabric (Комутуєма структура, комутуєма матриця)

Сама популярна топологія Fibre Channel зараз і з високою часткою ймовірності в майбутньому.

Ця топологія близька до зрозумілої багатьом топології звичайної мережі – є комутатор і пристрої, до комутатора підключені. Незважаючи на подібність Switched Fabric на мережу, реально ця топологія функціонує трохи по іншому, про що піде мова нижче. Помітьте, що й назва говорить саме за себе – перемикається матриця, що, ніяк не асоціюється з хабом або маршрутизатором звичайного Ethernet. Сучасні Switched Fabric, такі як QLogic SANBox 5800 на 20 FC портів, мають агреговану смугу пропущення 544 Gbits/s, тобто 20 портів на 8+8 Gbits/s плюс смуга, необхідна для каскадування (підключення до інший Switched Fabric).

Види портів Fibre Channel:

– NL_port – (Node Loop – Вузол петлі) порт на пристрої, через який пристрій підключений до Arbitrated Loop (Петля з арбітражем).

– FL_port – (Fabric Loop – Порт у петлі) порт на зовнішньому пристрої, що з'єднується з комутирується матрицей, що (fabric). Зрозуміло, топологія підключення в цьому випадку Arbitrated Loop (Петля з арбітражем).

– L_port (Loop port – Порт у петлі) просто термін, що поєднує й FL_port і NL_port.

– N_port (Node – Вузол) порт на пристрої, через який пристрій підключений по Point-To-Point (Точка – точка) топології.

– F_port (Fabric port – Порт матриці) порт на комутирується матрице, що, у топології Switched Fabric (Комутирується структура, що, що комутирується матриця).

– E_port (Expansion port – Порт розширення) порт, що з'єднує дві матриці, що комутуються між собою. Зв'язок, що з'єднує два E_port, звичайно називається ISL.

– TE_port (Trunking Expansion – З'єднання для розширення) – цей термін використовується для опису декількох портів, об'єднаних разом для збільшення смуги пропущення.

– G_port (Generic – Загальний, найпростіший) – порт, емулюючий F_port або E_port.

Безумовно, технічні дані про Fibre Channel цікаві самі по собі, але не зрозумівши практичного змісту у використанні Fibre Channel, не можна по достоїнству оцінити всі переваги цього чудового інтерфейсу. Тому ми плавно переходимо до прикладів практичної реалізації систем на Fibre Channel.

Отже, що ми маємо зараз у переважній більшості організацій? Залежно від розміру організації, кількості оброблюваних даних, кількості користувачів і т. П. ми бачимо n серверів різного рівня й продуктивності, кожний зі своїм дисковим RAID масивом і всі обміни даними в організації здійснюються через локальну мережу. Згодом сервера утворять своєрідний зоопарк різних моделей, різної продуктивності й різних по можливостях. Під кожне нове завдання або для кращого рішення старої, як правило, купується новий сервер знову ж зі своїм дисковим масивом, потім він перестає справлятися зі своїми обов'язками, купується наступний сервер і процес повторюється.

Проблеми такий, можна сказати, класичної архітектури побудови мережі підприємства, зовсім очевидні:

– Кожний сервер коштує досить великих грошей, оскільки в складі сервера обов'язково присутній недешевий RAID масив.

– Перенос програмного забезпечення й даних зі старого сервера на новий трудомісткий і особливо складний у випадку неможливості зупинки старого сервера.

– Створення кластера (кластерів) вимагає покупки спеціального комплекту (комплектів) устаткування.

– Весь обмін даними в організації йде через локальну мережу. Які би гарні маршрутизатори не застосовувалися, з ростом обсягу даних мережа регулярно стає вузьким місцем і продуктивність всієї комп'ютерної системи організації знижується. Установка нового сервера (серверів) і нових комутаторів дозволяє якось "розшити" вузькі місця, але згодом, якщо організація збільшується або її обсяги ростуть, усе повторюється спочатку. До того ж реальна пропускна здатність навіть гігабітної мережі невелика, оскільки навіть досить дорогі мережеві комутатори не забезпечують сумарну смугу пропущення рівній сумі всіх потоків через комутатор.

– Неможливий перерозподіл ресурсів дискової пам'яті між серверами. Таке завдання рівносильне заміні цілком сервера, що, до речі, часто й робляться.

– Адміністрування системи, що складає з різномастого встаткування й не має програмних засобів для керування всією системою в цілому занадто залежить від конкретних людей.

– Сервера встановлюються в одній або декількох кімнатах, що при техногенній аварії (прорив води наприклад, або опалення, пожежі, нарешті) приводить до величезних втрат – і дані губляться й сервера виходять із ладу. Відновлення системи може зажадати масу часу й грошей.

Багато просунутих керівників IT підрозділів почали використовувати зовнішні SCSI to IDE/SATA системи зберігання даних. Це дозволяє "відв'язати" хоча б дискову пам'ять від конкретного сервера і якщо буде потреба міняти тільки один компонент, яким як правило, є сервер, обчислювальних можливостей якого часто не вистачає. У цьому варіанті можна купувати сервера тільки виходячи з їхніх обчислювальних можливостей і не платити щораз за великий убудований дисковий масив.

Безумовно, така архітектура більше зручна, ніж класична, але вона вирішує тільки малу частину проблем і не ліквідує головні проблеми – високе навантаження на мережу й труднощі адміністрування системи. Тому далі ми розповімо про зовсім інший варіант побудови серверної системи підприємства.

Використання переваг Fibre Channel як високошвидкісної спеціалізованої мережі для передачі даних дозволяє принципово змінити архітектуру обчислювальної мережі організації. Fibre Channel дає можливість відокремити всі потоки даних між серверами підприємства, архівування даних і т. П. від локальної мережі користувачів.

У цьому варіанті можливості з конфігурування величезні – будь-який сервер може звертатися до будь-яким, дозволеним адміністратором системи дисковому ресурсу, можливий доступ до тому самому диска декількох пристроїв одночасно, причому з високою швидкістю, що не йде ні в яке порівняння зі швидкістю передачі даних по Ethernet. Не забувайте, що для кожного комп'ютера, підключеного до дискового ресурсу цей ресурс представляється як локальний. У цьому варіанті й backup даних стає легким і прозорим завданням. У будь-який момент можна створити кластер, визволивши під нього ресурси на кожній з FC систем зберігання. Масштабування також досить наочно й зрозуміло – залежно від того, недостача яких можливостей виникла, можна або додати сервер, що буде куплений виходячи винятково з його обчислювальних можливостей, або додати нову систему зберігання.

Існує досить багато різного програмного забезпечення, яке дозволяє фактично управляти всіма системами зберігання як єдиним масивом + адміністрування, у результаті чого й виходить SAN (Storage Area Network). Зрозуміло, що в цій схемі є очевидний елемент ненадійності – єдина комутуєма матриця, для всіх серверів і систем зберігання. Цей недолік легко вбирається установкою дублюючої другої матриці. Завдяки продуманій архітектурі Fibre Channel, друга матриця може працювати "паралельно" з першої й у випадку виходу будь-якої матриці з ладу система в цілому цього просто не помітить. Правильні системи зберігання, у свою чергу, мають 2 канали Fibre Channel (4 порти), що також уможливлює розпаралелювання процесів за допомогою другої матриці. На рисунку 3.1 ви можете бачити структурну схему системи у вигляді спрощеної схеми системи з дублюванням.

Не можна не розповісти ще про одну досить важливу й потрібну особливість Fibre Channel – можливості сегментування або, як прийнято в термінології Fibre Channel, зонування системи. Поділ на зони подібно поділу на віртуальні мережі (VLAN) у локальній мережі – пристрої, що перебувають у різних зонах, не можуть "бачити" один одного. Поділ на зони можливо або за допомогою комутирується матриці, що (Switched Fabric) або на основі вказівки адреси WWN (World Wide Name). Адреса WWN подібна MAC адресі в мережах Ethernet, кожний FC контролер має свою унікальну WWN адресу, що привласнює йому виробник, а будь-яка правильна система зберігання даних дозволяє ввести адреси тих контролерів або портів матриць, з якими цьому пристрою дозволений працювати. Поділ на зони призначено в першу чергу для підвищення безпеки й продуктивності мереж зберігання даних. У відмінності від звичайної мережі, із зовнішнього миру не можна "проломити" зони й одержати доступ до закритого для даної зони пристрою.

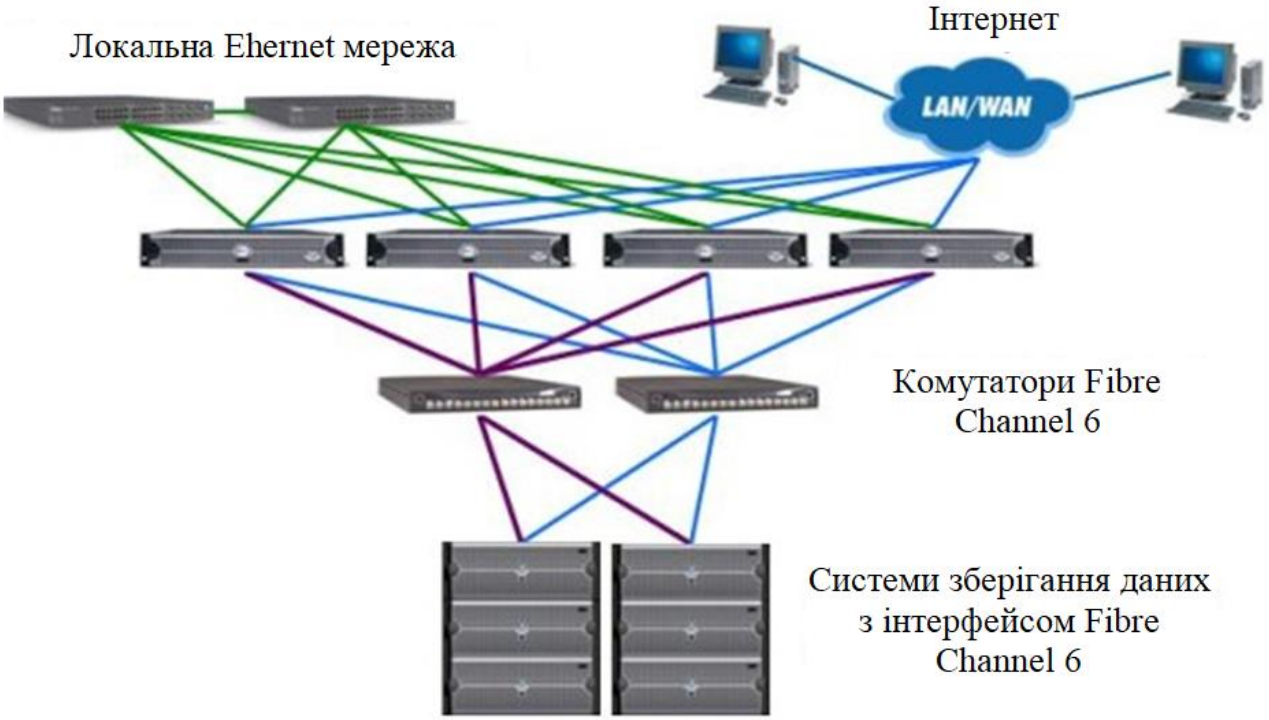


Рисунок 1 – Структурна схема системи

Зрозуміло, сфера застосування Fibre Channel не обмежується тільки серверними системами підприємств. Один із самих цікавих напрямків використання – робота з відео й цифровим кіно (Digital Cinema). Історично в Україні компанії, що працюють із кіно/відео матеріалом були одними з перших споживачів зовнішніх систем зберігання даних. Причина очевидна – кіно/відео матеріал вимагає величезних обсягів дискової пам'яті й без зовнішніх дискових масивів у багатьох випадках було просто неможливо працювати над проектами. Зараз в Україні є чимало кіно-, відео-компаній, у яких кількість систем зберігання даних обчислюється десятками.

Але, з ростом ринку кіно й телебачення в Україні зросла спеціалізація співробітників, що займаються комп'ютерною обробкою кіно- відео- матеріалів і виникла серйозна проблема – як обробляти матеріал послідовно декільком фахівцям? Або треба пересаджувати їх з однієї робочої станції на іншу й тим самим пропустити всіх необхідних людей через станцію, до якої підключений зовнішній дисковий масив з конкретним фільмом, або переганяти матеріал по мережі з одного масиву на інший, або (не варто сміятися, ми це бачили на власні очі), перетаскувати систему зберігання від одного комп'ютера до іншого. Система зберігання, до речі, може важити від 15 до 40 кілограмів. Всі ці способи досить помітно збільшують час роботи над проектом, оскільки навіть перекачування по мережі з однієї робочої станції на іншу терабайтів даних процес тривалий. Зрозуміло, що у відмінності від бізнес-застосунків, обробка відео по локальній мережі неможлива, занадто мала швидкість обміну даними.

Тому для компаній, що займаються post-production, застосування Fibre Channel є самим логічним виходом із цієї ситуації й ряд компаній уже успішно застосовують у своїй роботі Fibre Channel. Структура системи в цьому випадку не відрізняється від раніше розглянутої, просто замість серверів у систему входять робочі станції. У цьому варіанті всі проблеми відпадають – по завершенні чергового етапу інший співробітник починає займатися тим же самим фільмом, нікуди не переміщаючи файли й анітрошки не втрачаючи у швидкості доступу до даних. Використовуючи спеціалізоване програмне забезпечення, цілком можлива й одночасна робота декількох користувачів над одним проектом, що істотно прискорює процес. При обробці серіалів такі переваги Fibre Channel просто життєво необхідно використовувати.

Є ще одна серйозна причина для переходу на Fibre Channel – шум. Системи зберігання даних містять у собі, як правило, до 16 жорстких дисків, кілька блоків живлення й вентилятори охолодження. Все це технічна пишнота, на жаль, шумить і шумить помітно. Якщо для бізнес-застосунків це не настільки важливо, оскільки сервера й системи зберігання звичайно перебувають у спеціальних приміщеннях, у яких персонал постійно відсутній, то для людей, що займаються творчістю з ранку до вечора шум є досить серйозною проблемою. Працюючи з SCSI системами зберігання, компанії йдуть на різні хитрування для ліквідації шуму. Наприклад, забирають робочі станції разом із системами зберігання в ізольовані приміщення, подовжуючи кабелі до миші, клавіатурі й монітору. Є й інші, не менш заморочливі варіанти. Застосування ж Fibre Channel ліквідує проблему шуму як клас. Припустимого для FC інтерфейсу відстані в сотні метрів від комп'ютера з лишком вистачить для видалення системи зберігання від робочої станції в будь-якому будинку.

Купили, підключили, але як всім цим управляти?

Питання правильний і своєчасний. Отже, уявимо собі, що ми купили декілька Fibre Channel систем зберігання, підключили до нього кілька серверів у корпоративній системі або робітники станції для групової обробки відео в кінокомпанії. Що далі? Проблема в тому, що Fibre Channel дискова система зберігання з погляду комп'ютера є звичайний внутрішній локальний диск, підключений через звичайний дисковий контролер. Відповідно, якщо до цьомго FC диску буде мати доступ кілька комп'ютерів, то зовсім незрозуміло, яким образом і хто буде стежити за тим, щоб один комп'ютер не записував у ті самі місця диска одночасно з іншим комп'ютером? Та й просто як одному комп'ютеру хоча б побачити, що хтось чужий таємничим образом змінив уміст його внутрішнього диска?

Рішення, а точніше спосіб не рішення цього завдання істотно залежить від сфери застосування.

Бізнес

Найчастіше в бізнес застосуваннях не потрібний поділ одного локального дискового простору між декількома комп'ютерами або такий поділ штатно підтримується операційною системою (типовий приклад – кластер). У багатьох бізнес застосуваннях адміністратори цілком задовольняються гнучкими можливостями Fibre Channel систем по перерозподілі дискового простору між комп'ютерами, легкістю конфігурування, можливостям по масштабуванню й т. П. Тому в бізнес застосуваннях можна обмежитися штатними можливостями адміністрування, які надають як Fibre Channel матриці, так і самі системи зберігання.

Цифровий кінематограф і телебачення

Тут теж часто застосовується простий підхід – віртуальна "перекидання" дисків від одного користувача до іншого залежно від етапів роботи над проектом, або елементарне тверде закріплення певного дискового простору за конкретним комп'ютером (користувачем). До того ж кваліфікація системних адміністраторів у кіно- відео- компаніях найчастіше буває набагато нижче, ніж у великих комерційних структурах, банках і т. П. і саме по собі застосування Fibre Channel у кіно- відео- багатьом їхнім керівникам і технічному персоналу здається, на жаль, непотрібним. На щастя, останнім часом Fibre Channel стає усе більше й більше популярним навіть у невеликих студіях.

Зрозуміло, варіанти "вижимання" з Fibre Channel систем усього, що вони вміють і можуть, є, але проблема в масовому незнанні цих можливостей. Якщо перебільшувати проблему, то її можна сформулювати в такий спосіб – як, зберігаючи величезні швидкості обміну даними, можливості гнучкого апаратного налаштування, масштабування й т. П. управляти SAN як локальною мережею?

Програма дозволяє набудовувати й управляти практично всіма можливостями SAN, додаючи до них такі корисні речі як перемикання трафіку на LAN у випадку обриву кабелю або виходу з ладу FC контролера, керування смугою пропущення й т. П. Переваги – великі можливості з адміністрування, відсутність виділеного сервера метаданих, гарний захист від збоїв, немає прив'язки до конкретних типів матриць – систем зберігання – FC контролерів.

До переваг варто віднести підтримку крім Windows також Mac OS і Linux Red Hat. Недоліки – відносно висока вартість рішення, складова $1100 на комп'ютер, підключений до SAN.

Ціна питання

Ще кілька років тому назад Fibre Channel могли застосовувати тільки дуже небідні організації. Комутатори (Switched Fabric) коштували до десятків тисяч доларів, контролери по кілька тисяч. Ціни на системи зберігання теж не радували – FC системи зберігання коштували на $ 1500-2000 більше, ніж точно такої ж системи з SCSI інтерфейсом. Але останнім часом, завдяки популярності, що розширюється, Fibre Channel ціни стали помітно знижуватися. На весну 2020 року ситуація така:

Контролери PCI Express – $900 за порт.

Комутатори (Switched Fabric) – $450 за порт

Системи зберігання – на $400 дорожче аналогічні з SAS інтерфейсом.

Недешево, скаже потенційний покупець, який придивлявся до можливостей Fibre Channel. На перший погляд це дійсно так. Але, за рахунок зовсім іншої конфігурації системи застосування Fibre Channel дозволить заощадити значні суми на відмові від застосування в серверах дорогих RAID контролерів і дисків, на значно менші витрати на розширення системи і її адміністрування. Звичайно, застосування Fibre Channel для двох-трьох серверів або робочих станцій економічно невиправдано – але для більших або систем, що розвиваються, їсти зміст відразу використовувати Fibre Channel, оскільки це дасть істотну економію при масштабуванні

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів зберігання даних з використанням технології Fibre Channel 6. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем зберігання даних з використанням технології Fibre Channel 6. Досліджена система зберігання даних з використанням технології Fibre Channel 6. На основі отриманих результатів досліджень створена програмна реалізація системи зберігання даних з використанням технології Fibre Channel 6. Розроблені алгоритми дозволяють успішно вирішувати завдання зберігання даних з використанням технології Fibre Channel 6. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. зі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.

7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція “Проблеми й перспективи розвитку ІТ-індустрії” м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ “ХПИ”, 2009. – С.52-53.
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.

УДК 004

С. Смірнов, магістр гр. КІ-20МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ХМАРНОГО АНТИВІРУСНОГО ЗАБЕЗПЕЧЕННЯ

У статті розроблено програмне забезпечення, яке призначено для системи хмарного антивірусного забезпечення. Метою розробки є дослідження та програмна реалізація системи хмарного антивірусного забезпечення.Об’єктом дослідження є процес хмарного антивірусного забезпечення. Предметом дослідження є методи хмарного антивірусного забезпечення. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи хмарного антивірусного забезпечення В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерна інженерія, хмари, антивірусне забезпечення

Постановка проблеми. Масове застосування персональних комп'ютерів, на жаль, виявилося пов'язаним з появою програм-вірусів, що самовідтворюються, які перешкоджають нормальній роботі комп'ютера та руйнують файлову структуру дисків і наносять збиток збереженої в комп'ютері інформації. Це ж й відноситься до комп’ютерів приєднаних до Інтернету, або інших пристроїв, які під’єднані до Інтернету.

Щоб ефективно боротися з вірусами, необхідно мати подання про структуру алгоритмів вірусів і орієнтуватися в методах протидії вірусам. Вірусом називається спеціально створена програма, здатна самостійно поширюватися в комп'ютерному середовищі. Якщо вірус потрапив у комп'ютер разом з однією із програм або з файлом документа, то через якийсь час інші програми або файли на цьому комп'ютері будуть заражені. Якщо комп'ютер підключений до локальної або глобальної мережі, то вірус може поширитися й далі, на інші комп'ютери. Автори вірусних програм створюють їх з різних спонукань, однак результати роботи вірусів виявляються, як правило, схожими: інфекції псують програми й документи, які знаходяться на комп'ютері, що часто приводить до їхньої втрати. Деякі віруси здатні знищувати взагалі всю інформацію на дисках комп'ютерів, вартість якої може в десятки й сотні разів перевищувати вартість самого комп'ютера.

Для захисту від вірусів можна використовувати:

– загальні засоби захисту інформації, які корисні також і як страховка від фізичного псування дисків, що неправильно працюють програм або помилкових дій користувачів;
– профілактичні міри, що дозволяють зменшити ймовірність зараження вірусом;
– спеціалізовані програми для захисту від вірусів.

Загальні засоби захисту інформації корисні не тільки для захисту від вірусів. Є два основні різновиди цих засобів:
– копіювання інформації – створення копій файлів і системних областей дисків;
– розмежування доступу запобігає несанкціоноване використання інформації, зокрема, захист від змін програм і даних вірусами, що неправильно працюють програмами й помилковими діями користувачів.

Існують три рубежі захисту від комп'ютерних вірусів:
– запобігання надходження вірусів;
– запобігання вірусної атаки, якщо вірус все-таки надійшов на ПК;
– запобігання руйнівних наслідків, якщо атака все-таки відбулася.

Існують три методи реалізації захисту:
– Програмні методи захисту.
– Апаратні методи захисту.
– Організаційні методи захисту.

Хмарні антивіруси відносяться до програмних методів захисту, хоча, якщо будувати комплексну систему захисту від вірусів, то потрібно використовувати усі вище перераховані методи.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи хмарного антивірусного забезпечення

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи хмарного антивірусного забезпечення.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:
– Огляд існуючих систем хмарного антивірусного забезпечення.
– Дослідження системи хмарного антивірусного забезпечення.
– Програмна реалізація системи хмарного антивірусного забезпечення.

Об'єктом дослідження є процес хмарного антивірусного забезпечення.

Предметом дослідження є методи хмарного антивірусного забезпечення.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Перш, ніж розглядати хмарне антивірусне забезпечення, розглянемо, що таке антивірусне ядро й що таке хмарне антивірусне забезпечення.

Антивірусне ядро – реалізація механізму сигнатурного сканування й евристичного аналізу на основі наявних сигнатур вірусів.

Хмарне антивірусне забезпечення – набір антивірусів, що використовують однакове антивірусне ядро або ядра, призначений для рішення практичних проблем по забезпеченню антивірусної безпеки комп'ютерних систем. В хмарне антивірусне забезпечення також в обов'язковому порядку входять засоби відновлення антивірусних баз.

Крім цього хмарне антивірусне забезпечення додатково може містити в собі поведінкові аналізатори й ревізори змін, які зовсім не використовують антивірусне ядро.

Як допоміжна утиліта хмарне антивірусне забезпечення може містити (і на практиці звичайно містить) планувальник завдань.

Виходячи з поточної необхідності в засобах захисту виділяють наступні типи хмарного антивірусного забезпечення:
– Хмарне антивірусне забезпечення для захисту робочих станцій.

– Хмарне антивірусне забезпечення для захисту файлових серверів.
– Хмарне антивірусне забезпечення для захисту поштових систем.
– Хмарне антивірусне забезпечення для захисту шлюзів.

Хмарне антивірусне забезпечення для захисту робочих станцій

Призначений для забезпечення антивірусного захисту робочої станції, на якій він установлений. Складається, як і вказувалося раніше із засобів безперервної роботи й призначених для періодичного запуску, а також засобів відновлення антивірусних баз.

До засобів безперервної роботи відносяться:

– Антивірусний сканер при доступі – антивірусний сканер, що здійснює перевірку файлів, до яких звертається операційна система (прямо, або опосередковано через користувача). Для прискорення процесу роботи сканера часто застосовується можливість відключення засобів евристичного аналізу.

– Антивірусний сканер локальної поштової системи – антивірусний сканер, призначений для автоматичної перевірки всієї вхідної й вихідної із системи поштової кореспонденції до одержання її користувачем/вихідним поштовим сервером. Цей тип сканерів з'явилася порівняно недавно, його розробка обумовлена тим, що більшість вірусів використовує для поширення електронну пошту. Виділяють два види сканерів локальної поштової системи – що використовують і не використовують прив'язку до поштового клієнта. Перший тип характеризується великим числом підтримуваних поштових протоколів, однак можливості практичного застосування звужуються необхідністю використовувати конкретний поштовий клієнт. Другий тип, навпроти, підтримує більше обмежений набір протоколів (звичайно, SMTP і POP3), однак робить це для будь-яких поштових клієнтів. Можливе використання обох типів сканерів у рамках одного антивірусного комплексу.

Засоби періодичного запуску:

– Антивірусний сканер на вимогу – антивірусний сканер, що здійснює перевірку файлів по запиту користувача або третьої програми (наприклад, планувальника). На практиці хмарне антивірусне забезпечення для робочої станції найчастіше включає ще й поведінкові блокатори, що також відносяться до засобів безперервної роботи.

Хмарне антивірусне забезпечення для захисту файлових серверів

Призначений для забезпечення антивірусного захисту сервера, на якому встановлений. Вказівка на файловий сервер у назві є скоріше даниною історії, більш коректно буде звучати термін «мережний». Визначення того, наскільки має потребу в антивірусному захисті сервер, здійснюється не тільки виходячи з його призначення (є сервер файловим, поштовим, або виконує іншу функцію), а й з використовуваної на ньому платформи. Більше того, найчастіше саме платформа є визначальною характеристикою при виборі засобів захисту мережного сервера. Мова про це піде нижче.

Відмінності в складі антивірусного комплексу для файлового сервера, у порівнянні з хмарним антивірусним забезпеченням для робочої станції, походять із різного призначення цих типових вузлів мережі, а точніше з головного розходження: робоча станція звичайно є АРМ співробітника, тоді як сервер у якості АРМ не використовується.

Виходячи із цього, хмарне антивірусне забезпечення для захисту файлових серверів звичайно складається із двох яскраво виражених представників засобів безперервного роботи й періодичного запуску:

– Антивірусного сканера при доступі – аналогічний сканеру при доступі для робочої станції.

– Антивірусного сканера на вимогу – аналогічний сканеру на вимогу для робочої станції.

А також засобу відновлення антивірусних баз.

Сканер локальної поштової системи відсутній з описаної вище причини.

Хмарне антивірусне забезпечення для захисту поштових систем

Безумовно, хмарне антивірусне забезпечення не призначений для захисту поштової системи від поразки вірусами, його призначення – перешкоджати доставці заражених повідомлень користувачам мережі. Як уже вказувалося раніше, сьогодні одним з головних засобів доставки вірусів у локальну мережу є саме електронна пошта. Тому, при наявності в локальній мережі спеціалізованого вузла, що обробляє вхідну й вихідну з мережі поштову кореспонденцію (поштового сервера), логічно буде використовувати засіб централізованої перевірки всього поштового потоку на наявність вірусів. Проте, термін «для захисту поштових систем» є устояним і повсюдно застосовується при вказівці практичних реалізацій цього типу комплексів.

Хмарне антивірусне забезпечення для захисту поштових систем, як і інші антивірусні комплекси включає хмарні антивіруси обох типів.

Засоби безперервної роботи:

– Фільтр поштового потоку – здійснює перевірку на наявність вірусів усього прийнятого й поштового потоку, що відправляється, сервера, на якому встановлений комплекс.

– Сканер загальних папок (баз даних) – здійснює перевірку на наявність вірусів баз даних і загальних папок користувачів у режимі реального часу (у момент звертання до цих папок або баз). Може становити єдине ціле з фільтром поштового потоку залежно від реалізації технології перехоплення повідомлень/звертань до папок і передачі на перевірку.

Засоби періодичного запуску:

– Антивірусний сканер на вимогу – здійснює перевірку на наявність вірусів поштових скриньок користувачів і загальних папок у випадку використання таких на поштовому сервері. Перевірка здійснюється на вимогу адміністратора антивірусної безпеки або у фоновому режимі. Якщо перевірка виконується у фоновому режимі, сканер також відноситься до засобів періодичного запуску, оскільки нічим не відрізняється від сканера на вимогу в комплексі для робочої станції.

Також, хмарне антивірусне забезпечення для захисту поштових систем обов'язково включає засіб відновлення антивірусних баз. Додатково, для зниження навантаження на сервер можуть виділятися окремі засоби для перевірки баз під час реплікацій. Такі засоби також відносяться до засобів періодичного запуску.

Хмарне антивірусне забезпечення для захисту шлюзів

Хмарне антивірусне забезпечення для захисту шлюзу, як виходить з назви, призначений для перевірки на наявність вірусів даних, через цей шлюз переданих.

На практиці основними каналами доставки вірусів у локальну мережу є SMTP, HTTP і FTP-потоки, отже, хмарне антивірусне забезпечення для захисту шлюзів переважно включає засоби безперервної роботи. Хмарні антивіруси періодичного запуску використовуються рідко, переважно для захисту файлової системи сервера, на якому встановлений комплекс:

– Сканер HTTP-потоку – призначений для перевірки даних, переданих через шлюз по протоколу http.

– Сканер FTP-потоку – призначений для перевірки даних, переданих через шлюз по протоколу FTP. У випадку використання FTP over HTTP FTP-Запити будуть перевірятися сканером HTTP-потоку.

– Сканер SMTP-потоку – призначений для перевірки даних, переданих через шлюз по SMTP.

Природно, як і в попередніх випадках у комплекс в обов'язковому порядку входить засіб для відновлення антивірусних баз.

Комплексний підхід до забезпечення антивірусної безпеки передбачає погоджене застосування правових, організаційних і програмно-технічних мір, спрямованих на захист від можливих атак зловмисників. Відповідно до цього підходу в організації повинен бути реалізований наступний комплекс мер:

– заходи щодо виявлення й усуненню вразливостей, на основі яких реалізуються вірусні погрози. Це дозволить виключити причини можливого виникнення вірусних атак;

– міри, спрямовані на своєчасне виявлення й блокування вірусних атак;

– міри, що забезпечують виявлення й ліквідацію наслідків вірусних погроз. Даний клас мір захисту спрямований на мінімізацію збитку, нанесеного в результаті реалізації вірусних погроз.

Важливо розуміти, що ефективна реалізація перерахованих вище мір на підприємстві можлива тільки за умови наявності нормативно-методичного, технологічного й кадрового забезпечення антивірусної безпеки.

Нормативно-методичне забезпечення антивірусної безпеки припускає створення збалансованої правової бази в області захисту від вірусних погроз. Для цього в компанії повинен бути розроблений комплекс внутрішніх нормативних документів і процедур, що забезпечують процес експлуатації системи антивірусної безпеки. Склад таких документів багато в чому залежить від розмірів самої організації, рівня складності комп'ютерної мережі (КМ), кількості об'єктів захисту й т.д. Так, наприклад, для великих організацій основним нормативним документом в області захисту від шкідливого коду повинна бути концепція або політика антивірусної безпеки. Для невеликих компаній досить розробити відповідні інструкції й регламенти роботи користувачів, а також включити вимоги до забезпечення антивірусного захисту до складу політики інформаційної безпеки організації.

У рамках кадрового забезпечення антивірусної безпеки в компанії повинен бути організований процес навчання співробітників з питань протидії вірусним погрозам. Програма навчання повинна бути спрямована на мінімізацію ризиків, пов'язаних з помилковими діями користувачів, що приводять до реалізації вірусних атак. Прикладами таких дій є: запуск додатків з неперевірених зовнішніх носіїв, використання нестійких до вгадування паролів доступу, накачування Active-X об'єктів з недовірених Web-сайтів і інше. У процесі навчання повинні розглядатися як теоретичні, так і практичні аспекти антивірусного захисту. При цьому програма навчання може складатися залежно від посадових обов'язків співробітника, а також від того до яких інформаційних ресурсів він має доступ.

Технологічне забезпечення повинне бути спрямоване на створення комплексної системи антивірусного захисту (КСАЗ). Розглянемо підсистеми захисту, які повинні входити до складу КСАЗ для забезпечення захисту на рівні мережі, робочих станцій і серверів комп'ютерної мережі (КМ).

Захист на рівні мережі

Основним компонентом КСАЗ на рівні мережі є система розмежування доступу, що може реалізовуватися на трьох рівнях моделі OSI – канальному, мережному й прикладному. На канальному рівні розмежування доступу здійснюється на основі віртуальних локальних мереж VLAN (Virtual Local Area Network), на які розділяється КМ. Розподіл на такі віртуальні мережі виробляється за допомогою налаштувань комутаторів, у яких кожний фізичний порт включається в певну віртуальну мережу. Хости можуть вільно обмінюватися даними один з одним у рамках однієї віртуальної мережі, а керування взаємодією між різними віртуальними мережами здійснюється за допомогою списків контролю доступу ACL (Access Control List). У цих списках визначаються правила, відповідно до яких дозволяється або забороняється інформаційний обмін між різними мережами VLAN. Так, наприклад, якщо для роботи КМ два вузли не повинні обмінюватися між собою інформацією, то вони розділяються на різні віртуальні мережі, між якими забороняється взаємодія. У випадку, якщо комп'ютерний проникне на один з таких вузлів КМ йому не вдасться одержати доступ до тих ресурсам, які зберігаються на інших серверах, включених в інші віртуальні мережі.

На мережному й транспортному рівнях моделі OSI для розмежування доступу можуть застосовуватися міжмережні екрани, призначені для блокування потенційно небезпечних пакетів даних, на основі яких поширюються комп'ютерні віруси. Як правило, міжмережні

екрани встановлюються в точці підключення КМ до мережі Інтернет і забезпечують фільтрацію пакетів зі шкідливим кодом.

Розмежування доступу на прикладному рівні може реалізовуватися на основі технологій, що забезпечують можливість перевірки рівня безпеки робочих станцій перед наданням їм доступу до ресурсів КМ. Так, наприклад, якщо на робочій станції буде відсутнє антивірусне ПЗ, або не будуть оновлені сигнатурні бази даних, то в цьому випадку доступ станції до КМ буде заблокований. Прикладом такої технології є Cisco Network Admission Control.

На прикладному рівні моделі OSI рекомендується використовуватися мережні засоби виявлення й запобігання атак, призначені для виявлення несанкціонованої вірусної активності за допомогою аналізу пакетів даних, що циркулюють у КМ. Підсистема доповнює функції міжмережних екранів (МЕ) за рахунок можливості більш детального контентного аналізу вмісту переданих пакетів даних. Датчики системи виявлення атак установлюються до й після МЕ, а також у кожному із сегментів, що захищаються.

Крім системи виявлення атак для захисту КМ також рекомендується використання засобу аналізу захищеності, призначені для виявлення технологічних і експлуатаційних уразливостей КМ за допомогою проведення мережного сканування. Як об'єкти сканування можуть виступати робочі станції користувачів, сервери, а також комунікаційне встаткування.

На прикладному рівні також можуть використовуватися шлюзові засоби антивірусного захисту, що дозволяють сканувати файли, передані по мережних протоколах SMTP, POP3, HTTP, FTP і ін. Даний тип антивірусів підключається до міжмережного екрана, проксі-серверу або встановлюється в розрив каналу зв'язку на виділеному вузлі. На рівні шлюзу також може забезпечуватися захист від поштових повідомлень, що містять спам.

Засоби захисту від вірусних погроз на рівні мережі перераховані в таблиці 1.

Захист на рівні робочих станцій користувачів

Базовим елементом захисту робочих станцій є засоби антивірусного захисту (таблиця 2). Основне завдання даних засобів полягає в антивірусній перевірці всіх файлів, які надходять на робочу станцію по мережі або через зовнішні носії інформації. У доповненні до засобів антивірусного захисту на станції рекомендується встановлювати персональні мережні екрани, які дозволяють контролювати мережну активність додатків, а також хостові засоби виявлення атак. У випадку, якщо на станціях користувачів обробляється конфіденційна інформація, то вона повинна підлягати резервному копіюванню.

Таблиця 1 – Засоби захисту від вірусів на рівні мережі

№	Рівень моделі OSI	Найменування засобів захисту
1	Прикладний рівень	Шлюзові засоби антивірусного захисту Шлюзові засоби захисту від спаму Мережні системи виявлення атак Засоби контролю доступу до ресурсів КМ Засоби аналізу захищеності
2	Транспортний рівень	Міжмережні екрани
3	Мережний рівень	
4	Канальний рівень	Засоби розмежування доступу засобами VLAN
5	Фізичний рівень	Фізичне ізолювання певних сегментів КМ друг від друга

Таблиця 2 – Засоби захисту від вірусів на рівні робочих станцій користувачів

	Рівень моделі вузла КМ	Найменування засобів захисту
	Рівень інформаційних ресурсів	Засоби резервного копіювання інформації
	Рівень прикладного ПЗ	Засоби антивірусного захисту Персональні мережні екрани Хостові засоби виявлення й запобігання атак
	Рівень загальносистемного ПЗ	

	Рівень апаратного забезпечення	–

Захист на рівні серверів

На сервери, також як і на робочі станції повинні встановлюватися засоби антивірусного захисту, що забезпечують виявлення й блокування шкідливого коду. На відміну від робочих станцій, для забезпечення більш високого рівня захисту на сервери можуть установлюватися багатовендерні хмарні антивіруси, до складу яких одночасно входить кілька скануючих ядер різних виробників. Прикладом програмного продукту, що може використовуватися для реалізації КСАЗ, є система Antigen компанії Microsoft, призначена для антивірусного захисту серверів Exchange, SharePoint, SMTP-Шлюзів і іншого прикладного ПЗ. Даний продукт може містити в собі до восьми антивірусних ядер різних виробників.

Для захисту поштових серверів від спаму на них може бути встановлене спеціалізоване ПЗ, що дозволяє виявляти повідомлення рекламного характеру. Крім засобів захисту від вірусів і спаму на серверах доцільно розміщати засобу контролю цілісності інформаційних ресурсів, резервного копіювання, виявлення атак і мережного екранування.

Таблиця 3 – Засоби захисту від вірусів на рівні серверів

	Рівень моделі вузла КМ	Найменування засобів захисту
	Рівень інформаційних ресурсів	Засоби контролю цілісності інформації Засоби резервного копіювання інформації
	Рівень прикладного ПЗ	Засоби антивірусного захисту Засоби захисту від спаму Персональні мережні екрани Хостові засоби виявлення й запобігання атак
	Рівень загальносистемного ПЗ	
	Рівень апаратного забезпечення	–

Крім розглянутих вище засобів захисту КМ, що функціонують на рівні мережі, робочих станцій і серверів, до складу КСАЗ також повинна входити підсистема керування антивірусною безпекою, призначена для виконання наступних функцій:

– віддаленої установки й деінсталяції антивірусних засобів на серверах і робочих станціях користувачів;

– віддаленого керування параметрами роботи підсистем захисту, що входять до складу КСАЗ;

– централізованого збору й аналізу інформації, що надходить від інших підсистем. Дана функція дозволяє автоматизувати процес обробки даних, що надходять,, а також підвищити оперативність прийняття рішень по реагуванню на виявлені інциденти, пов'язані з порушенням антивірусної безпеки.

Структурна схема розміщення підсистем захисту, що входять до складу комплексної системи антивірусної безпеки в КМ показана на рисунку 1.

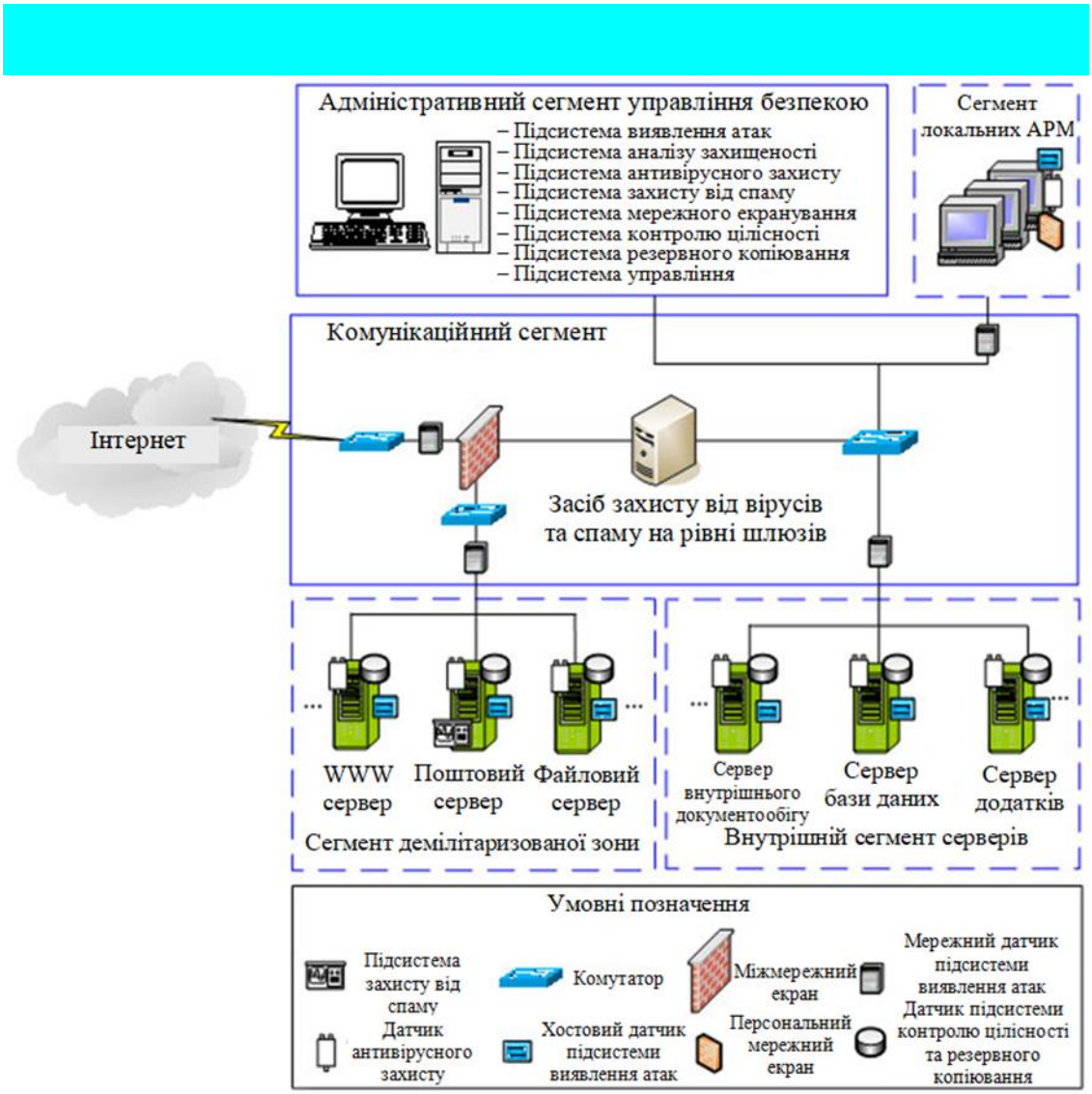


Рисунок 1 – Структурна схема системи

Важливо відзначити, що впровадження такої комплексної системи антивірусного захисту являє собою складний багатоступінчастий процес, що може містити в собі наступні етапи:

– аудит інформаційної безпеки КМ, що спрямований на збір вихідної інформації, необхідної для розробки плану впровадження КСАЗ;

– формування вимог до КСАЗ, призначеної для захисту КМ. На даному етапі формується технічне завдання на впровадження КСАЗ;

– розробка техноробочого проекту по впровадженню КСАЗ, що містить опис проектних рішень, схем установки, параметрів налаштування КСАЗ і інших службових даних;

– навчання персоналу організації, відповідального за адміністрування КСАЗ;

– пусконалагоджувальні роботи, пов'язані з розгортанням КСАЗ. У рамках даного етапу робіт спочатку створюється пилотна зона, у якій проводиться попереднє тестування впроваджуваної КСАЗ, після якого реалізується повномасштабне впровадження комплексу захисту в КМ;

– технічний супровід КСАЗ, у рамках якого вирішуються питання, пов'язані з обслуговуванням системи в процесі її експлуатації.

Склад етапів, а також їхня тривалість залежить від розмірності КМ, яка захищається, а також від масштабів впровадження КСАЗ. Роботи, пов'язані із впровадженням і експлуатацією СОА можуть проводитися як власними силами підприємства, так і із залученням зовнішніх організацій, що спеціалізуються на наданні послуг в області інформаційної безпеки.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів хмарного антивірусного забезпечення. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем хмарного антивірусного забезпечення. Досліджена система хмарного антивірусного забезпечення. На основі отриманих результатів досліджень створена програмна реалізація системи хмарного антивірусного забезпечення. Розроблені алгоритми дозволяють успішно вирішувати завдання хмарного антивірусного забезпечення. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
2. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
3. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
4. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
5. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
6. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
7. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.
8. Смирнов С. А. Комплекс gert-моделей технологии облачной антивирусной защиты телекоммуникационной системы / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Безпека інформації: наук. - практ. журн. – К.: НАУ, 2015. – Т. 21, № 3. – С. 251-262.
9. Смирнов С. А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А. А. Смирнов, А. К. Дидык, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2016. – № 2 (46). – С. 146-149.
10. Смирнов С. А. Модели системы нейросетевых экспертов безопасной маршрутизации в облачных антивирусных системах / А. А. Смирнов, А. К. Дидык, А. Н. Дреев, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2016. – Вип. 3 (140). – С. 36-39.

УДК 004

О. Смірнов, магістр гр. КІ-20МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті розроблено програмне забезпечення, яке призначено для системи стеганографічного захисту інформаційних ресурсів. Метою розробки є дослідження та програмна реалізація системи стеганографічного захисту інформаційних ресурсів. Об’єктом дослідження є процес стеганографічного захисту інформаційних ресурсів. Предметом дослідження є методи стеганографічного захисту інформаційних ресурсів. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи стеганографічного захисту інформаційних ресурсів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, стеганографічний захист, інформаційні ресурси

Постановка проблеми. У століття високих технологій інформація представляється найбільшою цінністю. Тому не дивно, що останнім часом створюється безліч засобів для її захисту. Серед відповідних напрямків найбільш розвинена криптографія – алгоритми постійно вдосконалюються, доводиться їхня стійкість.

Але в цього напрямку є, щонайменше, два мінуси. По-перше, на відміну від теоретичних принципів, у конкретні програмні реалізації можуть закрадатися помилки, що приводять до розшифровки за час, менший чим розрахунковий. По-друге, очевидно, що у зв'язку з розвитком технологій через якийсь час перебір, що займає на сучасному встаткуванні не один рік або навіть десятиліття, буде виконуватися за розумний час.

Стеганографія використовує принципово інший підхід. Вона приховує не тільки інформацію, але й сам факт її наявності. У цьому випадку в зловмисника не буде практично ніяких зачіпок, щоб догадатися, де вона може перебувати.

Основною метою комп'ютерної стеганографії є приховання файлу повідомлення усередині файлу-контейнера. Крім того, така операція повинна залишитися непоміченою – файл-контейнер зобов'язаний не втрачати функцій, а наявність схованого повідомлення повинно бути максимально складно виявити.

Як і будь-які інструменти, стеганографічні методи вимагають до себе уваги й обережного обігу, тому що можуть бути використані як для цілей захисту, так і для цілей нападу.

Комп'ютерні технології додали новий імпульс розвитку й удосконалюванню стеганографії, з'явився новий напрямок в області захисту інформації – комп'ютерна стеганографія (КС).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи стеганографічного захисту інформаційних ресурсів”

Мета й завдання дослідження Метою роботи є дослідження та програмна реалізація системи стеганографічного захисту інформаційних ресурсів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем стеганографічного захисту інформаційних ресурсів.
– Дослідження системи стеганографічного захисту інформаційних ресурсів.
– Програмна реалізація системи стеганографічного захисту інформаційних ресурсів.

Об'єктом дослідження є процес стеганографічного захисту інформаційних ресурсів.

Предметом дослідження є методи стеганографічного захисту інформаційних ресурсів.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Дамо опис алгоритмів стеганографії, яки використовуються у цій магістерській роботі. У цей час методи комп'ютерної стеганографії розвиваються по двох основних напрямках:

1. Методи, засновані на використанні спеціальних властивостей комп'ютерних форматів;

2. Методи, засновані на надмірності аудіо й візуальної інформації.

Порівняльні характеристики існуючих стеганографічних методів наведені в таблиці 1.

Таблиця 1 – Порівняльні характеристики стеганографічних методів

Стеганографічні методи	Коротка характеристика методів	Недоліки	Переваги
1. Методи використання спеціальних властивостей комп'ютерних форматів даних			
1.1. Методи використання зарезервованих для розширення полів комп'ютерних форматів даних	Поля розширення є в багатьох мультимедійних форматах, вони заповнюються нульовою інформацією й не враховуються програмою	Низький ступінь скритності, передача невеликих обмежених обсягів інформації	Простота використання

Стеганографічні методи	Коротка характеристика методів	Недоліки	Переваги
1.2. Методи спеціального форматування текстових файлів			
1.2.1. Методи використання відомого зсуву слів, пропозицій, абзаців	Методи засновані на зміні положення рядків і розміщення слів у пропозиції, що забезпечується вставкою додаткових пробілів між словами	1. Слабка продуктивність методу, передача невеликих обсягів інформації 2. Низький ступінь скритності	Простота використання. Є опубліковане програмне забезпечення реалізації даного методу
1.2.2. Методи вибору певних позицій букв (нульовий шифр)	Акровірш – окремий випадок цього методу (наприклад, початкові букви кожного рядка утворять повідомлення)		
1.2.3. Методи використання спеціальних властивостей полів	Методи засновані на використанні спеціальних "невидимих", схованих		

форматів, не відображуваних на екрані	полів для організації виносок і посилань (наприклад, використання чорного шрифту на чорному тлі)		

Стеганографічні методи	Коротка характеристика методів	Недоліки	Переваги
1.3. Методи приховання в невикористовуваних місцях гнучких дисків	Інформація записується у звичайно невикористовуваних місцях ГМД (наприклад, у нульовій доріжці)	1. Слабка продуктивність методу, передача невеликих обсягів інформації 2. Низький ступінь скритності	Простота використання. Є опубліковане програмне забезпечення реалізації даного методу
1.4. Методи використання функцій, що імітують (mimic-function)	Метод заснований на генерації текстів і є узагальненням акровірша. Для таємного повідомлення генерується осмислений текст, що приховує саме повідомлення	1. Слабка продуктивність методу, передача невеликих обсягів інформації 2. Низький ступінь скритності	Результуючий текст не є підозрілим для систем моніторингу мережі

Стеганографічні методи	Коротка характеристика методів	Недоліки	Переваги
1.5. Методи видалення ідентифікуючий файл заголовка	Приховуване повідомлення шифрується й у результату віддаляється ідентифікуючий заголовок, залишаючи тільки шифровані дані. Одержувач заздалегідь знає про передачу повідомлення й має відсутній заголовок	Проблема приховання вирішується тільки частково. Необхідно заздалегідь передати частина інформації одержувачеві	Простота реалізації. Багато засобів (White Noise Storm, S-Tools), забезпечують реалізацію цього методу з PGP шифроалгоритмом
2. Методи використання надмірності аудіо й візуальної інформації			
2.1. Методи використання надмірності цифрові фотографії, цифрового звуку й цифрового відео	Молодші розряди цифрових відліків містять дуже мало корисної інформації. Їхнє заповнення додатковою інформацією практично не впливає на якість сприйняття, що й дає можливість приховання конфіденційної інформації	За рахунок введення додаткової інформації спотворюються статистичні характеристики цифрових потоків. Для зниження компрометуючих ознак потрібна	Можливість схованої передачі великого обсягу інформації. Можливість захисту авторського права, схованого зображення товарної марки, реєстраційних номерів і т.п.

		корекція статистичних характеристик	

Як видно з таблиці 1, перший напрямок заснований на використанні спеціальних властивостей комп'ютерних форматів подання даних, а не на надмірності самих даних. Спеціальні властивості форматів вибираються з урахуванням захисту приховуваного повідомлення від безпосереднього прослуховування, перегляду або прочитання. На підставі аналізу матеріалів табл. 1 можна зробити вивід, що основним напрямком комп'ютерної стеганографії є використання надмірності аудіо й візуальної інформації. Цифрові фотографії, цифрова музика, цифрове відео – представляються матрицями чисел, які кодують інтенсивність у дискретні моменти в просторі й/або в часі. Цифрова фотографія – це матриця чисел, що представляють інтенсивність світла в певний момент часу. Цифровий звук – це матриця чисел, що представляє інтенсивність звукового сигналу в послідовно, що йдуть моменти, часу. Всі ці числа не точні, тому що не точні пристрої оцифровки аналогових сигналів, є шуми квантування. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку й візуального образа. Їхнє заповнення відчутне не впливає на якість сприйняття, що й дає можливість для приховання додаткової інформації.

Графічні кольорові файли зі схемою змішання RGB кодують кожну крапку рисунка трьома байтами. Кожна така крапка складається з аддітивних складових: червоного, зеленого, синього. Зміна кожного із трьох найменш значимий біт приводить до зміни менш 1% інтенсивності даної крапки. Це дозволяє приховувати в стандартній графічній картинці обсягом 800 Кбайт близько 100 Кбайт інформації, що не помітно при перегляді зображення.

Розглянемо методи приховання інформації у графічних документах.

Всі алгоритми вбудовування схованої інформації можна розділити на кілька підгруп:

Працюючі із самим цифровим сигналом. Наприклад, метод LSB.

«Упаювання» схованої інформації. У цьому випадку відбувається накладення приховуваного зображення (звуку, іноді тексту) поверх оригіналу. Часто використовується для вбудовування ЦВЗ.

Використання особливостей форматів файлів. Сюди можна віднести запис інформації в метадані або в різні інші не використовувані зарезервовані поля файлу.

По способу вбудовування інформації стегоалгоритми можна розділити на лінійні (аддітивні), нелінійні й інші. Алгоритми аддітивного впровадження інформації полягають у лінійній модифікації вихідного зображення, а її добування в декодері виробляється кореляційними методами. При цьому ЦВЗ звичайно складається із зображенням-контейнером, або «вплавляється» (fusion) у нього. У нелінійних методах вбудовування інформації використовується скалярне або векторне квантування. Серед інших методів певний інтерес представляють методи, що використовують ідеї фрактального кодування зображень. До аддітивным алгоритмів можна віднести:

A17 (Cox).

A18 (Barni).

L18D (Lange).

A21 (J. Kim).

A25 (C. Podilchuk).

Метод LSB

LSB (Least Significant Bit, найменший значущий біт) – суть цього методу полягає в заміні останніх значущих бітів у контейнері (зображення, аудио або відеозапису) на біти приховуваного повідомлення. Різниця між порожнім і заповненим контейнерами повинна бути не відчутна для органів сприйняття людини.

Суть методу полягає в наступному: Допустимо, є 8-бітне зображення в градаціях сірого. 00h (00000000b) позначає чорний колір, FFh (11111111b) – білий. Усього є 256 градацій (28). Також припустимо, що повідомлення складається з 1 байта – наприклад,

01101011b. При використанні 2 молодших біт в описах пікселів, нам буде потрібно 4 пікселя. Допустимо, вони чорного кольору. Тоді пікселі, що містять сховане повідомлення, будуть виглядати в такий спосіб: 00000001 00000010 00000010 00000011. Тоді колір пікселей зміниться: першого – на 1/255, другого й третього – на 2/255 і четвертого – на 3/255. Такі градації, мало того що непомітні для людини, можуть взагалі не відобразитися при використанні низькоякісних пристроїв виводу.

Методи LSB є нестійкими до всіх видів атак і можуть бути використані тільки при відсутності шуму в каналі передачі даних.

Виявлення LSB-кодованого стего здійснюється по аномальних характеристиках розподілу значень діапазону молодших бітів відліків цифрового сигналу.

Всі методи LSB є, як правило, адитивними (A17, L18D).

Інші методи приховання інформації в графічних файлах орієнтовані на формати файлів із втратою, приміром, JPEG. На відміну від LSB вони більше стійкі до геометричних перетворень. Це виходить за рахунок варіювання в широкому діапазоні якості зображення, що приводить до неможливості визначення джерела зображення.

Луна-методи

Луна-методи застосовуються в цифровий аудіостеганографії й використовують нерівномірні проміжки між луна-сигналами для кодування послідовності значень. При накладенні ряду обмежень дотримується умова непомітності для людського сприйняття. Луна характеризується трьома параметрами: початковою амплітудою, ступенем загасання, затримкою. При досягненні якогось порога між сигналом і луною вони змішуються. У цій крапці людське вухо не може вже відрізнити ці два сигнали. Наявність цієї крапки складно визначити, і вона залежить від якості вихідного запису, слухача. Найчастіше використовується затримка близько 1/1000, що цілком прийнятно для більшості записів і слухачів. Для позначення логічного нуля й одиниці використовується дві різних затримки. Вони обидві повинні бути менше, ніж поріг чутливості вуха слухача до одержуваного еха. Луна-методи стійкі до амплітудних і частотних атак, але нестійкі до атак за часом.

Фазове кодування

Фазове кодування (phase coding, фазове кодування) – також застосовується в цифровий аудіостеганографії. Відбувається заміна вихідного звукового елемента на відносну фазу, що і є секретним повідомленням. Фаза елементів, що йдуть підряд, повинна бути додана таким чином, щоб зберегти відносну фазу між вихідними елементами. Фазове кодування є одним з найефективніших методів приховання інформації.

Метод розширеного спектра

Метод вбудовування повідомлення полягає в тім, що спеціальна випадкова послідовність вбудовується в контейнер, потім, використовуючи погоджений фільтр, дана послідовність детектується. Даний метод дозволяє вбудовувати велика кількість повідомлень у контейнер, і вони не будуть створювати перешкоди один одному. Метод запозичений із широкополосного зв'язку.

Опис стегосистеми

Ефект маскування в просторовій області може бути пояснений шляхом побудови стохастичних моделей зображення. При цьому зображення представляється у вигляді марковського випадкового поля, розподіл вірогідності якого підкоряється, наприклад, узагальненому гаусовському закону.

Таким чином, можна запропонувати наступну узагальнену схему впровадження даних в зображення:

1. Виконати фільтрацію зображення за допомогою орієнтованих смугових фільтрів. При цьому отримаємо розподіл енергії по частотно-просторових компонентах.
2. Обчислити поріг маскування на основі знання локальної величини енергії.
3. Масштабувати значення енергії впроваджуваного ЦВЗ в кожному компоненті так, щоб воно було менше порогу маскування.

Багато алгоритмів вбудовування інформації так або інакше використовують цю схему.

Високорівневі властивості СЛЗ поки рідко враховуються при побудові стегоалгоритмів. Їх відмінністю від низькорівневих є те, що ці властивості виявляються «вторинно», обробивши первинну інформацію від СЛЗ, мозок видає команди на її «підстроювання» під зображення. Перерахуємо основні з цих властивостей.

1. Чутливість до контрасту. Висококонтрастні ділянки зображення, перепади яскравості звертають на себе значну увагу.
2. Чутливість до розміру. Великі ділянки зображення «помітніше» менших розміром. Причому існує поріг насичення, коли подальше збільшення розміру не істотне.
3. Чутливість до форми. Довгі і тонкі об'єкти викликають більшу увагу, ніж круглі однорідні.
4. Чутливість до кольору. Деякі кольори (наприклад, червоний) «помітніші» за інші. Цей ефект посилюється, якщо фон заднього плану відрізняється від кольору фігур на ньому.
5. Чутливість до місцеположення. Людина схильна в першу чергу розглядати центр зображення.
6. Люди зазвичай уважніші до зображень переднього плану, ніж заднього.
7. Якщо на зображенні є люди, в першу чергу звертається увага на них. На фотографії людина звертає першочергову увагу на обличчя, очі, рот, руки.
8. Чутливість до зовнішніх подразників. Рух очей спостерігача залежить від конкретної обстановки, від отриманих їм перед переглядом або під час його інструкцій, додаткової інформації.

В якості даних, що вбудовуються може використовуватися будь-яка інформація: текст, повідомлення, зображення тощо. При вбудовуванні ЦВЗ, такими даними буде логотип банку. Роль контейнеру буде відігравати банківський документ, який необхідно захистити від спотворень та модифікацій зловмисниками.

Стегоключ або просто ключ – секретний ключ, необхідний для приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування заздалегідь зашифрованого повідомлення) в стегосистемі може бути один або декілька стегоключів.

Цифрові водяні знаки бувають трьох видів: робасті чи стійкі (мається на увазі, що такі ЦВЗ стійкі до різного роду дій над зображенням-контейнером), крихкі (змінюються або руйнуються при незначній модифікації контейнера) і напівкрихкі (стійкі по відношенню до одних дій і нестійкі по відношенню до інших). Стійкі ЦВЗ використовуються, коли автор хоче, щоб ідентифікаційний код, логотип компанії і т.п. збереглися при максимальних спотвореннях контейнера. Крихкі ЦВЗ, разом з ЕЦП, застосовуються для перевірки цілісності електронних документів. Алгоритми вбудовування крихких ЦВЗ відрізняються від інших особливою чутливістю до будь-яких спотворень і ефективні при рішенні задачі контролю цілісності і захисту від фальсифікації. У разі напівкрихких ЦВЗ зображення, наприклад, може бути переведене в інший формат або стиснене, при цьому не можна вирізувати або вставити в нього фрагмент; для аудіотрека можна змінити звучання частот, але не можна прибрати голос виконавця. Щоб технологія ЦВЗ забезпечувала захист, водяні знаки повинні відповідати наступним вимогам:

індивідуальність алгоритму нанесення ЦВЗ;

невидимість мітки для користувачів;

можливість виявлення несанкціонованого використання файлу, поміченого ЦВЗ;

неможливість витягання ЦВЗ третіми особами;

стійкість до змін носія/контейнера.

Виявлення ЦВЗ в захищеному зображенні відбувається за допомогою стегодетектора. Після вилучення цифровий водяний знак порівнюється з шаблоном. Відсутність чи спотворення ЦВЗ можуть бути обумовлені впливом помилок в каналі зв'язку, чи навмисних атак порушників.

В результаті виконання даного магістерської роботи було розроблено програмне забезпечення стеганографічного захисту інформаційних ресурсів. Дана система повинна

захищати від несанкціонованого доступу конфіденційну інформацію, що передається по Інтернету та локальних мережах.

Структурна схема розробленого програмного забезпечення представлена на рисунку 1.

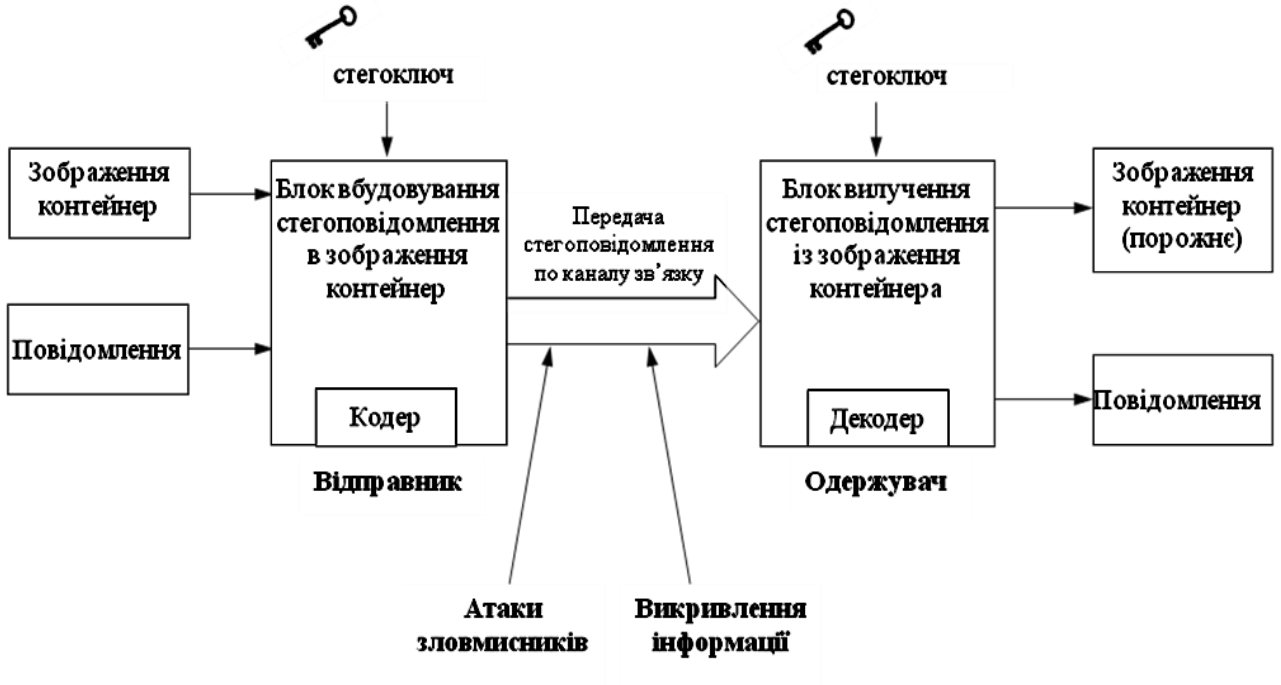


Рисунок 1 – Структурна схема системи

В якості даних, що вбудовуються може використовуватися будь-яка інформація: текст, повідомлення, невелике зображення тощо.

Роль контейнеру буде відігравати будь-яке кольорове цифрове зображення, що задовольняє стандартним вимогам до контейнерів для стегоповідомлень.

Стегоключ – секретний ключ, необхідний для приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування заздалегідь зашифрованого повідомлення) в стегосистемі може бути один або декілька стегоключів.

Вбудовування повідомлення в зображення контейнер відбувається за допомогою стегокодера, який крім приховування інформації здійснює також і перешкодостійке кодування.

Після цього зображення з прихованим повідомленням передається по каналу зв'язку, де може зазнавати атак зловмисників, а також викривлень інформації в наслідок перешкод у каналі зв'язку або застосувань алгоритмів стиснення з втратами.

Вилучення повідомлення із зображення контейнера здійснюється за допомогою стегодетектора. Стегодекодер перевіряє наявність прихованого повідомлення і в разі його існування, вилучає інформацію.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів стеганографічного захисту інформаційних ресурсів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем стеганографічного захисту інформаційних ресурсів. Досліджена система стеганографічного захисту інформаційних ресурсів. На основі отриманих результатів досліджень створена програмна реалізація системи стеганографічного захисту інформаційних ресурсів. Розроблені алгоритми дозволяють успішно вирішувати завдання стеганографічного захисту інформаційних ресурсів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Разработка метода и алгоритмов синтеза больших ансамблей недвоичных дискретных сигналов на основе обобщенных перестановочных преобразований / А.А. Кузнецов, Ал.М. Носик, А.А. Смирнов, Л.Н. Качур, Ан.М. Носик // Збірник наукових праць «Системи обробки інформації». – Випуск 5(72). – Х.: ХУПС – 2008. – С. 151-156.
2. Смирнов А.А. Формирование дискретных сигналов с многоуровневой функцией корреляции / А.А. Кузнецов, А.А. Смирнов, В.Н. Сай // Збірник наукових праць «Системи обробки інформації». – Випуск 5 (95). – Х.: ХУПС. – 2011. – С. 50-60.
3. Смирнов А.А. Дискретные сигналы с многоуровневой функцией корреляции / А.А. Кузнецов, А.А. Смирнов, В.Н. Сай // Радиотехника: Всеукраинский межведомственный научно-технический сборник. Тематический выпуск «Информационная безопасность» – Выпуск 166. – Х.: ХНУРЭ. – 2011. – С. 142-152.
4. Смирнов А.А. Математическая модель и структурная схема стеганографической системы / А.А. Кузнецов, А.А. Смирнов, е.в. мелешко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. Випуск 25. Частина 1. – Кіровоград: КНТУ. – 2012. – С. 273-281.
5. Смірнов О.А. Стеганографічне приховування інформації із використанням прямого розширення спектру / О.о. кузнецов, О.а. смірнов // Збірник тез доповідей науково-практичної конференції «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку». м. Харків. 21-22 березня 2012 р. – Харків. АВВ МВС. – 2012. – С. 49-52.
6. Смирнов А.А. Математическая модель и структурная схема стеганографической системы / А.А. Кузнецов, А.А. Смирнов, Е.В. Мелешко // Збірник тез XIII міжнародного науково-практичного семінару «Комбінаторні конфігурації та їх застосування». м. Кіровоград. 13-14 квітня 2012 р. – Кіровоград: КНТУ. – 2012. – С. 91-92.
7. Смирнов А.А. Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов / А.А. Кузнецов, А.А. Смирнов // Радиотехника: Всеукраинский межведомственный научно-технический сборник. Тематический выпуск «Информационная безопасность» – Выпуск 166. – Х.: ХНУРЭ. – 2011. – С. 134-141.
8. Смірнов О.А. Дослідження ймовірнісних властивостей стеганографічного захисту інформації із використанням прямого розширення спектру / О.о. кузнецов, О.а. смірнов, л.т. пархуць, ю.м. рябуха // Системи управління, навігації та зв'язку. – Випуск 1 (21) том 1. – К.: ДП «ЦНДІНУ». – 2012. – С. 115-121.
9. Смирнов А.А. Встраивание данных в контейнеры-изображения с использованием сложных дискретных сигналов / А.А. Кузнєцов, А.А. Смирнов // Збірник тез XI міжнародної науково-технічної конференції «Проблеми інформатики и моделювання». м. Харків. 25 листопада 2011 р. – Харків: НАНУ, НТУ «ХПІ», РВНЗ «КГУ». – 2011. – С.42.
10. Smirnov O.A. Use of Complex Discrete Signals for Steganographic Information Security / A.A. Kuznetsov, A.A. Smirnov // International Journal of Engineering Practical Education. – Volume 1, Issue 1. – USA, Indiana, Riley: Science and Engineering Publishing Company. – 2012. – P. 21-25.

УДК 004

С. Сільченко, магістр гр. КІ-20МЗ,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ СУПУТНИКОВИМ HD РЕСИВЕРОМ НА БАЗІ ПРОЦЕСОРУ GX6605S

У статті розроблено програмне забезпечення, яке призначено для системи керування супутниковим HD ресивером на базі процесору GX6605S. Метою розробки є дослідження та програмна реалізація системи керування супутниковим HD ресивером на базі процесору GX6605S. Об'єктом дослідження є процес керування супутниковим HD ресивером на базі процесору GX6605S. Предметом дослідження є методи керування супутниковим HD ресивером на базі процесору GX6605S. Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи керування супутниковим HD ресивером на базі процесору GX6605S. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, HD ресивер, GX6605S

Постановка проблеми. Передача даних через супутники – область техніки зв'язку, що займається питаннями передачі Інтернету, телефонного зв'язку та телевізійних програм від передавальних земних станцій до приймачів із використанням штучних супутників землі (ШСЗ) як активних ретрансляторів [1-5]. Супутникове віщання є сьогодні самим економічним, швидким і надійним способом передачі ТБ сигналу високої якості в будь-яку точку великої території. До переваг СТБ відносяться також можливість використання сигналу необмеженим числом прийомних установок, висока надійність ШСЗ, невеликі витрати і їхня незалежність від відстані між джерелом і споживачем [4].

Важливою проблемою в прийомних установках СТБ є можливість автоматичного керування ними. Вирішити цю проблему можна за допомогою мікропроцесорних пристроїв.

Використання мікроелектронних засобів у виробах виробничого й культурно-побутового призначення не тільки приводить до підвищення техніко-економічних показників виробів (вартості, надійності, споживаній потужності, габаритних розмірів) і дозволяє багаторазово скоротити строки розробки, відсунути строки "морального старіння" виробів, але й надає їм принципово нові споживчі якості (розширені функціональні можливості) [3-8].

Використання мікропроцесорів у системах керування забезпечує досягнення високих показників ефективності при низькій вартості, таким чином, немає розумної альтернативної елементарної бази для побудови керуючих і/або регулюючих систем, як використання мікропроцесорів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування супутниковим HD ресивером на базі процесору GX6605S

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи керування супутниковим HD ресивером на базі процесору GX6605S.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем керування супутниковим HD ресивером на базі процесору GX6605S.

– Дослідження системи керування супутниковим HD ресивером на базі процесору GX6605S.

– Програмна реалізація системи керування супутниковим HD ресивером на базі процесору GX6605S.

Об'єктом дослідження є процес керування супутниковим HD ресивером на базі процесору GX6605S.

Предметом дослідження є методи керування супутниковим HD ресивером на базі процесору GX6605S.

Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Проектування пристрою вводу/виводу

МП GX6605S є поліпшеною модифікацією попередніх МП та спеціально розроблена в ньому система введення/виведення інформації забезпечує необхідну функціональність. От чому свій вибір і зупинив саме на цій мікросхемі.

GX6605S забезпечує введення/виведення інформації паралельної інформації, застосовується як елемент загального призначення, що сполучає різні типи периферійних пристроїв з магістраллю даних систем обробки інформації.

Обмін інформацією між магістраллю даних систем і мікросхемою здійснюється через 8 розрядний двонаправлений трьохстабільний канал даних. Для зв'язку з периферійними пристроями використовується 24 лінії В/В, згруповані в три 8 розрядних канали ВА, ВВ, ВС, напрямок передачі інформації й режими роботи яких визначаються програмним способом.

Мікросхема може функціонувати в 3-х основних режимах.

У режимі 0 забезпечується можливість синхронної програмно керованої передачі даних через 2 незалежних 8 розрядних канали ВА, ВВ і два 4 розрядних канали ВС.

У режимі 1 забезпечується можливість вводу або виводу інформації в/або з периферійного пристрою через 2 незалежних 8 розрядних канали ВА, ВВ по сигналах квітирування. При цьому лінії каналу С використовуються для прийому й видачі сигналів керування обміном.

У режимі 2 забезпечується можливість обміну інформацією з периферійними пристроями через двохнаправлену 8 розрядну шину ВА по сигналах квітирування. Для передачі й прийому сигналів керування обміном використовуються 5 ліній каналу ВС.

Вибір відповідного каналу й напрямок передачі інформації через канал визначається сигналами А0, А1 і сигналами $\overline{RD}$, $\overline{WR}$, $\overline{CS}$. Режим роботи кожного з каналів ВА, ВВ, ВС визначається вмістом регістра керуючого слова (РКС). Роблячи запис керуючого слова в РКС можна перевести мікросхему в один з 3-х режимів роботи: режим 0-простий В/В; режим 1-стробуємий В/В; режим 2-двонаправлений канал. При подачі сигналу SR РКС установлюється в стан, при якому всі канали настроюються на роботу в режимі 0 для вводу інформації. Режим роботи каналів можна змінити як на початку, так і в процесі виконання працюючої програми, що дозволяє обслуговувати різні периферійні пристрої в певному порядку однією мікросхемою. При зміні режиму роботи будь-якого каналу всі вхідні й вихідні регістри каналів і тригери стану скидаються.

У нашому випадку необхідно запрограмувати мікросхему на вивід інформації у режимі 0. Саме тому далі буде розглянутий тільки цей режим.

При роботі мікросхеми у режимі 0 забезпечується простий В/В інформації через кожний з 3-х каналів і сигналів керування обміном інформацією з периферійними пристроями не потрібно.

У цьому режимі мікросхема являє собою сукупність 2-х 8 розрядних і 2-х 4 розрядних каналів введення або виведення. У режимі 0 можливі 16 різних комбінацій схем введення/виведення каналів ВА, ВВ, ВС. Це визначається комбінаціями в розрядах D4; D3; D1; D0 регістра керуючого слова.

Для нашого випадку код повинен мати наступну вказівку

D4	D3	D1	D0	BA;BB;BC
0	0	0	0	Виведення

У режимі 0 вхідна інформація не запам'ятовується, а вихідна зберігається у вихідних регістрах до запису нової інформації в канал або до запису нового режиму.

Для електричного з'єднання мікросхеми і схеми керування необхідно:

1) шину даних D0÷ D7 схеми керування з'єднати з виводами D0÷ D7 мікросхеми 580ВВ55.

2) Два молодших розряди адресної шини з'єднати з виводами A0÷ A1 мікросхеми.

3) Виводи $\overline{RD}$, $\overline{WR}$ мікропроцесора GX6605S з'єднати з виводами $\overline{RD}$, $\overline{WR}$ мікросхеми відповідно.

4) На вхід SR "Установка у вихідний стан" мікросхеми подати низький рівень (підключити до корпуса).МП GX6605S має вбудовану статичну оперативну пам'ять (SRAM) розміром 16...64 Кбайт, що може використатися для зберігання коду й/або даних. SRAM може зберігати 8, 16 і 32-бітні дані.

Вміст SRAM при скиданні МП зберігається. Контролер SRAM має у своєму складі буфер відкладеного запису, необхідний для забезпечення роботи центрального процесора без його зупинки на час запису в SRAM. У буфері відкладеного запису завжди втримуються останні дані, передані програмою для запису в SRAM.

Уміст буфера записується у SRAM, коли програма передає у буфер наступну порцію даних, призначених для приміщення у SRAM. Якщо в деякий момент часу відбувається скидання мікроконтролера, то остання поміщена в буфер відкладеного запису порція даних буде загублена. Щоб уникнути цього, а також перед перекладом мікроконтролера у режим зниженого споживання розроблене програмне забезпечення періодично робить фіктивну операцію запису. Це дає гарантію того, що останні записані дані будуть перебувати в SRAM і після скидання.

Проектування фіксуючої схеми

В блок індикації необхідно подавати сигнали № каналу (2 індикатори) у строго певні моменти часу.Для цього необхідно передбачити пристрій, що по сигналах від процесора, буде пропускати інформацію на один з індикаторів блоку індикації. Як елементи фіксуючої схеми будемо використовувати 2 регістри.

	EO	C	D_n	Вихід
Завантаження й зчитування	H	↗	"H", "B"	"H", "B"
Завантаження регістра й розрив виходів	B	↗	"H", "B"	відповідно

Рисунок 1 – Регістр приймає й відображає інформацію синхронно з позитивним перепадом на тактовому вході

Таким чином, подаючи тактуючі сигнали на вхід C (№11) регістра 1533UP23, ми дозволяємо проходження сигналів на відповідний індикатор у строго певні моменти часу.

Проектування схеми, що погоджує

Для організації виводу інформації в інші блоки тюнера будемо використовувати регістр тактуємий сигналами від мікропроцесора.

Для прийому інформації до пристрою керування будемо використовувати шинний формувач. Як відомо шинний формувач забезпечує передачу інформації в обох напрямках.

Для забезпечення тільки вводу даних вивід №1 з'єднаємо з корпусом. Якщо з'явиться необхідність у виводі більшої кількості інформації із пристрою керування, то за допомогою мікросхеми SN74ALS245 можна буде вирішити дану проблему.

Проектування схеми дешифрації

Раніше були розглянуті основні блоки схеми керування й було відзначено, що МП у строго певні моменти часу повинен взаємодіяти з певними мікросхемами. Тому в даній схемі необхідно передбачити пристрій, що по сигналах від процесора, буде підключати до його шин адреси або даних ту або іншу мікросхему або групу мікросхем. Із цього можна укласти,

що в схемі системи повинен протікати деякий процес однозначного вибору й він організується подачею на лінії адреси A11 ÷ A15 певного коду вибору або сигналу дозволу доступу до окремого блоку або блоків. На щастя, ця проблема є класичною й вона має просте рішення. Зокрема можна використовувати дешифратор, виконаний у вигляді ТТЛ пристрою середнього рівня інтеграції, призначеного для перетворення двійкового коду в напругу логічного рівня, що з'являється в тім вихідному проведенні, десятковий номер якого відповідає двійковому коду. У наслідку вихідне проведення дешифратора підключають до входу “Вибір мікросхеми” потрібної мікросхеми (наприклад вивід №18 (CS) мікросхеми HM6516-9).

Як дешифратор будемо використовувати мікросхему SN74ALS138. Вибір даного дешифратора обумовлений кількістю вихідних ліній і навантажувальною здатністю.

Мікросхема SN74ALS138 – високошвидкісний дешифратор, що перетворить трьохразрядний код A0 ÷ A2 (№1 ÷ 3) у напругу низького логічного рівня, що з'являється на одному з восьми виходів 0 ÷ 7. Дешифратор має трьохвходовий логічний елемент дозволу.

Як інформаційні сигнали будемо використовувати сигнали, що надходять по адресних лініях A11 ÷ A13; сигнали дозволу, сигнали, що надходять по адресних лініях A14 ÷ A15 (вхід №4 приєднаємо до корпуса).

Проектування цифро-аналогового перетворювача

Для перетворення цифрової інформації в аналогову необхідно використовувати ЦАП. Основною характеристикою ЦАП є розв'язна здатність, обумовлена числом розрядів N. Теоретично ЦАП, що перетворить N-розрядні двійкові коди, повинен забезпечувати 2^N різних значень вихідного сигналу з розв'язною здатністю $(2\ N\text{-}1)^{-1}$.

З динамічних параметрів основними є: час установки вихідного сигналу; f_{max} перетворення.

У нашому випадку необхідно організувати формування 3-х аналогових сигналів ANL1, ANL2 і ANL3, які будуть пропорційні цифровим сигналам на виходах каналу A, B, C мікросхеми 82C55 відповідно. Значить необхідно передбачити 3 цифро-аналогових перетворювачі. Свій вибір я зупинив на 10 розрядному ЦАП прецизійного типу AD7520. Для побудови повної схеми перетворювача до мікросхеми AD7520 необхідно підключити операційний підсилювач. Як операційний підсилювач будемо використовувати MC1556G, що має схему внутрішньої корекції.

Час реакції на переривання в мікропроцесорній системі критично, як правило, тільки для швидких переривань FI. Значення часу реакції лежить у деякому можливому діапазоні, тобто може бути максимальним і мінімальним. Коли переривання FI дозволені, максимальний час реакції на FI (для самого "поганого" випадку) складається з:

– $T_{syncmax}$ найбільш тривалий час запиту, що може знадобитися на реакцію синхронізатора. Цей час становить два процесорних цикли;

– T_{ldm} час, що вимагається для завершення самої довгої команди. (Сама довга команда – LDM, що завантажує всі регістри, включаючи PC.);

– T_{ldm} дорівнює 20 процесорним циклам у системі з нульовим часом очікування;

– T_{exc} час входу в оброблювач Data Abort. Воно становить три процесорних цикли;

– T_{fiq} час входу в оброблювач FI. Воно становить два процесорних цикли.

Таким чином, повний час очікування для самого "поганого" випадку становить 27 циклів процесора, що небагато менше 0.7 мкс у системі з тактовою частотою процесора 40 Мгц. При обчисленні максимального часу очікування IRQ необхідно враховувати ту обставину, що обробка переривань FI, що мають пріоритет вище, ніж в IRQ, може затримати вхід в оброблювач IRQ.

Мінімальний час очікування для FI або IRQ – це найкоротший час запиту, що може знадобитися на реакцію синхронізатора $T_{syncmin}$, складене згодом T_{fiq}, що в сумі становить чотири процесорних цикли.

Додаткові пояснення до схеми керування

1) Щоб уникнути запису або зчитування "помилкової" інформації під час включення або вимикання напруги живлення в схемі пристрою керування передбачена мікросхема DD8 – чотирьох канальний комутатор цифрових і аналогових сигналів. Кожний ключ має свій вхід і вихід сигналу, а також вхід дозволу проходження сигналу EI. Канал провідності двох направлений. Комутатор CD4066B має опір каналу 80 Ом, опір входу керування 10^{12}Ом. Відкриваюча напруга на вході EI – 3У. Канал пропустить цифрові рівні з амплітудою до $U_{ип}$. Час затримки поширення сигналу 10...25 мс.

2) У схемі керування використовується мікросхема DD6: логічний елемент АБО із двома виходами. Ці функції реалізуються за допомогою мікросхеми SN74ALS32. Також використовується мікросхема DD9: логічний елемент АБО-НІ з одним входом (інвертор). Ці функції реалізуються за допомогою мікросхеми SN54ALS04.

3) При вхідному імпульсному сигналі з пологими фронтом і зрізом імпульс на вході формуючого логічного елемента також не буде прямокутним, оскільки якийсь час ключова схема буде перебувати в підсилювальному режимі. Крім того, на фронті й зрізі вихідного імпульсу будуть присутні посилені перешкоди, що надійшли в "підсилювач" із проведення живлення. Імпульс із зашумленими й несформованими фронтом і зрізом непридатний для перемикання тактових входів тригерів, регістрів і лічильників.

Підвищення $К_U$ формувача до 10^3 разів і більше за рахунок послідовного включення декількох буферних елементів не дає точної прив'язки моменту перемикання до певного граничного вхідного імпульсу.

У таких випадках використовують так звану схему тригера Шмідта, що складається із двокаскадного підсилювача, охопленого слабким позитивним зворотним зв'язком. Тригери Шмідта виявилися незамінними й в інтегральної схемотехніці, як в аналоговій, так і цифровій. Передатна характеристика тригера Шмідта має значний гістерезис.

Вихідний сигнал логічного елемента Шмідта має круті імпульсні перепади, тривалість яких не залежить від швидкості наростання або спаду вхідного сигналу. Імпульсні перепади за часом відповідають моментам, коли вхідний сигнал перевищує напруга спрацьовування $U_{спр}$ і стає менше, ніж напруга відпускання $U_{відп}$. У даній схемі пристрою керування тригер Шмідта – у вигляді мікросхеми SN74ALS14 (DD2).

4) Перш ніж послідовність коротких імпульсів подавати на вхід SID мікропроцесора, необхідно забезпечити гарну стабільність тривалості даних імпульсів, тому що на вході елемента Шмідта всі вони будуть мати різну тривалість.

У складі серій ТТЛ є кілька аналого-імпульсних схем – мультивібраторів, що чекають.

Вони дозволяють розширити тривалість коротких імпульсів, сформувати імпульси потрібної тривалості з гарною стабільністю по тривалості. Свій вибір я зупинив на мікросхемі SN74ALS123 – два чекаючи мультивібратори з можливістю перезавантаження. Кожний мультивібратор має виходи Q і $\overline{Q}$, вхід скидання, 2 входи дозволу запуску: В-Прямій, $\overline{A}$-інверсний.

Тривалість вихідного імпульсу визначається часозадаючими елементами Сτ и Rτ ; $\tau_{вих}$=0,45 Rτ С.τ .

Таким чином розглянувши апаратну частину системи керування супутниковим HD ресивером на базі процесору GX6605S перейдемо до її програмного забезпечення.

Розробка структурної схеми

Відповідно до поставленого завдання магістерської роботи – розробка програмного забезпечення системи керування супутниковим HD ресивером на базі процесору GX6605S, була розроблена програма, яка дозволяє виконувати поставлені завдання. Перед розглядом структурної схеми системи, розглянемо роботу супутникового ТБ і розпишемо виниклу проблематику.

Як показано на рисунку 2, супутники щодо поверхні землі розташовані під різними кутами геостаціонарної орбіти. Для роботи з ними використовується чотири дорогих конверторних головки зі спеціальним перехідником під комп'ютерну плату (рисунок 3).

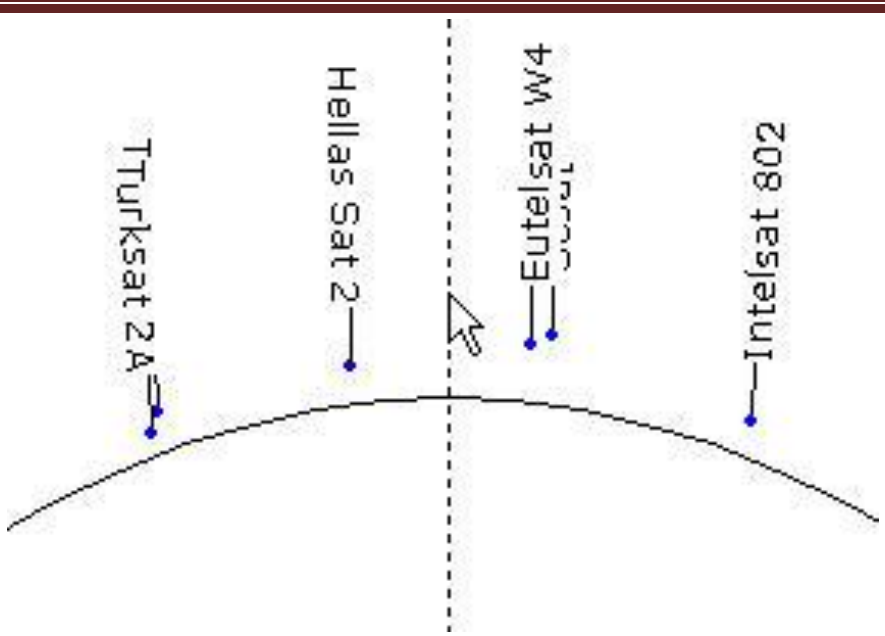


Рисунок 2 – Розташування супутників відносно поверхні Землі

Рисунок 3 – Підключення чотирьох дорогих конверторні головки із дзеркалом на різні супутники

Головки направляються під різними кутами до супутників подаючи сигнал, але дана система дорога та має ряд обмежень.

Для подолання проблеми використання великої кількості головок використовують мотоприводи які направляють одну головку на необхідний супутник як показано на рисунку 4.

Управляють положенням супутникової тарілки (далі дзеркалом) за допомогою спеціального перемикача (рисунок 3.5), що взаємодіє із ПК через протокол DiSEq 1.2.

DiSEq (Digital Satellite Equipment Control) – спеціальний протокол зв'язку для обміну даними між супутниковим ресивером і іншими пристроями – такими, як: перемикачі, поляризатори, позиціонери й т.п. Для передачі сигналу використовується коаксіальний кабель. Режим обміну даними через кабель – двосторонній, з можливістю подачі живлення.

Стандартом передбачена сумісність із традиційним перемиканням напруги 13/17 вольт і тоном 22 кГц.

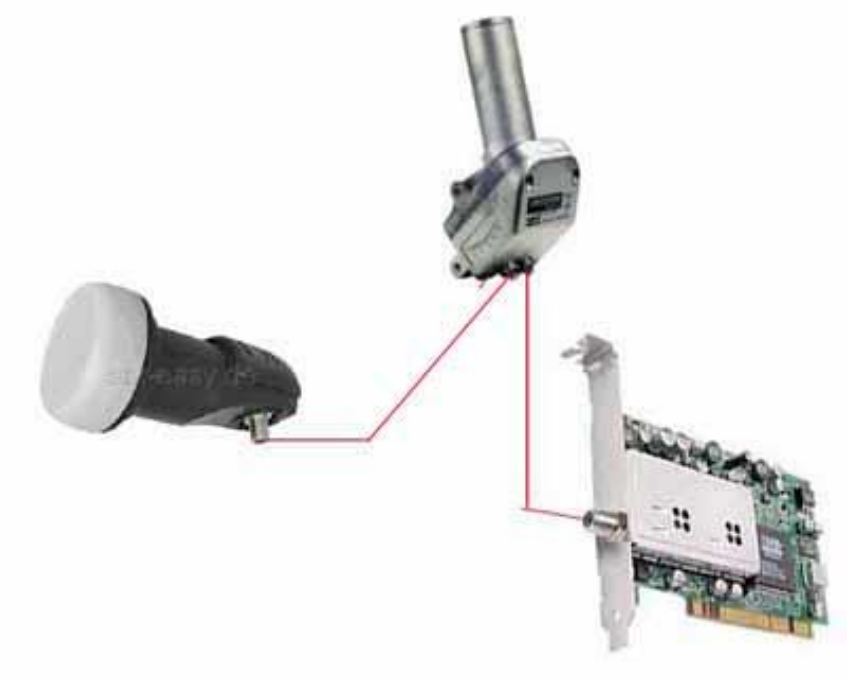


Рисунок 4 – Підключення однієї конверторних головки із дзеркалом і мотоприводом на різні супутники

Протокол DiSEq використовується для керування різною периферією в прийомних системах супутникового ТБ. Команди DiSEq передаються по лінії постійного живлячої напруги 12-20В за допомогою тонових посилок частотою 22кГц (±20%) і номінальною амплітудою 650мВ (±250мВ) при напрузі живлення 13/18В.

DiSEq використовує для передачі широтно-імпульсну маніпуляцію, при якій від ширини огібаючих імпульсів залежить переданий біт. Час передачі одного біта становить 1.5мс і умовно розділено на 3 рівні частини по 500мкс (±100мкс).

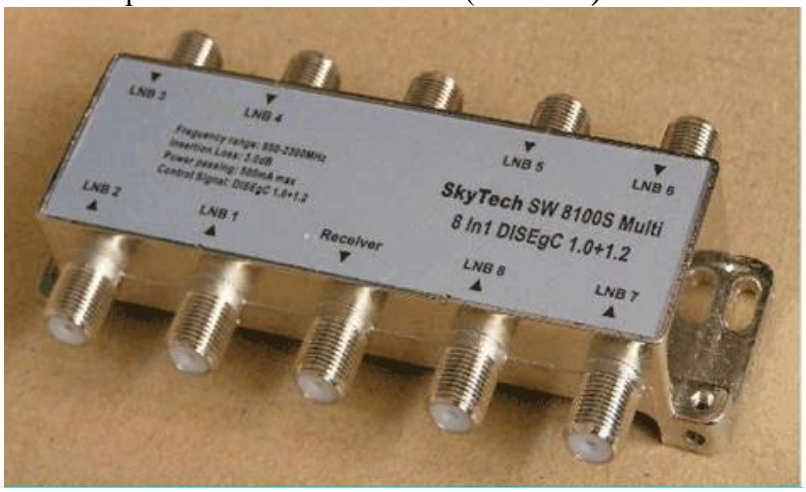


Рисунок 5 – Зовнішній вигляд перемикача SkyTech SW8100S, 8LNB

Для біта 0 ширина що обгинає становить 1.0 мс, що відповідає 22 імпульсам, а для біта 1 ширина що обгинає становить 0.5мс, а це 11 імпульсів.

Але в системи з однією конверторною головкою, дзеркалом і мотоприводом є істотний недолік – відсутність універсального програмного забезпечення, яке має можливість автоматично шукати сигнал і набудовувати позиції.

У зв'язку із цим розроблене магістерське програмне забезпечення розроблено з розумінням даного факту, й взаємодіє із протоколом DiSEq 1.2.

При розробці програми використовувався наступний набір устаткування.

1. Супутникова тарілка (дзеркало) – без назви харківського виробництва.
2. Конверторна головка – LNB.
3. Мотопривод – Strong 21100.
4. Тюнер (ресивер) – StarTrack 750CU.
5. Комп'ютерна плата керування мотоприводом – TT-PCline Budget 1401 (SkyStar 3) рисунок 3.6.
6. Перемикач DiSEq – SkyTech SW8100S, 8LNB.
7. Кабелі й кронштейни – без назви харківського виробництва.

Рисунок 6 – Використовувана плата TT-PCline Budget 1401 (SkyStar 3)

Розглянемо структурну схему системи зображену на рисунку 3.7, на якій розглянута робота й взаємодія всієї системи в цілому.

Розроблена програма на персональному комп'ютері робить моніторинг роботи системи за допомогою комп'ютерної плати керування. Дзеркало може бути орієнтоване на 16 різних позицій – геостаціонарної орбіти супутників, згідно протоколу DiSEq 1.2.

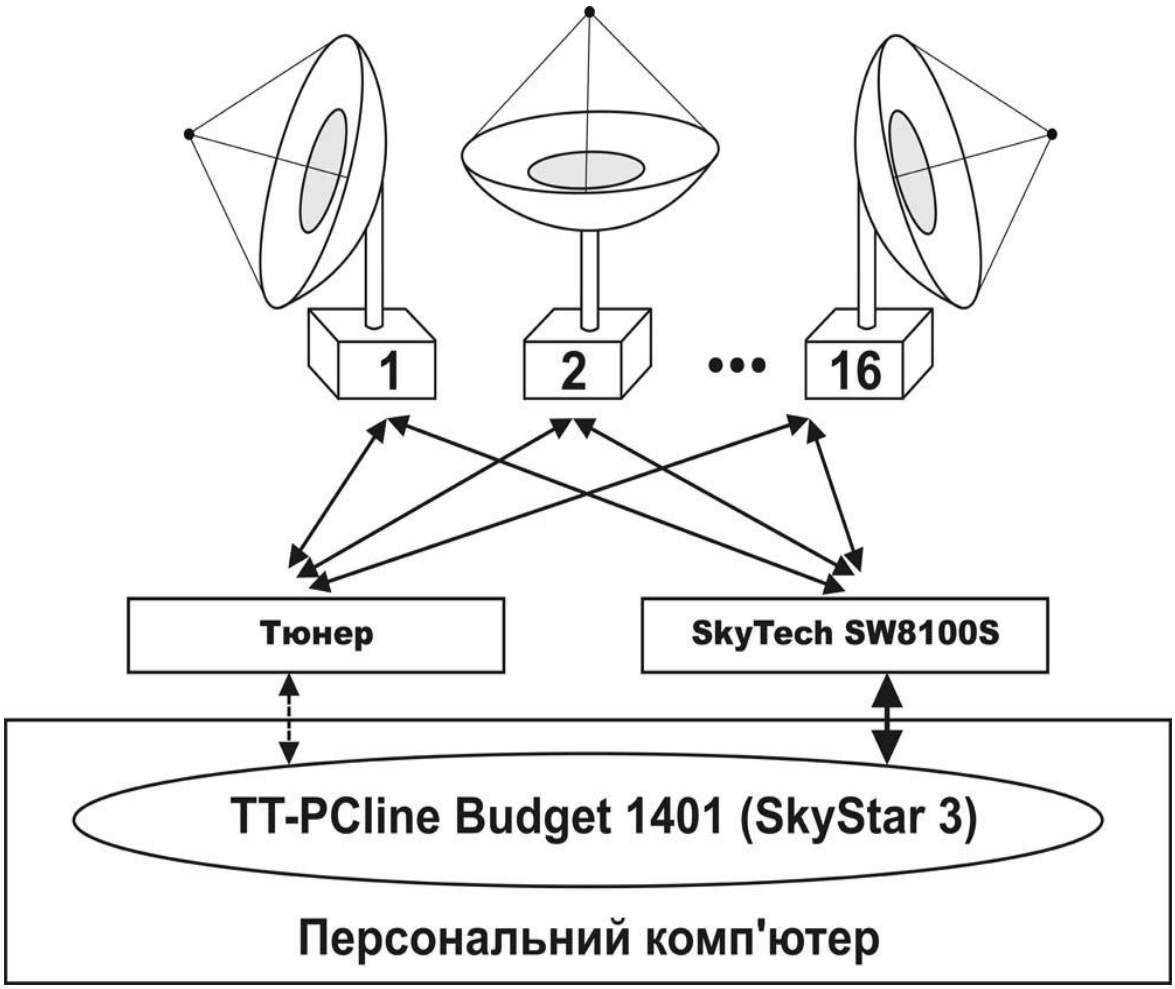


Рисунок 7 – Структурна схема системи

У свою чергу супутниковий тюнер управляє й відображає отриману картинку залежно від бажання користувача на ПК або на звичайний телевізор. Комп'ютерна плата керування теж може відігравати роль тюнера але через погане відображення картинки був обраний варіант із зовнішнім тюнером, що дає додаткову перевагу переклад сигналу або його дублювання з монітора комп'ютера на телевізор.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування супутниковим HD ресивером на базі процесору GX6605S. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем керування супутниковим HD ресивером на базі процесору GX6605S. Досліджена система керування супутниковим HD ресивером на базі процесору GX6605S. На основі отриманих результатів досліджень створена програмна реалізація системи керування супутниковим HD ресивером на базі процесору GX6605S. Розроблені алгоритми дозволяють успішно вирішувати завдання керування супутниковим HD ресивером на базі процесору GX6605S. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
2. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних

Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
3. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
4. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
5. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
6. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
7. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.
8. Коваленко А.С. Експертна система технічного діагностування інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2015. – № 1(41). – С. 106-111.
9. Коваленко А.С. Удосконалення методу технічного обслуговування об’єктів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко, О.П. Доренський // Системи озброєння і військова техніка. – Х.: ХУПС, 2016. – № 2(46). – С. 109-114.
10. Коваленко А.С. Метод визначення оптимального комплексу робіт з відновлення працездатності інтегрованої системи технічної діагностики в умовах ресурсних обмежень / А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2016. – Вип. 3(140). – С. 85-72.

УДК 004

В. Сергатий, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІДЕОНАГЛЯДУ РЕАЛІЗОВАНОЇ НА БАЗІ AXIS P1364-E ТА AXIS P1365-E MK II

У статті розроблено програмне забезпечення, яке призначено для системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Метою розробки є дослідження та програмна реалізація системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Об’єктом дослідження є процес відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Предметом дослідження є методи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Методи дослідження базуються на методах теорії обробки мультимедійних даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, відео нагляд, Axis P1364-E, Axis P1365-E Mk II

Постановка проблеми. Камери Axis лінійки P13 у вуличному виконанні розраховані на роботу в діапазоні температур від -40 до +50 0 С і широко застосовуються. Усього дана лінійка включає 9 моделей камер. Недавно компанія заявила про значне розширення асортиментів камер, що збираються в Україні – до 16 моделей, що випускаються раніше, додалося ще 10, причому дві з них з лінійки камер P13 (Axis P 1364-E й Axis P 1365-E Mk II).

Всі використовувані технічні засоби для її забезпечення, у тому числі камери відеоспостереження, підлягають обов'язковій сертифікації. Сертифікації підлягають як впроваджувані засоби, так і вже встановлені.

До камер відеоспостереження пред'являється цілий ряд функціональних і технічних вимог у частині розв'язної здатності, оптичних характеристик, ступеня стиску зображення, частоти кадрів і т.д. Більшість сучасних камер для цього ринку легко їм задовольняють, зокрема, мінімальний припустима розв'язна здатність становить 1,2 Мпікселів. Дотримання даних характеристик повинне підвищити безпеку, про при цьому захищеність самих камер відеоспостереження ніяк не регламентується. Якщо відносно систем контролю доступу говориться, що вони повинні забезпечувати захист «технічних і програмних засобів від несанкціонованого доступу . у вигляді системи паролів», то до відеокамер не пред'являється навіть цих елементарних вимог.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II.

– Дослідження системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II.

– Програмна реалізація системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II.

Об'єктом дослідження є процес відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II.

Предметом дослідження є методи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II.

Методи дослідження базуються на методах теорії обробки мультимедійних даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис AXIS P 1364-E

AXIS P 1364-E RU(0739-014) – вулична HDTV 720p камера IP-відеоспостереження, призначена для роботи при дуже слабкому освітленні, що підтримує фірмові технології Axis: Lightfinder, WDR – Forensic Capture, P-iris, Zipstream і оснащена системою віддаленого фокусування. Камера P 1364-E RU(0739-014) дозволяє одержати відеозображення з розв'язною здатністю HDTV 720p при частоті кадрів 50/60 кадр/с, забезпечуючи при цьому придушення шуму й зниження размиття об'єктів, що рухаються, при недостатнім освітленні. Технологія Axis Zipstream значно знижує обсяг переданого трафіку й вимоги до обсягу пам'яті для зберігання даних. Підтримка камерою широкого динамічного діапазону WDR – Forensic Capture дозволяє одержати відеозображення, що оптимально для розпізнавання об'єктів завдяки винятковому пророблению деталей – навіть у самих несприятливих умовах освітленості. Можливість віддаленого регулювання заднього фокуса підвищує ефективність установки камери й забезпечує чіткість зображення. Модель P 1364-E RU(0739-014) відповідає стандартам IP66, IP67, NEMA 4X і IK10. У комплект поставки камери входить кронштейн для кріплення на стіну й сонцезахистний козирок. Технологія Arctic Temperature Control гарантує запуск і роботу камери при температурах від -40 до 50°C.

Характеристики:

– Максимальна розв'язна здатність, пікс. – 1280x960.
– Виконання камери – Циліндрична.
– Об'єктив – Варіофокальний.

– Вулична – Так.
– Поворотна – Немає.
– Функції – Підтримка аудіо/Живлення по PoE/Вулична.
– Живлення по PoE – Так.
– Підтримка звуку – Так.
– Кількість пікселів, Мпікс. – 1.2.
– Фокусна відстань, мм. – 2.8 – 8.5.
– Робоча температура, °C – – 40 – 50.
– Виробник – Axis.
– Посилання на виробника – https://www.axis.com/ru – ru/products/axis – p1364 -e.
– Альтернативна структура – 106/126.

Особливості P 1364-E RU(0739-014):

– Технології Lightfinder і WDR – Forensic Capture.
– HDTV 720p із частотою 50/60 кадр/с.
– Технологія Axis Zipstream.
– Двостороння передача звуку.
– Технологія Arctic Temperature Control.

Технічні характеристики AXIS P 1364-E RU(0739-014):

– Зображення КМОП, 1/3”, прогресивне розгорнення, RGB.
– Об'єктив ІЧ-фільтр, об'єктив CS-mount, P-Iris, мегапіксельна розв’язна здатність Зі змінною фокусною відстанню 2,8–8,5 мм, F1,2 Горизонтальний кут огляду: 83°–33.3° Вертикальний кут огляду: 61°–24.7.
– Режим День/Ніч Автоматично керований інфрачервоний фільтр.
– Мінімальна освітленість Колір: 0,1 лк; ч/б: 0,01 лк, F1,2.
– HDTV 720p, 50/60 кадр/с: Колір: 0,4 лк; ч/б: 0,02 лк, F1,2.
– Швидкість спрацьовування затвора Від 1/28 000 з до 2 із при 50 Гц Від 1/33 500 з до 2 із при 60 Гц Відео.
– Стиск відео Профілі Baseline, Main і High кодека H.264 (MPEG-4, частина 10/AVC), Motion JPEG.
– Розв’язна здатність HDTV 720p, 25/30 кадр/с (з WDR): від 1280 x 960 до 160 x 90.
– HDTV 720p, 50/60 кадр/с (без WDR): від 1280 x 960 до 160 x 90.
– Частота кадрів До 50/60 кадр/с (50/60 Гц).
– Передача відеопотоку Передача декількох потоків, що налаштовуються окремо, у форматах H.264 і Motion JPEG.
– Технологія Axis Zipstream при використанні H.264.
– Контрольована частота кадрів і трафік VBR/MBR H.264.
– Передача декількох відеопотоків.
– До 8 окремих фрагментів загального зображення.
– Налаштування зображення. Регулювання стиску, кольору, яскравості, чіткості, контрасту, балансу білого, експозиції й ділянок експонування; широкий динамічний діапазон WDR-Forensic Capture: до 120 дБ залежно від об'єкта зйомки; тонке налаштування дій при слабкому освітленні; поворот: 0°, 90°, 180° і 270°а , накладення тексту на зображення, зони маскування, дзеркальне відбиття зображень Аудіо.
– Передача аудіо потоку. Двостороння повнодуплексна.
– Стиск аудіо. AAC LC 8/16/32/48 кГц, G.711 PCM 48 кГц, G.726 ADPCM 48 кГц; Що налаштовується бітрейт.
– Ввод/вивід аудіо. Вхід для зовнішнього мікрофона або лінійний вхід, лінійний вихід Мережа.

– Безпека. Захист паролем, фільтрація IP-адрес, шифрування HTTPSb ,контроль мережного доступу IEEE 802.1Xb , дайджест-перевірка дійсності, журнал доступу користувачів.

– Підтримувані протоколи: IPv4/v6, HTTP, HTTPSb , SSL/TLSb , Qo Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMPv1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SFTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH Системна інтеграція.

– Програмний інтерфейс. Відкритий API для інтеграції ПЗ, включаючи VAPIX® і платформу застосунків камер AXIS; Система відеохостингу AXIS Video (AVHS) з підключенням камери одним клацанням; Профіль ONVIF S;.

– Аналітика. Відеодетектор руху, активне оповіщення при несанкціонованих діях, детектор звуку.

– Підтримка платформи застосунків камер AXIS, що забезпечує установку таких застосунків як відеодетектор руху AXIS Video Motion Detection 3, детектор перетинання заданої лінії AXIS Cross Line Detection, автоматичне цифрове спостереження AXIS Digital Autotracking.

– Спрацьовування сигналу тривоги. Аналітика, події локального запису даних, зовнішній вхід, рівень звуку, розклад Дії по подіях.

– Завантаження файлів: по FTP, SFTP, HTTP, HTTPS і електронній пошті, через загальні мережні папки.

– Розсилання повідомлень: по електронній пошті, HTTP, HTTPS і TCP.

– Вихідний сигнал на зовнішнє встаткування.

– Відеозапис на зовнішній накопичувач, відтворення аудіокліпів.

– Буферизація відео до й після тривоги.

– Передвстановка PTZ, маршрут обходу охорони, накладення тексту.

– Перемикання режимів «день-ніч», активація індикаторів стану.

– Режим WDR.

– Відправлення SNMP-Пастки.

– Потокова передача дані Дані про події.

– Убудовані засоби установки Помічник фокусування, лічильник пікселів, віддалена регулювання заднього фокуса Загальні характеристики.

– Матеріал корпуса Полімерний корпус, клас захисту IP66, IP67 і NEMA 4X, клас ударомiцності IK10.

– Колір: білий NCS S 1002-B.

– Пам'ять ОЗП: 512 МБ, флеш-пам'ять: 256 МБ.

– Живлення. Технологія Power over Ethernet (PoE) IEEE 802.3af/802.3at, тип 1, клас 3; макс. 12,95 Вт, звичайно 5,0 Вт.

– Рознімання RJ45 10 BASE-T/100 BASE-TX PoE.

– Ввод-вивід: 4-контактна (2,5 мм) клемна колодка вводу/виводу для 2 входів, що налаштовуються-виходів.

– RS-485/422, 2 шт., 2 положення, повнодуплексний режим, клемна колодка.

– Мікрофонний/лінійний вхід 3,5 мм; лінійний вихід 3,5 мм.

– Рознімання керування діафрагмою P-iris (сполучимо з DC-iris).

– Локальне зберігання даних. Підтримка карт пам'яті microSD/microSDHC/microSDXC.

– Підтримка відеозапису по мережі на виділений мережний накопичувач (NAS).

– Умови експлуатації Від -40 до 50°C.

– Відносна вологість: 10-100% (з утворенням конденсату).

– Відповідність стандартам EN 55022, клас A; EN 61000-3-2; EN 61000-3-3; EN 55024; EN 61000-6-1; EN 61000-6-2; FCC, частина 15, розділ B, клас A; ICES-003, клас A;

VCCI, клас A; C-tick AS/NZS CISPR 22, клас A; KCC KN32, клас A, KN35; IEC/EN/UL60950;IEC/EN/UL60950EN50121-4/IEC 62236; IEC/EN/UL 60950-22; IEC/EN 60529 IP66; NEMA 250, тип 4X; IEC 60068-2-6; IEC 60068-2-27; IEC/EN 62262 IK10.

– Розміри 382 x 155 x 120 мм.

– Маса 1,8 кг.

– Приналежності в комплекті поставки Комплект рознімань, посібник з установки, ліцензія на декодер для Windows на 1 користувача, настінний кронштейн, сонцезахистний козирок. Датчик, що подає сигнал тривоги при вторгненні.

– Додаткові аксесуари Кріплення Axis, об'єктиви Axis, інжектори Axis Кронштейн для коридорного режиму AXIS Bracket A.

– ПЗ для керування відео. Застосунки AXIS Camera Companion, AXIS Camera Station,.

– ПЗ для керування відео, що поставляються партнерами Axis по розробці застосунків.

– Мови. Українська, англійська, німецька, французька, іспанська, італійська, китайська (спрощена), японська, корейська, португальська.

– Гарантія. Відомості про 3 -літню гарантію.

Мережна камера AXIS P 1365-E Mk II

– Надійна конструкція із захистом від ударів.

– Працює при температурах від -40°C до 50°C.

– Технологія Lightfinder дозволяє одержувати кольорові зображення навіть при дуже слабкому освітленні..

– Розв’язна здатність HDTV 1080p при частоті 50/60 кадр/с.

– Розроблена компанією Axis технологія Zipstream.

Міцна мережна камера AXIS P 1365-E Mk II, призначена для роботи в суворих умовах на вулиці, забезпечує відмінну якість зображення з високою деталізацією навіть при слабкому освітленні. AXIS P 1365-E Mk II прекрасно підходить для установки в банках, урядових закладах, на паркуваннях і будь-яких інших об'єктах, де необхідні зображення з високою деталізацією або огляд більших площ на відкритому повітрі.

Особливості Axis P 1365-E Mk II

Міцна модель, готова до роботи

Камера AXIS P 1365-E Mk II призначена для зовнішньої установки й експлуатації в екстремальних умовах – вона може працювати навіть при температурах -40°C і 50°C. Функція Arctic Temperature Control гарантує безпечний запуск камери при температурах до -40°C навіть після аварійного відключення живлення. Ви можете бути впевнені, що кожух камери зможе витримати як суворі погодні умови, так і дії вандалів, оскільки він має захист, що відповідає стандартам IP66, IP67, NEMA 4X і IK10. Модель AXIS P 1365-E Mk II поставляється в комплекті з настінним кронштейном і сонцезахистним козирком для захисту від пилу, дощу, снігу й сонячного світла.

AXIS P 1365-E Mk II дозволяє одержати якісне зображення, придатне для розпізнавання об'єктів – навіть при зйомці в темряві. Модель демонструє найвищу світлочутливість, що в сполученні з технологією Axis Lightfinder дозволяє одержувати високоякісні, причому кольорові, зображення навіть при слабкій освітленості й у темряві. А за допомогою технології WDR – Forensic Capture, що знижує рівень шуму й підсилює сигнал, ви будете мати зображення з високою деталізацією, незважаючи на нічний час зйомки. Відзначимо, що AXIS P 1365-E Mk II має розв’язна здатність HDTV 1080p і підтримує частоту до 50 або 60 кадр/с у форматах H.264 і Motion JPEG, що дозволяє вести зйомку швидкорухаючихся об'єктів і людей з високим розв’язною здатністю.

Висока якість. Низьке навантаження на мережу

У моделі AXIS P 1365-E Mk II застосована технологія Axis Zipstream, що дозволяє аналізувати відеопотік і визначати важливі ділянки зображення в режимі реального часу.

Знайдені важливі ділянки стискуються в меншому ступені, чим інша частина зображення, щоб зберегти деталі, що представляють інтерес, з максимальним розв'язною здатністю. Такий підхід скорочує трафік і обсяг пам'яті для зберігання даних на величину до 50%, у порівнянні з вихідним відеозаписом. У результаті вдається одержати зображення високої якості при значній економії ресурсів.

Таблиця 1 – Технічні характеристики IP-камери Axis P 1365-E Mk II

Камера	
Матриця	КМОП, 1/2.8", прогресивне розгорнення, RGB
Об'єктив	ІЧ-фільтр, об'єктив CS-mount, діафрагма P-iris Зі змінною фокусною відстанню 2,8 – 8 мм, F1,3 Горизонтальний кут огляду: 84° – 39° Вертикальний кут огляду: 46° – 21°
День/Ніч	Автоматично керований інфрачервоний фільтр
Мінімальна освітленість	Колір – 0.11 лк; ч/б – 0.01 лк, F1.3 HDTV 1080p, 50/60 кадр/с: колір – 0.22 лк; ч/б – 0.02 лк; F1.3
Швидкість спрацьовування затвора	Від 1/66500 до 2 з
Панорамування, нахил і масштабування	Цифрове PTZ-керування, що завантажується драйвер PTZ (передвстановлений Pelco D)
Відео	
Відеокодек	Профілі Baseline, Main і High формату H.264 (MPEG-4, частина 10/AVC) Motion JPEG
Розв'язна здатність	HDTV 1080p, 25/30 кадр/с (з WDR): від 1920 x 1080 до 160 x 90 HDTV 1080p, 50/60 кадр/с (без WDR): від 1920 x 1080 до 160 x 90
Потокове відео	Передача декількох потоків, що налаштовуються окремо, у форматах H.264 і Motion JPEG технологія Axis Zipstream при використанні H.264 Контрольована частота кадрів і смуга пропущення, VBR/CBR H.264
Передача декількох відеопотоків	До 8 окремих фрагментів загального зображення
Налаштування зображення	Стиск, колір, яскравість, чіткість, контраст, баланс білого, установка експозиції, області експозиції, компенсація зустрічної заствітлення, широкий динамічний діапазон з функцією Forensic Capture до 120 дБ залежно від об'єкта зйомки, тонке налаштування дій при слабкому освітленні, поворот: 0°, 90°, 180°, 270°, включаючи включаючи коридорний режим, накладення тексту й зображень, маска закритих зон; дзеркальне відбиття зображень.
Аудіо	
Передача аудіопотоку	Двостороння повнодуплексна
Стиск аудіо	AAC-LC 8/16 кГц, G.711 PCM 8 кГц, G.726 ADPCM 8 кГц Що налаштовується бітрейт
Мережа	
Безпека	Захист паролем, фільтрація IP-адрес, шифрування HTTPSc, контроль доступу по мережі IEEE 802.1Xc, дайджест-перевірка дійсності, журнал доступу користувачів
Підтримувані	IPv4/v6, HTTP, HTTPSc, SSL/TLSc, Qo Layer 3 DiffServ, FTP, SFTP,

протоколи	CIFS/SMB, SMTP, Bonjour, UPnPTM, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS, SSH
Потокова передача даних	Дані подій
Убудовані засоби установки	Помічник фокусування, лічильник пікселів, віддалене регулювання заднього фокуса
Загальні характеристики	
Корпус	Полімерний корпус, клас захисту IP66, IP67 і NEMA 4X, клас удароміцності IK10 Колір: білий NCS S 1002-B
Пам'ять	ОЗП: 512 МБ, флеш-пам'ять: 256 МБ
Живлення	технологія Power over Ethernet (PoE) IEEE 802.3af/802.3at, тип 1, клас 3, макс. 12,95 Вт, звичайно 4,3 Вт
Рознімання	RJ45 10 BASE-T/100 BASE-TX PoE Клемна колодка для 2 входів, що налаштовуються,/виходів для сигналів тривоги (на виході: 12 У пост. струму, макс. навантаження 50 мА) RS-485/422, 2 шт., 2 положення, повнодуплексний режим, клемна колодка Мікрофонний/лінійний вхід 3,5 мм; лінійний вихід 3,5 мм Рознімання керування діафрагмою P-Iris (сполучимо з DC-iris)
Локальне зберігання даних	Підтримка карт пам'яті microSD/microSDHC/microSDXC Підтримка відеозапису на виділений мережний накопичувач (NAS) Рекомендації з вибору карт SD і мережного накопичувача NAS можна знайти на сайті www.axis.com
Умови роботи	Від -40°C до 50°C Відносна вологість 10-100% (з конденсатом)
Відповідність стандартам	EN 55022 клас B; EN 55024; EN 61000-6-1; EN 61000-6-2; FCC частина 15 розділ B клас B з екранованим кабелем (STP); FCC частина 15 розділ B клас A з неекранованим кабелем (UTP); ICES-003 клас B; VCCI клас B; RCM AS/NZS CISPR 22 клас B; KCC KN32 клас B; KN35; IEC/EN/UL 60950-1; IEC/EN/UL 60950-22 EN 50121-4/IEC 62236, IEC/EN 60529 IP66, IEC/EN 60529 IP67, NEMA 250, тип 4X, IEC 60068-2-6, IEC 60068-2-27, IEC/EN 62262 IK10
Вага	1,8 кг
Розміри	382 x 155 x 120 мм
Приналежності в комплекті	Комплект рознімань, посібник з установки, однокористувальницька ліцензія на декодер для Windows, компакт-диск із засобами для установки й керування, настінний кронштейн, сонцезахистний козирок
Додаткові аксесуари	Кабельна коробка AXIS T94R01P Кріплення для монтажу на стовпі AXIS T91A47 Кронштейн для коридорного режиму AXIS Bracket A Дверний датчик AXIS Door Switch A Монтажна шафа AXIS T98A 16-VE
ПЗ для керування відео	Застосунки AXIS Camera Companion, AXIS Camera Station, ПЗ для керування відео, що поставляються партнерами Axis по розробці застосунків, доступні на сторінці www.axis.com/techsup/software
Гарантія	Відомості про 3 -літньої гарантії Axis і варіанті розширеної гарантії

Розробка структурної схеми

Сучасне життя неможливо представити без систем відеоспостереження. Вони встановлюються всюди – в аеропортах і на вокзалах, у банках і супермаркетах, у заміських будинках і приватних квартирах. Легко можна переконатися, що установка відеоспостереження стала однією з головних прикмет сучасності.

Пристрої, що входять до складу систем відеоспостереження, постійно вдосконалюються. Завдяки цьому щорічно з'являються більше точні й більше надійні системи відеоспостереження.

У цей час найбільшим попитом користуються два типи систем відеоспостереження. У першому типі установка відеоспостереження використовує персональний комп'ютер у якому є необхідне програмне забезпечення й плата відеозахвата. Другий тип відеосистем використовує цифровий реєстратор, що скорочено називають DVR (Digital Video Recorder).

Сучасні системи відеоспостереження можуть не тільки спостерігати за подіями або записувати їх, але й транслювати відеозапис по Інтернету або передавати її на мобільний телефон.

По своєму центральному влаштуванню відеосистеми підрозділяються на кілька типів:

Перший тип – найпростіша й найдешевша система – аналогова система відеоспостереження, основним пристроєм якої є квадратор. Цей пристрій виводить на монітор зображення, що надходять від декількох різних відеокамер. Різні режими роботи квадратора дозволяють виводити на монітор зображення від однієї камери, або від всіх одночасно, або виводити зображення по черзі.

Однак система на базі квадратора може записувати події тільки тоді, коли вона оснащена додатковим пристроєм – відеомагнітофоном. Тому установка відеоспостереження, що використовує квадратор, доцільна тільки на тих об'єктах, які цілодобово охороняються. Це можуть бути, наприклад, паркування, прохідні або автостоянки.

Другий тип – система відеоспостереження на базі відеореєстратора. Вона має більше широке коло функцій, тому що реєстратор приймає, аналізує, обробляє й записує всі вступників на нього дані. До одного відеореєстратора модно підключити від 16-ти до 64-х відеокамер. Така відеосистема легко передає зображення по Інтернету, на смартфон, на персональний комп'ютер. Набір функцій відеореєстратора набагато більше, ніж квадратора.

Останнім часом все частіше встановлюється відеоспостереження на базі персонального комп'ютера. Такий тип відеосистем набагато більше зручний і функціональний по порівнянням з аналоговим типом. Для включення у відеосистему в комп'ютер вставляється додатковий пристрій – плата відеозахвату. Ця плата, за допомогою необхідного програмного забезпечення трансформує аналоговий сигнал у цифровий формат.

Перетворений сигнал може стискуватися, записуватися, архівуватися, виводитися на екран. До входу-виходу плати відеозахвата можна підключити відразу кілька камер відеоспостереження. Останні розробки відеоплат оснащені важливою функцією стиску відеоінформації. Примітно те, що відеоспостереження в нічних умовах поводиться також як і в денний час доби.

IP система відеоспостереження використовує, у якості складових, IP-камери й IP-відеореєстратори. Для передачі відеопотоків використовується стек протоколів TCP/IP. У даний момент це саме динамічно, що розвивається напрямок, ринку, чому сприяє неухильно, що знижується вартість, що становить системи.

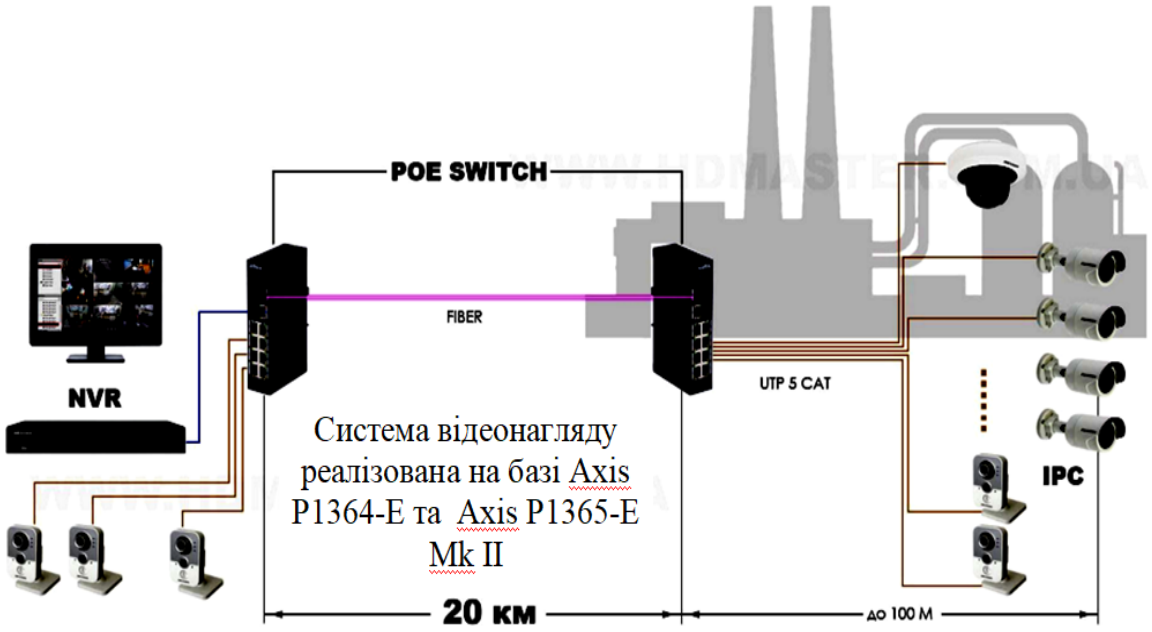


Рисунок 1 – Структурна схема системи

Переваги:

– Висока розв'язна здатність, обмежена лише пропускною здатністю мережі й параметрами використовуваного устаткування.

– Відстань передачі відеопотоку від IP-камери відеоспостереження не обмежено межами локальної мережі. У такий спосіб досягається масштабованість системи. IP-відеореєстратор здатний записувати відеопотоки від IP-камер що перебувають, наприклад, в іншому місті.

– Можливість використання для передачі відеопотоків існуючі комп'ютерні мережі.

– Можливість тонкого налаштування параметрів IP-відеокамер через web-інтерфейс. Настроїти можна як параметри зображення, такі як: яскравість, контрастність, колірний баланс, так і вибрати кодек для роботи з відеозображенням, виставити зони зображення по яких камера видасть сигнал об виявлення руху, указати e-mail або параметри ftp сервера, на який будуть відправлені кадри у випадку виявлення руху в кадрі й багато чого іншого.

– Завдяки технології TCP/IP стала можливим побудова бездротових систем HD і Full HD відеоспостереження що використовують Wi-Fi камери.

– Розв'язна здатність IP камер і реєстраторів не обмежується розв’язною здатністю HD і Full HD. Бюджетний сегмент ринку завойовують камери й реєстратори підтримуюча розв’язна здатність 4 Мп і все більше застосування знаходить устаткування розв’язної здатності 4k (8 – 12 Мп).

Мережний відеореєстратор (NVR) вхідний у комплект для IP відеоспостереження виконує роль сервера запису відеопотоків від камер. Його завдання – забезпечити надійний запис на жорсткий диск, надати зручний і швидкий пошук потрібного відео в архіві за цікавлюючому вас критерієм, будь то пошук за часом доби або по тривожній події, такому як рух у кадрі. Крім того, до NVR можна одержати доступ із клієнтського ПЗ, для віддаленого перегляду живого відео й архівів на смартфонах, планшетах або за допомогою віддалених стаціонарних PC.

Мережні протоколи, застосовувані в IP-відеоспостереженніIP-відеокамери використовують у своїй роботі безліч мережних протоколів, необхідних, як для передачі відео-потоку по мережі, так і для дистанційного керування камерою. У даній статті коротко розглянуті найбільше часто застосовувані в IP-відеоспостереженні мережні служби й протоколи:

– IPv4 – Міжмережевий протокол IP (Internet Protocol) четвертої версії, уперше описаний в 1981 році й донині є основним протоколом, що об'єднав локальні мережі в глобальну мережу Інтернет.

– В IPv4 застосовуються чотирьохбайтні (32 бітні) адреси (один байт це десяткове число від 0 до 255), таким чином, IP адреса може виглядати, наприклад, так: 192.168.0.5. Істотним недоліком протоколу IPv4 є обмежена кількість унікальних адрес 2^{32} = 4 294 967 296, причому, ще ряд адрес зарезервований для: мереж сервісів-провайдерів, приватних мереж і інших службових цілей. Це змушує застосовувати так звані динамічні IP адреси, тобто адреси, які надаються клієнтові тільки на певний час із області незайнятих адрес даної підмережі.

– IPv6 – новий Інтернет протокол, випущений в 1996 році, зі збільшеною довжиною адреси до 128 біт, що дозволить, по різних підрахунках, забезпечити кожного жителя землі від 300 мільйонів до $5x10^{28}$ унікальних адрес. Насправді, такий великий простір адрес зроблений для ієрархічного розподілу, що спростить маршрутизацію, таким чином, значна частина адрес не буде використана взагалі.

– IPv6 адреси представляються як вісім груп шістнадцяткових цифр розділених двокрапками, наприклад: 2000:11a3:13dc:05fd:ff21:ccf2:123f:01ff.

– У даний момент, IPv6 використовується не значно, у майбутньому планується спільне використання протоколів як IPv6, так і IPv4 для підтримки застарілих пристроїв.

– HTTP (HyperText Transfer Protocol) – протокол для передачі гіпертексту за технологією « клієнт-сервер». Клієнт, тобто Інтернет браузер користувача, подає запит на сервер у вигляді URL (Uniform Resource Identifier) – унікального ідентифікатора ресурсу й одержує із сервера запитувану WEB сторінку.

– Гіпертекст – це спеціально відформатований текс за допомогою, так званих HTML (HyperText Markup Language – мова розмітки гіпертексту) ТЕГів, які розпізнає Інтернет браузер, наприклад Internet Explorer. Приклад форматування може виглядати так:Привіт Всім!, що відобразиться в браузері курсивом – *Привіт Всім!*

– HTTPS (Hypertext Transfer Protocol Secure) – Модифікація протоколу HTTP з можливістю шифрування даних криптографічними протоколами SSL і TLS. Даний протокол застосовується, наприклад, для автентифікації користувачів, передачі важливих документів, у платіжних системах і т.п.

– FTP (File Transfer Protocol) – протокол передачі файлів, розроблений в 1971 році. Застосовується, наприклад, для закачування файлів на сервер, скачування файлів із сервера на локальний комп'ютер і тому подібних завдань. Звичайно використовується з FTP – клієнтом, програмою, як правило, із двома вікнами, де «перетаскуючи» мишею файли й папки з одного вікна в інше здійснюється завантаження/вивантаження файлів.

– TCP (Transmission Control Protocol) – протокол керуючий передачею даних, що перевіряє установку мережного з'єднання, надсилає новий запит у випадку втрати пакетів і не допускає дублювання пакетів. Таким чином, здійснюється надійна передача даних з повідомленням сторони, що відправляє, про якість передачі.

– UDP (User Datagram Protocol) – протокол передачі так званих «датаграм» – блоків даних, без перевірки успішності з'єднання, втрати пакетів і дублювання, що значно знижує якість передачі даних. Однак такий підхід буває досить корисний при коротких запитах від великої кількості клієнтів до сервера, як, наприклад, в онлайн-іграх, що звільняє сервер від очікування перевірки цілісності пакетів.

– DNS (Domain Name System) – система доменних імен, відповідальна за відповідність IP-адрес іменам хостов. Звичайно використовується для визначення IP-адреси по ім'ю хоста (по ім'ю сайту).

– DHCP (Dynamic Host Configuration Protocol) – протокол необхідний для автоматичного одержання комп'ютером IP-адреси й інших параметрів необхідних для нормальної роботи в мережі.

– SMTP (Simple Mail Transfer Protocol) – протокол для передачі пошти в Інтернеті, розроблений в 1982 році, застосовується, в основному, для відправлення вихідної пошти із клієнтської програми, наприклад "Outlook", на поштовий сервер.

– RTP (Real-time Transport Protocol) – протокол для передачі даних у реальному часі, з контролем послідовності пакетів і синхронізації даних. Даний протокол добре підходить для передачі відео й аудіоданих по мережі.

– DynDNS – сервіс який дозволяє користувачеві з динамічним IP-адресою, одержати піддомен (доменне ім'я третього рівня), зі статичною адресою, на який, сервіс DynDNS перенаправляє запит користувача.

– Таким чином, комп'ютер, IP камера або будь-який інший мережний пристрій працює, начебто, з постійним IP-адресою. Статичний IP-адреса необхідна для роботи мережних камер.

– NTP (Network Time Protocol) – протокол призначений для синхронізації внутрішніх годин комп'ютера зі службами точного часу, наприклад – GPS.

– RTSP (Real Time Streaming Protocol) – протокол призначений для керування даними від мультимедіапристроїв, наприклад IP-камери, з можливістю передачі команд: "старт", "запис", "стоп" і т.п.

– RTCP (Real-Time Transport Control Protocol) – протокол передачі керуючих пакетів у реальному часі, що працює разом з RTP, забезпечуючи зворотний зв'язок і контроль якості передачі даних.

– IGMP (Internet Group Management Protocol) – протокол що дозволяє організовувати мережні пристрої в групи за допомогою маршрутизатора. Наприклад, для передачі даних від відео-сервера до численних клієнтів, що приймають відео^-трансляцію.

– ICMP (Internet Control Message Protocol) – протокол посилаючий повідомлення про помилки передачі даних, наприклад: "помилка автентифікації", "порт недосяжний", "вузол призначення невідомий" і т.п.

– ARP (Address Resolution Protocol) – протокол визначальний MAC-адреса по відомому IP-адресі.

– MAC-адреса (Media Access Control) – унікальний ідентифікатор, що перебуває в пам'яті кожного мережного пристрою.

– SOCKS – протокол, що дозволяє програмним клієнтам, що перебувають за міжмережевим екраном, звертатися до зовнішніх серверів. І, навпаки – зовнішнім клієнтам підключатися до серверів за мережним екраном.

– PPP (Point-to-Point Protocol) – протокол для здійснення прямого зв'язку між двома вузлами мережі, з можливістю стиску даних і шифрування.

– PPPoE (Point-to-point protocol over Ethernet) – протокол передачі кадрів протоколу PPP по мережах Ethernet.

– Bonjour – служба автоматичного виявлення мережних пристроїв у ближнім мережному оточенні, що використовує дані з DNS.

– UPnP (Universal Plug and Play) – технологія, що забезпечує автоматичне підключення й налаштування мережних пристроїв, відразу після приєднання до мережі. Дана технологія значно облягає використання мережних пристроїв звичайним користувачам.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Досліджена система відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II.

На основі отриманих результатів досліджень створена програмна реалізація системи відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Розроблені алгоритми дозволяють успішно вирішувати завдання відеонагляду реалізованої на базі Axis P1364-E та Axis P1365-E Mk II. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти,

взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
2. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
3. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.В. Коваленко // Тези доповідей Новітні технології – для захисту повітряного простору. Дев'ята наукова конференція. 18-19 квітня 2011 р. – Х.: ХУПС. – 2012. – С. 206
4. Дрєєв О.М. Вдосконалення стиснення зображень SPIHT методу шляхом додаткового кодування та відкладеної передачі уточнення вейвлет коефіцієнтів / О.М. Дрєєв // Дискретна математика та її застосування у економіко-математичному моделюванні та інформаційних технологіях. 11-13 жовтня 2012 р. – Запоріжжя: ЗНУ – 2012. – С. 22-23.
5. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19
6. Дреев А.Н. SPIHT кодирование с отложенной передачей значимых битов / А.Н. Дреев // Тези доповідей. Новітні технології – для захисту повітряного простору. Дев'ята наукова конференція 17 квітня 2013 р. – Х.: ХУПС. – 2013. – С. 206
7. Дреев А.Н. Повышение оперативности доставки данных повышенной востребованности в телекоммуникационных системах и сетях / А.Н. Дреев, А.А. Смирнов, Е.В. Мелешко // Проблеми і перспективи розвитку IT-індустрії 25-26 квітня 2013 р. Системи обробки інформації. – Випуск 3 (110). Том 2. – Харків: ХУПС. – 2013. С. – 199.
8. Дрєєв О.М. Середньостатистичний та найімовірніший час доставки багатопакетного повідомлення в телекомунікаційній системі або мережі / О.М. Дрєєв, О.А. Смірнов // V Всеукраїнська науково-практична конференція "Інформатика та системні науки" ІСН – 2014, 13-15 березня 2014 року, м. Полтава – С. 92
9. Дреев А.Н. Экстраполяция квазипериодических процессов с аддитивными помехами / А.Н. Дреев, А.А. Смирнов // П'ята Міжнародна науково-практична конференція "Інформаційні технології та моделювання в економіці" 15-16 травня 2014 р. – Черкаси – С. 59
10. Дреев А.Н. Статистическая модель передачи многопакетного сообщения в телекоммуникационной системе или сети / А.Н. Дреев, А.А. Смирнов // «Компьютерное моделирование в наукоемких технологиях (КМНТ-2014)» Харьков, 28-31 мая 2014 года – С. 137-140

УДК 004

В. Свистунов, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АВТОМАТИЗАЦІЇ ВИРОБНИЧИХ ПРОЦЕСІВ СТВОРЕННЯ СОНЯЧНИХ БАТАРЕЙ КЛАСУ TIER 2

У статті розроблено програмне забезпечення, яке призначено для системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Метою розробки є дослідження та програмна реалізація системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Об'єктом дослідження є процес автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Предметом дослідження є методи автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Методи дослідження

базуються на методах теорії автоматизованого управління, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, сонячні батареї, Tier 2

Постановка проблеми. Загальновизнано, що основним фактором розвитку цивілізації є використання джерел енергії. В основному ми використовуємо традиційні енергоресурси, такі як – нафта, вугілля, природний газ. При цьому наноситься колосальний збиток екології нашого загального будинку за назвою ЗЕМЛЯ. Сотні тисяч барелів нафти зливаються в океан, мільйони тонн окису вуглецю викидаються в атмосферу, чотири сотні АЕС виробляють десятки тонн радіоактивних відходів [1-5].

Але справа не тільки в цьому, запаси цих традиційних джерел далеко не нескінченні. Тому їх відносять до непоновлюваних джерел енергії.

Наприклад, у рік у світі споживається стільки нафти, скільки її утвориться за 2 млн. років [2]. У зв'язку із цим останнім часом велика увага приділяється так званим поновлюваним джерелам енергії, таким як енергія вітру, сонця, припливу й т.д. У цьому ряді сонячна енергетика посідає не останнє місце.

Повна кількість сонячної енергії, що надходить на поверхню Землі за тиждень перевищує енергію всіх світових запасів нафти, газу, вугілля й урану [6].

Перетворення сонячної енергії в електричну здійснюється нині в тому числі й за допомогою фотоелектричних перетворювачів – ФЕП. Матеріалом для них служить один з найпоширеніших у земній корі елементів – кремній, а "паливом" – безкоштовні сонячні промені. Як стаціонарні джерела електрики, фотоелектричні станції привабливі для районів, не забезпечених електрикою від централізованої енергосистеми. Установка сонячних модулів вигідна там, де витрата енергії незначна, а проводка електромереж вимагає чималих витрат [2-8].

Для забезпечення потреб у сонячних батареях, необхідно виробництво по їх виробленню. Для підвищення якості виробництва, запроваджують автоматизовані системи управління.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем автоматизації виробничих процесів створення сонячних батарей класу Tier 2.

– Дослідження системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2.

– Програмна реалізація системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2.

Об'єктом дослідження є процес автоматизації виробничих процесів створення сонячних батарей класу Tier 2.

Предметом дослідження є методи автоматизації виробничих процесів створення сонячних батарей класу Tier 2.

Методи дослідження базуються на методах теорії автоматизованого управління, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Для виробництва елементів сонячних батарей, використовується автоматизована система, елементом якої є ряд верстатів з ЧПУ, які,

виходячи із завантаженого програмного забезпечення, виконують ту або іншу операцію, по формуванню елемента сонячної батареї.

Всі команди передаються по лініях зв'язку, які використовують інтерфейс передачі даних з керуючого пристрою на верстат з ЧПУ.

Один з можливих варіантів відкритої архітектури системи керування наведено на рисунку 1.

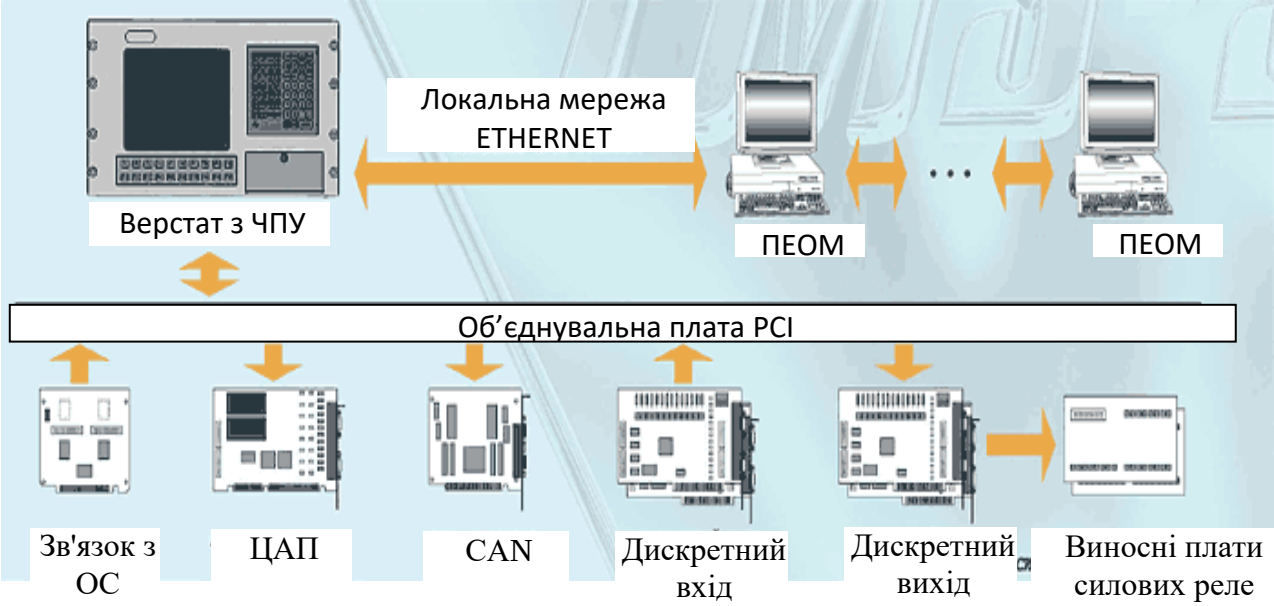


Рисунок 1 – Відкрита архітектура системи керування

Основа системи керування верстатом з ЧПУ для формування елемента сонячної батареї – персональний комп'ютер промислового виконання, виготовлений по новітніх технологіях. Відкрита архітектура системи керування в комплексі з потужним програмним забезпеченням дозволяють легко інтегрувати в її состав комп'ютерні компоненти провідних виробників обчислювальної техніки.

Програмне забезпечення системи реалізоване на базі ядра твердого реального часу, що гарантує високу якість виконання таймерних завдань керування сервоприводами й циклами електроавтоматики. Завдяки новій технології Biesse WRT (Windows Real Time), що розширює функціональні можливості Windows для роботи в реальному часі, стійка ЧПУ верстата перебуває безпосередньо на ПК, що дозволяє сконцентрувати все необхідне апаратне забезпечення без використання додаткових плат керування. Відкрита структура системи дозволяє включати до складу системи програмні модулі користувача. При реалізації системи необхідно реалізувати наступні модулі:

Модуль графічної підтримки. Графіка дозволяє:

переглядати реальний рух інструмента;

перевіряти елементи траєкторії інструмента при відключеному верстаті;

робити точне настроювання приводів у режимі осцилоскопування.

Модуль пооперацийного контролю. Система виготовляється з використанням пооперацийного контролю, починаючи від підготовки виробництва й до випуску готового виробу, включаючи температурний прогін з наступною функціональною перевіркою роботи всіх модулів. Технологічне програмування використовує:

звичні G-функції;

трибуквені коди, що дозволяють давати осмислені назви макрокомандам;

вбудована мова опису графічних об'єктів, що дозволяє програмувати складні 2D контури безпосередньо із креслення без використання САПР. ЧПУ сам обчислює крапки перетинання й торкання геометричних елементів. Таке рішення дозволяє легко орієнтуватися у виборі функцій для складання керуючих програм вручну.

Середовище статистичних даних, у якому записуються дані про роботу верстата й вироблених деталей, щоб здійснювати моніторинг надійності в часі й продуктивності верстата. Середовище може конфігуруватися під користувача, що дозволяє реєструвати можливих операцій, наприклад, таких як настроювання верстата, контроль обробки, задані паузи, цикли змащення елементів верстата й т.д.

Система телесервісу. Дозволяє миттєво одержувати прямий доступ через модем до стійки ЧПУ верстата. Таким чином, дозволяє перевірити дані верстата, програми користувача, сигнали вводу/виводу, змінні системи, а також установлювати оновлені версії ПЗ, що дозволяє:

Проводити діагностику в реальному часі

Швидко вирішувати проблеми

Зменшити час простою

Установлювати оновлені версії ПЗ в реальному часі

Обслуговування й робота з ЧПУ при формуванні елемента сонячної батареї не викликає ніяких труднощів у персоналу. Через повідомлення користувачеві надається повний контроль за виконуваними операціями, а також за станом комплексу ЧПУ – верстат.

Керування пристроєм ЧПУ повинне бути виконане в діалоговому режимі з використанням меню, що дозволяє легко орієнтуватися у виконуваних операціях.

Система підключення верстатів до ПЕОМ, що дозволяє інтегрувати існуючі верстати з ЧПУ, призначені для виробництва елементів сонячних батарей, (у тому числі й з морально й фізично застарілими системами ЧПУ) із сучасними CAD/CAM-системами повинна відповідати наступним вимогам:

– Висока надійність роботи.

– Використання наявного (найчастіше застарілого) устаткування. При цьому вартість модернізації не повинна перевищувати 1-5% вартості верстата.

– Підключення в мережу верстатів з будь-якими інтерфейсами введення інформації з єдиного протоколу. Дана вимога пов'язане із широким спектром наявного встаткування із всілякими інтерфейсами введення інформації – від магнітної стрічки й перфострічки до портів RS-232, RS-422 та USB. Єдиний протокол зв'язку з верстатами дозволяє значно спростити матзабезпечення на ПЕОМ. Можлива автоматична фіксація завантаження верстатів, включених у мережу, і передача відповідної інформації.

– Передача керуючих програм великого й особливо великого обсягу. Одноразова передача керуючих програм на верстати, а якщо керуюча програма перевищує мегабайт, то й організація режиму «підкачування». Отримані в ЧПУ програми можуть бути піддані корекції, тому керуюча програма повинна бути передана на верстат по можливості одноразово

– Відсутність доробок пристроїв ЧПУ верстата. Очевидно, що підключення верстата в мережу доцільно здійснювати через наявні у верстаті інтерфейси вводу-виводу.

– Максимально просте спілкування оператора верстата з ПЕОМ. У пристроях сполучення передбачені індикація й клавіатура, що дозволяють операторові верстата приймати/передавати необхідні керуючі програми/параметри від ПЕОМ і відслідковувати режими передачі.

– Технічні засоби підключення в комп'ютерну мережу повинні бути основою для розробки гнучкого програмного забезпечення (залежно від умов конкретного виробництва), що дозволяє значно скоротити строки впровадження керуючих програм для обробки різних деталей на верстатах з ЧПУ.

– Система передачі керуючої програми на верстати з ЧПУ повинна працювати як з архівом керуючої програми, так і з базою даних керуючої програми, що найчастіше використовує СУБД працюючої на підприємстві АСУ.

Опис запропонованої модернізації існуючого програмного забезпечення

На існуючих верстатах з ЧПУ, механіка дозволяє, а застаріла електроніка верстата, а також можливості завантажувальних пристроїв і носія інформації не дозволяють повністю

автоматизувати систему виробництва сонячних модулів. Тобто. для того, щоб верстати працювали в повністю автоматизованому режимі, необхідно до існуючого програмного забезпечення розробити ряд програмних модулів, які б дозволили прибрати існуючі недоліки.

Програмне забезпечення, яке дозволяє ліквідувати деякі з недоліків, виявлених в результаті проведення дослідження, описаного у попередньому пункті. Зокрема при вирішені проблеми завантаження керуючих програм великого розміру в існуючі верстати з ЧПУ, для виробництва елементів сонячних батарей, з їхнім малим обсягом пам'яті, вихід полягає в реалізації наступного принципу: якщо в стійки не може бути цілком завантажена велика керуюча програма – її треба розбити на частини, а верстати нехай виконують програму, одержуючи її з одного центрального комп'ютера малими порціями. Керуюча програма великого обсягу, обробляється спеціальною програмою й одержує змінену керуючу програму (єдина велика керуюча програма усередині, розбита на шматки меншого розміру, що дозволяє завантажити шматок у стійку й оформлена образом, підходящим для стійки). Зі стійки запитується перетворений єдиний файл, що складається зі шматків. Перший раз завантажується перший шматок, потім він відпрацьовується. По завершенні шматка автоматично видаляється відпрацьований шматок з пам'яті й запитується наступний шматок єдиного файлу керуючої програми. Відпрацьовує – видаляє – запитує наступний шматок. Так доти, поки не будуть обрані всі шматки єдиного файлу керуючої програми.

Наступним моментом удосконалення стандартного програмного забезпечення є застосування передачі керуючої програми на верстат ЧПУ та даних, за допомогою USB порту.

Розглянемо пристрій USB всередині. Одна з головних концепцій USB полягає в тому, що в USB-системі може бути тільки один майстер. Їм є host-комп'ютер. USB – пристрою завжди відповідають на запити host-комп'ютера – вони ніколи не можу посилати інформацію самостійно. Є тільки одне виключення: після того, як хост перевів пристрій в suspend-режим, пристрій може надсилати запит remote wakeup. У всіх інших випадках хост формує запити, а пристрою відповідають на них. Хост завжди є майстром, а обмін даними повинен здійснюватися в обох напрямках:

OUT – відсилаючи пакет із прапором OUT, хост відсилає дані пристрою

IN – відсилаючи пакет із прапором IN, хост відправляє запит на прийом даних із пристрою.

До цьому потрібно просто звикнути. Щоб прийняти дані із пристрою, хост відсилає пакет із прапором IN. smile

По USB може передаватися кілька типів пакетів:

1. Token – запит, містить керуючу інформацію: напрямок операції (IN, OUT), номер endpoint

2. Data – пакет даних

3. Handshake – службові пакети, можуть містити підтвердження (ACK), повідомлення про помилку, відмова (NACK)

4. Special – службові пакети, такі як PING

Відсилання даних верстату ЧПУ, який застосовується для формування елемента сонячної батареї, виконуються в такий спосіб:

Щоб відіслати дані верстату, хост посилає пакет Token "OUT", потім пакет Data. Якщо верстат готовий обробити прийняті дані, він відсилає пакет Handshake "ACK", що підтверджує транзакцію. Якщо він зайнятий, то відсилає відмову – Handshake "NACK". Якщо відбулася якась помилка, то пристрій може не відсилати Handshake.

Для відсилання даних хосту виконуються наступні дії. Як уже говорилося, пристрій самостійно ніколи не відсилає дані. Тільки по запиту. Щоб прийняти дані, хост посилає пакет Handshake "IN". Пристрій по запиту може відіслати пакет Data, а потім Handshake "ACK". Або може відіслати Handshake "NACK", не посилаючи Data.

Специфікація USB визначає 4 типи потоків даних:

1. bulk transfer – призначений для пакетної передачі даних з розміром пакетів 8, 16, 32, 64 для USB 1.1 і 512 для USB 2.0. Використовується алгоритм перепосилки (у випадку виникнення помилок), а керування потоком здійснюється з використанням handshake пакетів, тому даний тип є достовірним. Підтримуються обоє напрямку – IN і OUT.

2. control transfer – призначений для конфігурування й керування пристроєм. Також, як і в bulk, використовуються алгоритми підтвердження й перепосилки, тому цей тип забезпечує гарантований обмін даними. Напрямку – IN (status) і OUT(setup, control).

3. interrupt transfer – схожий на bulk. Розмір пакета – від 1 до 64 байт для USB 1.1 і до 1024 байт для USB 2.0. Цей тип гарантує, що пристрій буде опитуватися (тобто хост буде відсилати йому token "IN") хостом із заданим інтервалом. Напрямок – IN.

4. isochronous transfer – призначений для передачі даних без керування потоком (без підтверджень). Область застосування – аудіо-потоки, відео-потоки. Розмір пакета – до 1023 байт для USB 1.1 і до 1024 байт для USB 2.0. Передбачений контроль помилок (на прийомній стороні) по CRC16. Напрямки – IN і OUT.

Специфікація USB визначає endpoint (EP), як джерело або приймач даних. Пристрій може мати до 32 EP: 16 на прийом і 16 на передачу. Звертання до того або інший endpoint'у відбувається по його адресі.

EP0 має особливе значення для USB. Це Control EP. Він повинен бути в кожному USB-пристрої. Цей EP використовує token "setup", щоб сигналізувати, що дані, що відправляються після нього, призначені для керування пристроєм. Використовуючи цей EP0, хост може передавати setup-пакет довжиною 8 байт і дані, які випливають за цим пакетом. У багатьох випадках може вистачати передачі тільки setup-пакета. Однак пристрій може використовувати й передачу даних по EP0, наприклад для зміни прошивань компонентів пристрою, або одержання розширеної інформації про пристрій. Розглянемо побайтно setup-пакет. Байт № 0 – bmRequestType – Поле для вказівки типу запиту, напрямку, одержувача. Байт № 1 – bRequest -ідентифікатор запиту. 2 – wValue – 16-бітне значення wValue, залежить від запиту. 3 – wValue. 4 – wIndex 16-бітне значення wIndex, залежить від запиту. 5 – wIndex. 6 -wLength кількість байт, що відсилаються після setup-пакета. 7 – wLength. Як видно setup-пакет містить 5 полів. bmRequestType і bRequest визначають запит, а wValue, wIndex і wLength – його властивості. Специфікація USB резервує діапазон значень bRequest під стандартні запити. Кожний пристрій зобов'язаний відповідати на всі стандартні запити. Далі наведені тільки кілька стандартних запитів, з якими ми будемо зіштовхуватися далі.

0x05 Set Address установка унікальної адреси пристрою в системі.

0x06 Get Descriptor одержання інформації про пристрій. Тип інформації залежить від поля wValue.

Інший діапазон пристрій може використовувати за своїм розсудом.

Розпізнавання пристрою, що тільки що підключився до системи відбувається в такий спосіб. Уже згадувалося, що кожний пристрій зобов'язаний забезпечити доступ до EP0. Але крім цього, воно ще повинне відповідати на запити, зазначені в специфікації USB для EP0. Користуючись цими запитами й відбувається розпізнавання пристрою в системі.

Алгоритм детектування нового пристрою наступний:

1. хост відсилає setup-пакет "Get Descriptor" (wValue = "device").

2. хост одержує ідентифікуючу інформацію про пристрій

3. хост відсилає setup-пакет "Set address", після чого пристрій одержує унікальну адресу в системі

4. хост відсилає інші setup-пакети "Get Descriptor" і одержує додаткову інформацію про пристрій: кількість EP, вимоги до живлення, і т.п.

Розроблювальне програмне забезпечення повинне включати наступні програмні блоки:

– програму мікроконтролера для кожного типу стійки, що забезпечує інтерфейс зі стійкою ЧПУ;

– програму для комп'ютера по обслуговуванню верстатів;

– програму для комп'ютера по індикації якості мережі;

– програму для комп'ютера – драйвер для адаптера мережі.

Розробка структурної схеми

Розробка програмного забезпечення системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2 було розроблене додаткове програмне забезпечення для верстата LGZTT-500, що забезпечує його додатковими функціями – контролю параметрів шаблона майбутньої пластини сонячної батареї, її розміри та інші технічні характеристики. Програмне забезпечення розроблено на основі програмного забезпечення, яке поставляється з верстатом, та доповнює стандартне програмне забезпечення рядом функцій перерахованих вище. Пр цьому введена можливість передавати дані на верстат за допомогою додаткового USB порту.

Верстат LGZTT-500 під який розроблене додаткове програмне забезпечення був закуплений товариством з обмеженою відповідальністю малим впроваджувальним підприємством «ОКХ Ярило» (далі ТОВ МВП «ОКХ Ярило»).

При експлуатації верстата виявилось ряд дефектів у програмному забезпеченні що поставляється з верстатом, а саме – відсутність можливості керування за допомогою ПЗ розмірами пластини та її технічними параметрами та отримувати кодів відповідей верстата при його роботі над пластиною. Всі ці дії виконуються у ручному режимі при нагляді оператора що значно ускладнює процес виготовлення через можливий людський фактор, що може привести до збою верстату та його поломку. Приведена структура станка та коди взаємодії дозволили розробити додаткове програмне забезпечення що я і виконав у магістерській роботі.

Розглянемо структурну схему роботи системи, а саме повний цикл виробничого процесу сонячних панелей. Без короткого огляду процесу виготовлення неможливо зрозуміти роль розробленого магістерського програмного забезпечення.

На рисунку 2 представлена розроблена структурна схема роботи системи, розглянемо її детально (зліва на право) для розуміння дій над верстатом та роботу програми.

Після закупки полікристалічного кремнію (покупної сировини) проводиться виробництво технічних злитків які будуть завантажуватися у верстат. Отримуються замовлення батарей (пластин) від покупців, докладні параметри батареї (пластин). Після цього інженери проводять аналіз цих даних та корегують виробничий процес якщо це необхідно, задають параметри у верстат та проводять виробництво батарей (пластин). Далі виконується перевірка технічних параметрів батарей (пластин) та поставка пластин замовникові.

У цей час у світі більше 90% фотоелементів виробляється на основі полікристалічного кремнію за технологіями, заснованим на використанні трихлорсилана.

Рисунок 2 – Структурна схема системи

«ОКХ Ярило» закупає полікристалічний кремній за високою ціною так як процес його виготовлення громіздкий та дорогий.

Через це кожний брак панелей являє собою значні матеріальні втрати товариства та розроблена магістерська програма дозволяє у значній мірі виправити це становище.

Процес виготовлення полі кремнію зображен на рисунку 3.

Трихлорсилан (ТХС) – SiHCl – кремнезмістовний неорганічне з'єднання, з використанням якого виробляється близько 90% світового обсягу полікристалічного кремнію (полікремнію). На основі трихлорсилана одержують моносилан і дихлорсилан, які також використаються у виробництві полікремнію. Трихлорсилан є сировиною в синтезі основного ряду кремніорганического мономеру. Існують і інші області застосування трихлорсилана, як, наприклад, мікроелектроніка, де ТХС використається для эпитаксиального осадження плівок монокрісталического кремнію.

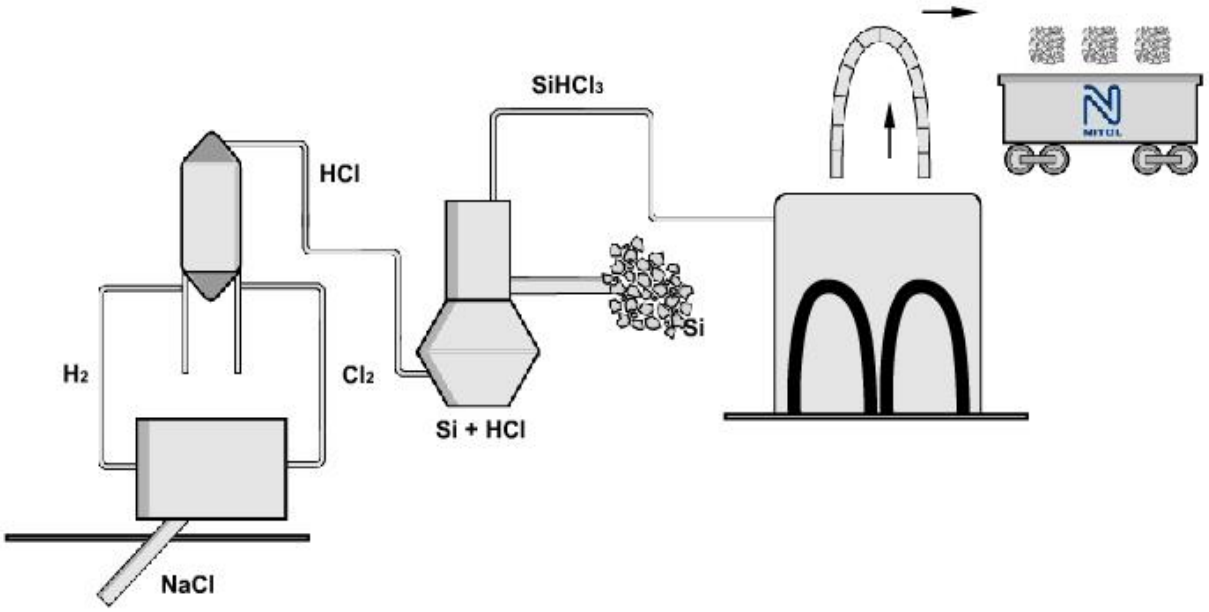


Рисунок 3 – Технологія виробництва полікремнію

Висновки. У статті наведене теоретичне узагальнення й рішення наукового завдання дослідження методів автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Досліджена система автоматизації виробничих процесів створення сонячних батарей класу Tier 2. На основі отриманих результатів досліджень створена програмна реалізація системи автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Розроблені алгоритми дозволяють успішно вирішувати завдання автоматизації виробничих процесів створення сонячних батарей класу Tier 2. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2013. – Вип. 6(113). – С. 255-257.
2. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 4(120). – С. 161-164.
3. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко , О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 2014. – № 1(37). – С. 126-129.
4. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
5. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
7. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
8. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
9. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
10. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.

УДК 004

А. Продкун магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ПІДПРИЄМСТВІ

У статті розроблено програмне забезпечення, яке призначено для системи контролю та управління доступом на підприємстві. Метою розробки є дослідження та програмна реалізація системи контролю та управління доступом на підприємстві. Об'єктом дослідження є процес контролю та управління доступом на підприємстві. Предметом дослідження є методи контролю та управління доступом на підприємстві. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи контролю та управління доступом на підприємстві. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, управління доступом

Постановка проблеми. Сучасні промислові інфраструктури та структури відпочинку, такі як готельні комплекси, офіси, приміщення корпорацій та банків, не обходяться без систем контролю та управління доступом. Завдяки контролю доступу можна запобігти крадіжкам або ушкодження майна, поставити заслін промисловому шпигунству, перекрити доступ на територію або в приміщення зловмисників. Система контролю доступу відповідає вимогам держстандарту: ДСТ 26342-89; ДСТ 50009; ДСТ 12.2.007.0; ДСТ 12.2.004; вимогам ІСО 9000 [1].

Як правило сучасна система контролю та управління побудована з використанням різного виду картрідерів з електронних карточок або таблеток iButton, при цьому пристрої, які організовують зчитування данних з електроних ідентифікаторів називаються картрідерами [1-5].

Нижче перерахуємо можливі варіанти використання картрідерів для забезпечення контролю та управління доступу до приміщень, котрі потребують захисту від фізичного вторгнення зловмисників.

Якщо до об'єкта пред'явлені підвищені вимоги безпеки, то безконтактний картрідер оснащується клавішною панеллю, при наявності якої користувач повинен спочатку ввести картку. У такий спосіб включається кодова клавіатура. Користувач набирає свій особистий код, і двері відкриваються. За допомогою кодової клавіатури вводиться й код тривоги, якщо даному співробітникові загрожує стороння особа [4].

Контролю й управлінню піддаються як двері з картрідерами, так і без них. Заздалегідь задається час відкриття двері, якщо тривалість відкриття більше заданої, подається тривога. Система може бути запрограмована так, щоб двері відкривалися на певний час (наприклад, на період робочого дня) або тільки тоді, коли в певній зоні перебувають особи, що мають право доступу. Кожні двері можна з'єднати з охоронною й протипожежною системами при подвійному контролі доступу [5].

При відстеженні рухів на виході й вході (подвійний контроль доступу) використовуються шлюзи. Через шлюз може пройти одна людина. А так як в шлюзовій кабіні встановлюються картрідери як на вході, так і на виході, то, якщо людина ввійшла в шлюз, їй необхідно вийти, щоб знову пройти у зворотному напрямку. Тобто одна й та людина контролюється подвійно, як на вході, так й на виході [6].

За допомогою картрідерів можна різними способами управляти ліфтом: наприклад, заблокувати певні поверхи, вхід на які буде здійснюватися при наявності права доступу, або викликати ліфт на «секретні» поверхи за допомогою картки, що також обмежить користування ліфтом.

Потік відвідувачів можна регулювати наданням кожному з них певного часу візиту. Інформація з різними даними відвідувача зберігається в системі.

Контроль в'їзду здійснюється автоматично й на відстані, якщо водій тримає картку збоку у вікна машини. Спеціальні картки монтуються на днище автомобіля й ідентифікуються за допомогою закладеної в полотно дороги дротової петлі. Ця петля повинна бути захищена від як випадкових, так і навмисних ушкоджень.

Для автомобілів разом із системою контролю можна використовувати картрідер , що працює на високих частотах (2,4 Ггц). За допомогою картрідера контролюється в'їзд, транспортування товарів і т.д. картку цей картрідер ідентифікує з відстані до 6 метрів. Система контролю доступу корисна й для обліку робочого часу співробітників

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи контролю та управління доступом на підприємстві.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи контролю та управління доступом на підприємстві.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

Огляд існуючих систем контролю та управління доступом на підприємстві.

Дослідження системи контролю та управління доступом на підприємстві.

Програмна реалізація системи контролю та управління доступом на підприємстві.

Об’єктом дослідження є процес контролю та управління доступом на підприємстві.

Предметом дослідження є методи контролю та управління доступом на підприємстві.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Електронні системи контролю доступу забезпечують можливість доступу певних осіб у певні приміщення й обмежують проникнення осіб, що не мають права доступу на ту або іншу територію.

Найпростіші електронні системи доступу – кодонаборні панелі й автономні картрідери карток. Складні системи, що включають у себе комп'ютери, мають більший набір функцій. Їх ПЗ дозволяє одержати різні види звітів про поточні події.

Виконавчі пристрої систем контролю доступу – це різні електрозамки, турнікети, автоматичні двері тощо. Якщо об'єктом доступу є автомобіль, то виконавчі механізми в цьому випадку – шлагбауми й автоматичні приводи воріт.

Всі СКУД будуються на базі ідентифікації чого-небудь. Ідентифікація ґрунтується на самих різних фізичних принципах.

Кодові клавіатури – найпростіші пристрої доступу, що ідентифікують код, набраний користувачем. Сполучені картрідери («карта + код») забезпечують захист у випадку втрати карти, тому що для доступу, крім пред'явлення карти, необхідно набрати код.

Магнітні карти використовуються багатьма системами. Картка проводиться через картрідер, що не завжди зручно. Знаходження карти недалеко від сильних магнітних джерел, а також її забруднення виводять карту з ладу.

Карта Виганда (Wigand) – пластикова картка із запресованими в неї відрізками дроту зі спеціального магнітного сплаву. У кожної карти є індивідуальний код, що зчитується при проведенні її повз магнітну головку. Ці карти зносостійкі, надійно захищені від підробки, але дорожче магнітних.

Безконтактні (Proximity) карти – зчитуються шляхом піднесення до картрідера, поза залежністю від положення стосовно нього. Ідентифікується на відстані 5-15 см, деякі моделі працюють на відстані 1-2 метри. Картка не зношується, не боїться впливів зовнішнього

середовища. На неї можуть наноситися напису й фотографії. Низькочастотна (125 кГц) Proximity-технологія прийнята за промисловий стандарт, оскільки Proximity-карта доступу досить надійна, порівняно недорога, а зчитування її цифрового коду (від 24 до 96 біт) зі швидкістю 2 кбайт відбувається вже на відстані 15 см. По цій же технології виготовляються ідентифікатори у вигляді брелоків, браслетів і ін.

Штрих-код наноситься на паперову або пластикову основу. Картка проводиться через проріз картрідера. Цю карту легко підробити. Якщо штрих-код видн тільки в ІЧ-діапазоні, то таку карту підробити або скопіювати складніше.

Радіоканал використовується для передачі коду картрідеру. Як ідентифікатор виступають радіобрелок або невеликий передавач. Високий ступінь захищеності мають системи з «блукаючим кодом». Мають великий радіус дії. Використовуються на воротах і шлагбаумах.

ІЧ-брелки передають код а ІЧ-діапазоні, добре захищені від перехоплення.

Смарт-карти мають вбудований процесор і контактні площадки для живлення й обміну зі картрідером. Високий ступінь захищеності. Безконтактні смарт-карти володіють крім комірок пам'яті ще й програмним забезпеченням, що перешкоджає розшифровці коду, переданого картрідеру картою, що значно підвищує безпеку. Смарт-карти з великим обсягом пам'яті мають у своєму розпорядженні мікропроцесор, що управляє функціями й розподілом пам'яті.

Електронні ключі – пристрої, що містять код і передають його картрідеру. Нагадують батарейку «таблетка». Зносостійкі, міцні, не бояться впливів зовнішнього середовища.

Біометричні системи розпізнавання засновані на аналізі індивідуальних біометричних характеристик людини (відбитки пальців, тембр голосу, геометрія кисті руки).

Широкий потенціал смарт-карт можливо розкрити, використовуючи їх у зв'язуванні з біометричною технологією. Відразу ж можна вирішити проблему дорожнечі й громіздкості чисто біометричних ідентифікаторів, розмістивши на смарт-карті замість коду, приміром, відбиток пальця. У цьому випадку відпадає необхідність у безпосередньому контакті зі картрідером. Біометричні ідентифікатори в найближчому майбутньому одержать широке поширення, тому що смарт-карти вже зараз недорогі, ціни на біометричні датчики знижуються, а потреба підвищення рівня безпеки назріла давно.

Існує кілька прийнятих конфігурацій підключення систем контролю доступу. Звичайно сигнали до дверей контрольованого об'єкта направляються від однієї панелі; картрідера із дверима об'єднані через протокол Виганда, пульт же може з'єднуватися з базовим комп'ютером по RS-485-інтерфейсу. Інші датчики й кнопки з'єднуються з панеллю прямо. При цьому кабельна обв'язка становить значиму частину вартості установки всієї системи. Заглядаючи в перспективу розвитку конфігурацій підключення, можна відзначити, що в майбутньому кожна система буде складатися із дверних груп, керованих окремими контролерами. Вони, у свою чергу, будуть зв'язані один з одним через RS-485 і через TCP/IP – з ядром системи.

Опис електронних ключів і картридерів

Електронні замки представляються ще занадто новим віянням, щоб бути повністю зрозумілими споживачеві. Розглянемо пристрій електронного замка, щоб вникнути в те, як він функціонує й виявити його переваги й недоліки.

Електронний замок складається із трьох основних частин: привода, блоку керування й ключевини (блоку ідентифікації). Тут варто відзначити, що в добротного замка ці частини повинні існувати окремо, вони не повинні інтегруватися друг у друга. Існує кілька видів замків по типу привода, що управляє засувами: комбінований електромеханічний замок (звичайний замок з електромагнітним блокуванням); комбінований електромеханічний замок, оснащений моторним приводом; електромагнітна засувка; моторний замок (у випадку грамотної реалізації дуже ефективно протистоїть злому); моторний замок із блокуванням засувів у відповідній частині (найбільш надійні, розкрити при добре реалізованих інших частинах замка попросту неможливо).

Тепер поговоримо про блоки керування. Вони служать для ідентифікації ключа й керування приводом замка. Якщо блок керування й кнопку відкриття двері можна встановити на значній відстані від інших частин замка (наприклад, взагалі не на двері); якщо він має діючий захист від перепадів напруги й працює від резервного джерела живлення, якщо всі провода, що йдуть від його до мотора, мають однаковий колір і товщину і якщо він спроектований таким чином, що має дублюючі системи й при ушкодженні мікропроцесора не запускає двигун, то перед нами – просто ідеальний блок керування.

Переходимо до розгляду «ключевин», або блоків ідентифікації. Їх існує безліч, важливо зробити правильний вибір (втім, як і з іншими складовими замка). Тут головне не перестаратися. Тобто в жодному разі не слід установлювати на двері квартири дактилоскопічні панелі або картрідери карт якого-небудь виду – відкритий тип ідентифікатора сильно залучає до себе увагу деяких особистостей (точніше не до себе, а до того, що може перебувати за дверима з таким ідентифікатором). Отже, ідентифікатори підрозділяються на контактні (звичайний або складальний резісторный ключ, карта з електронним кодом, кодова електронна «таблетка», смарт-карта), псевдобезконтактні (кодова клавіатура, магнітний ключ, магнітна карта, дактилоскопічна панель) і безконтактні (найкраще вибрати саме їх – у цьому випадку відкривається набагато менше можливість для злому).

Моторні замки – технічні пристрої, у яких керування запірним механізмом здійснюється за допомогою електродвигуна. Їхня висока ціна виправдана надійністю пристрою й технічною складністю. Зараз попитом користуються замки компаній ABLOY (Фінляндія), effeff (Німеччина); із числа новинок необхідно відзначити замок e-VOLUTION, що випускається фірмою CISA (Італія). Особливості даного замка: кілька режимів роботи, простота зі зміною, сигнал стану замка, наявність у комплекті акумулятора. Призначено цю модель для установки в потужні металеві двері.

У замках соленоїдного типу керування потужними запірними ригелями здійснюється за допомогою електромагнітних котушок. Від набору функціональних можливостей залежить ціна на ці вироби. На нашому ринку представлені замки фірм TECNAX (Швейцарія), effeff, YALE CORNI (Італія), PONGEE (Тайвань). Замки соленоїдного типу встановлюються в стандартні, алюмінієві або пластикові двері. Датчик, вбудований у замок даного типу, контролює двері й передають сигнал про її стан на керуючий контролер.

Електромагнітні замки вимагають постійного безперебійного електроживлення. Серед них є й врізні замки, використання яких зменшує площу дверного прорізу й робить екстер'єр дверей більше естетичним.

Електромеханічні замки «взводного» типу відрізняються тим, що тут не потрібна постійна подача електроенергії. Ці замки значно дешевше моторних і соленоїдних. Енергія, використовувана для роботи «взводних» замків, береться від пружини, зведеної при закритих дверях і разблокуємої при подачі керуючого електричного сигналу. При відсутності електроенергії двері залишаються закритими й можуть бути відкриті механічним ключем. Накладні й урізні замки «взводного» типу виробляються компаніями CISA і ISEO (Італія); менш дорогі накладні замки представлені фірмами YUS, MING YANG (Тайвань) і COMMAX (Корея).

Електромеханічні засувки – варіант найбільш простого рішення завдання дистанційного відкривання двері з механічним замком. Лідером виробництва засувок є компанія effeff, а серед інших виробників цих виробів можна відзначити фірми NUOVA FEB (Італія), Openers&Closers (Іспанія), COMMAX (Корея) і ін.

Вибираючи замок, необхідно знати, що у вуличних умовах краще використовувати електромеханічні й електромагнітні замки (при цьому робочу частину потрібно захистити від влучення опадів); електромеханічні засувки, що відрізняються здатністю довгострокового підключення до джерела живлення, установлюються на аварійних виходах і шлюзових проходах; до хитних дверей підійдуть замок, фиксуємий у середньому стані (тобто, або спеціальний замок для хитних дверей, або замок з датчиком положення двері).

Електронний замок із ключами iButton

Замок спроектовано для індивідуальних використань і має гранично просту конструкцію. На вхідних дверях зовні розташовується тільки панелька для iButton і светлодіод відкривання дверей. Відкривання дверей зсередини здійснюється за допомогою кнопки.

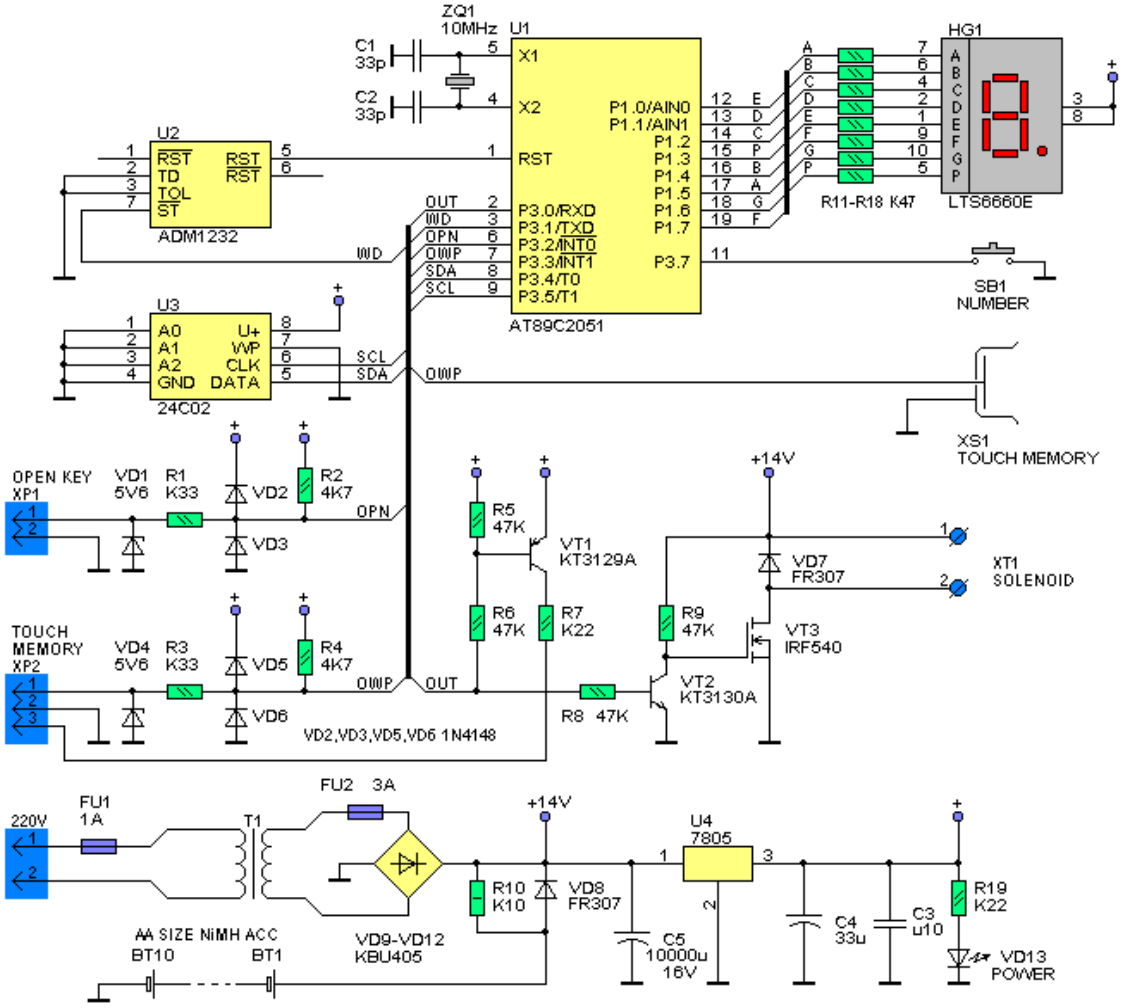


Рисунок 1 – Принципова схема замка

Як виконавчий механізм використовується стандартна засувка з електромагнітом, що розрахований на напругу 12В. Коди ключів зберігаються в енергонезалежній пам'яті й можуть стиратися й додаватися користувачем. Для захисту від несанкціонованого перепрограмування замка використовується майстер-ключ. Усього до пам’яті можна записати 9 ключів. Ця кількість продиктована можливостями 1-розрядного індикатора номера програмувального ключа. Якщо задіяти ще й букви, можна збільшити сумарну кількість ключів до 15. Це робиться шляхом заміни значення константи MAXK у програмі. Таким же способом можна й зменшити максимальну кількість ключів.

Принципова схема замка показана на рисунку 1. Основою конструкції є мікроконтролер U1 типу AT89C2051 фірми Atmel. До порту P1 підключений 7-сегментний індикатор, що використовується при програмуванні ключів. Для цих же цілей призначена й кнопка SB1, підключена до порту P3.7. Зберігання серійних номерів ключів здійснюється в мікросхемі EEPROM U3 типи 24C02, підключеної до портів P3.4 (SDA) і P3.5 (SCL). Зовнішня панелька для iButton підключається до порту P3.3 через роз’єм XP2 і елементи захисту VD4, R3, VD5 і VD6. резистор, що підтягує, R4 обраний відповідно до специфікації однопровідної шини. Паралельно зовнішній панельці підключена ще й внутрішня панелька

XS1, що використовується для програмування ключів. Кнопка відкривання двері підключена до порту P3.2 через роз'єм XP1 і такі ж елементи захисту, як і для iButton. Виконавчим пристроєм замка є електромагніт, підключений через термінал XT1. Електомагнітом управляє ключ VT3, у якості якого використовується потужний Моп-транзистор типу IRF540. Діод VD7 захищає від викидів самоіндукції. Ключем VT3 управляє транзистор VT2, що інвертує сигнал, який надходить із порту P3.0 і забезпечує керуючі рівні 0/12В на затворі VT3. Інверсія потрібна для того, щоб виконавчий пристрій не спрацьовувало під час скидання мікроконтролера, коли на порту присутній рівень логічної одиниці. 12-вольтові керуючі рівні дозволили застосувати звичайний Моп-транзистор замість більш дефіцитного низькопорогового (logick level). Для індикації відкриття замка використовується світлодіод, який управляється тим же портом, що й електромагніт, але через транзисторний ключ VT1. Світлодіод підключається через той же роз'єм, що й iButton. Оскільки пристрій повинен працювати цілодобово без обслуговування, для підвищення надійності встановлений супервізор U2 типу ADM1232. Він має вбудований сторожовий таймер і монітор живлення. На порту P3.1 мікроконтролер формує періодичні імпульси для скидання сторожового таймера.

Живлення пристрою здійснюється від вбудованого блока живлення, що містить трансформатор T1, випрямний міст VD 9-VD12 і інтегральний стабілізатор U4. Як резервне джерело живлення використовується батарея BT 1-BT10 з 10-ти NiMH-акумуляторів типорозміру AA ємністю 800мА/Ч. При живленні пристрою від мережі батарея акумуляторів заряджається через резистор R10 струмом приблизно 20мА, що становить 0.025С. Режим зарядки малим струмом називають краплинним (trickle charge). У такому режимі акумулятори можуть перебувати як завгодно довго, контроль кінця процесу зарядки не потрібен. Коли акумулятори виявляються повністю зарядженими, енергія, що забирається ними від джерела живлення, перетворюється в тепло. Але оскільки струм зарядки дуже маленький, виділюване тепло розсіюється в навколишній простір без скільки-небудь помітного збільшення температури акумуляторів.

Конструктивно пристрій виконаний у корпусі розміром 150x100x60мм. Більшість елементів, включаючи трансформатор живлення, змонтовано на друкованій платі. Акумулятори розміщаються в стандартних пластмасових тримачах, які закріплені усередині корпуса поруч із платою. У принципі, можна використовувати й інші типи акумуляторів, наприклад 12-вольтову кислотну необслуговувану батарею, що застосовується в охоронних системах. Для підключення виконавчого пристрою на платі є термінали типу ТВ-2, всі інші зовнішні ланцюги підключаються через малогабаритні роз'єми із кроком контактів 2.54мм. Роз'єми розташовані на друкованій платі й зовні корпуса недоступні. Провода виходять із корпуса через гумові ущільнювачі. Оскільки індикатор HG1, кнопка SB1 і панелька для iButton XS1 використовуються тільки під час програмування, вони розміщені на платі всередині пристрою. Це спрощує конструкцію корпуса й робить його більш захищеним від зовнішніх впливів. На бічній панелі корпуса розміщений тільки світлодіод індикації включення VD13.

При відкриванні дверей на електромагніт подається імпульс тривалістю 3 секунди. Логіка роботи пристрою така, що якщо кнопку відкривання двері втримувати, то весь цей час електромагніт буде під напругою й, відповідно, двері буде відкрито.

Замок може мати максимум 9 ключів, плюс один майстер-ключ. Коди ключів заносяться в енергонезалежну пам'ять під номерами від 1 до 9. Код майстер-ключа занесений у ПЗП мікроконтролера й не може бути змінений. Програмування нових ключів або стирання старих може бути зроблено тільки при наявності майстер-ключа. Як і інші ключі, майстер-ключ може використовуватися для відкривання замка.

Для програмування нового ключа потрібно проробити наступні дії:

1. Нажати кнопку програмування.
2. На індикаторі з'явиться буква «P», що означає вхід у режим програмування.
3. Торкнутися майстер-ключем панельки.

4. На індикаторі з'явиться цифра «1», що позначає номер програмувального ключа.

5. Кнопкою вибрати потрібний номер.

6. Торкнутися будь-яким ключем панельки.

7. Цифра на індикаторі почне мигати, що говорить про готовність до програмування.

8. Торкнутися панельки тим ключем, код якого потрібно занести до пам'яті.

9. У випадку успішного програмування цифра на індикаторі перестане мигати й почне горіти постійно.

10. Для виходів з режиму програмування потрібно просто почекати 5 секунд, після чого індикатор згасне.

Розробка структурної схеми

Для перевірки коректності реалізації даної задачі було виконано багато розрахунків та експериментальних матеріалів. Цьому питанню приділялась особлива увага тому, що помилка при розрахунку привела б до ряду негативних наслідків. Відлагодження та перевірка, що підтверджує вірність програмних рішень відбувалась за декількаами етапами:

математична перевірка окремих модулів;

математична перевірка всієї системи (з допомогою математичної логіки будується логічна схема всієї системи);

практична перевірка підпрограм (перевіряється процедурна частина кожної підпрограми окремо);

практична перевірка всієї системи у дії (перевіряється ситема в цілому за допомогою вводу різних даних у програму, потім на виході з програми перевіряємо отриману інформацію з очікуваною).

Для підтвердження правильності розрахунку програми були використані експериментальні дані різних форматів, були проведені консультації з даного питання зі спеціалістами.

Простота мови проектування та маніпулювання даними, зручність спілкування користувача з системою до мінімума вивчення цієї програми. Користувач програми – це людина, яка повинна володіти азами програмування. При написанні програми я намагалася, щоб програма відповідала наступним параметрам:

Швидкодія. Програма працює постійно з великою кількістю запитів від катрридерів.

Захист. Захищений канал передачі пакетів інформації.

Система, що написана може встановлюватись на будь-якому персональному комп'ютері – використовувати відносно швидкі алгоритми захисту зв'язку.

Можливість зручно і швидко формувати приклади і теорію для користувача.

Можливість звертання до системних ресурсів. Користувача системи цікавить її інформаційний та сенсовий зміст. Подробиці організації фізичного зберігання даних його не цікавлять.

Перш за все перед розробкою системи слід одержати уявлення на слідуючи моменти:

на які частини можна розбити систему;

одержати уявлення про кожну частину (фрагмент);

які процеси передачі і обробки даних знаходяться в кожному фрагменті;

на якому обладнанні планується реалізувати систему;

технологія функціюваня системи;

чи необхідна адаптація і настройка системи при змінах деяких умов.

Для розробки програми були попередньо розроблені структурна схема роботи системи, структурна схема взаємодії з картрідерами, функціональна схема роботи системи, діаграма процесів, а також блок-схеми алгоритму програми, розглянемо їх детально.

Розглянемо структурну схему роботи системи, що зображена на рисунку 2. У схемі можна чітко побачити два вхідних потоки даних, а саме дані, що надходять із периферії (дані про стан дверних прорізів) і дані оператора.

Розроблена сучасна система контролю й управління доступом до примішень підприємства (СКУД) базується на апаратурі фірми AS-Scan. Система розподілена на

мережні вузли, які з’єднуються з базовою станцією, що називається «сервер керування й зв'язку» і із системами архівації, системами контролю доступу.

Рисунок 2 – Структурна схема роботи системи

У розробленій системі застосовувалися мережні вузли засновані на зчитували магнітних карт серії Camp Tek MR, застосовувалися наступні моделі: 834 RS/KB, 834 USB, 836 USB, 836 RS/KB (рисунок 3).

Рисунок 3 – Зчитувач магнітних карт Camp Tek MR серії 843 і 836

Застосування встаткування фірми AS-Scan дозволяє встановлювати сервер контролю й керування на персональних комп'ютерах малої потужності. Так як встаткування бере на себе частину ресурсномістких операцій, прискорюючи процес обробки сигналів з перифірійного встаткування. При застосуванні даних пристроїв автор диплома враховував ці особливості.

Розроблена програма розбита на модульну структуру дозволяючи швидко змінювати необхідні параметри програми без корінної зміни структури.

Розглянемо основні модулі сервера контролю й керування, а також підсистеми архівації даних і контролю доступу.

Сервер контролю й керування:

1. Інтерфейс користувача – основою сервера контролю й керування є розроблене програмне забезпечення яке видається операторові сервера у вигляді інтерфейсу в якому відображаються всі операції, які відбуваються.

2. Модуль взаємодії з операційною системою – модуль контролю системних повідомлень від операційної системи. Так як щомісяця приходять все нові відновлення операційної системи, необхідно убезпечити систему від можливих системних збоїв, помилок ОС, вірусних атак. Цей модуль дозволяє аналізувати зміни в роботі ОС і провести детальний аналіз при виникненні проблем.

3. Модуль аналізу даних – модуль аналізу вхідних даних зі зчитувачів магнітних карт. Через можливе значно віддалення зчитувачів друг від друга, а також можливості злому системи необхідно убезпечити сервер аналізом переданих даних.

4. Модуль перевірки лінії зв'язку з об'єктами – через значно віддалення також необхідно постійно перевіряти зв'язок між сервером і зчитувачами магнітних карт і при необхідності робити відповідні контрольні дії.

5. Модуль захисту ПЗ – модуль перевірки роботи програми. Для мінімізації й виключення можливості злому сервера був написаний модуль контролю роботи програми який проводить перевірку записів у реєстрі, перевірку роботи розробленого програмного забезпечення з виділеною пам'яттю, операції читання запису на диск.

6. Модуль виведення статистики роботи – ведення статистики доступу до приміщень, з точним указанням дати й часу доступу. Для чіткого розуміння подій, які відбуваються в підприємстві необхідно мати доступ до зроблених дій.

7. Модуль кодування – модуль настроювання параметрів кодування. Тонке настроювання методу кодування ДСТУ 28147:2009 (довгі ключа, особливості предачі й.т.їнше.).

8. Модуль налагодження ПЗ – модуль загального настроювання розробленої програми.

Система архівації даних:

1. База даних контрольних підсистем – підсистема зберігання резервних копій, статистики роботи й т.д.

2. Таблиці підприємницької справи – таблиці ведення обліку роботи підприємства.

3. Таблиці доступу – таблиці пропускної системи доступу до приміщень підприємства.

4. Таблиці надзвичайних випадків – таблиці ведення статистики надзвичайних ситуацій для аналізу дій, зроблених персоналом.

Система контролю доступу:

1. Охорона правопорядку (система безпеки підприємства) – зв'язок з охороною підприємства при надзвичайних подіях.

2. Автоматизована телефонна система підприємства – організація зв'язку по підприємства, довідник підприємства.

3. Протипожежний контроль – екстрений виклик пожежних і служби газу (протипожежна й газова тривожна кнопка).

4. Інші служби – служби паркування автомобілів, доставки товару.

Коли людина проводить магнітною карткою через щілину картрідера відбувається зчитування 2 магнітних смужок – вихідна інформація з визначаемої карти.

Далі картрідер робить апаратне кодування даних з магнітної карти алгоритмом ДСТУ 28147:2009 і передачу інформації на сервер контролю й керування в зашифрованому виді.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контролю та управління доступом на підприємстві. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем

контролю та управління доступом на підприємстві. Досліджена система контролю та управління доступом на підприємстві. На основі отриманих результатів досліджень створена програмна реалізація системи контролю та управління доступом на підприємстві. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки. Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

Список літератури

1. Коваленко А.В. Технология тестирования DOM XSS уязвимости / А.В. Коваленко, А.С. Коваленко, А.А. Смирнов, С.А. Смирнов // Scientific & practical cyber security journal (SPCSJ) Volume 1. Issue 1. P. 38-45 Georgia. Tbilisi. Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667. URL: https://journal.scsa.ge/wp-content/uploads/2018/12/8-dom-xss-testing-technology-vulnerabilities.pdf
2. Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
3. Коваленко А.В. Разработка метода управления рисками разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Інформаційні технології: проблеми та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: Видавець Рожко С.Г., 2017. – 447 с.
4. Коваленко А.В. Комплекс математических моделей технологии тестирования web-приложений / А.В. Коваленко, А.А. Смирнов // Інформаційні технології: сучасний стан та перспективи: монографія / За загальною редакцією В.С. Пономаренка. – Х.: ТОВ «ДІСА ПЛЮС», 2018. – 461 с.
5. Коваленко А.В. Задачи распознавания ситуаций в erp системах / А.В. Коваленко, А.А. Смирнов, А.С. Коваленко // Збірник наукових праць "Системи обробки інформації". – Випуск 4(120). – Х.: ХУПС – 2014. – С. 161-164.
6. Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 5(142). – Х.: ХУПС – 2016. – С. 153-157.
7. Коваленко А.В. Проблемы анализа и оценки рисков информационной деятельности / А.В. Коваленко, А.А. Смирнов, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць "Системи обробки інформації". – Випуск 3(140). – Х.: ХУПС – 2016. – С. 40-42.
8. Коваленко А.В. Метод качественного анализа рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов, Н.Н. Якименко, А.П. Доренский // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 2(23). – Харків: ХУПС. – 2016. – С. 150-158.
9. Коваленко А.В. Метод количественной оценки рисков разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. – 2016. – С. 128-133.
10. Коваленко А.В. Использование псевдобулевых методов бивалентного программирования для управления рисками разработки программного обеспечения / А.В. Коваленко, А.А. Смирнов // Системи управління, навігації та зв'язку. – Випуск 1 (37). – Полтава: ПолтНТУ. – 2016. – С. 98-103.

УДК 004

О. Піскова, магістр гр. КН-120МЗ,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ IP-ТЕЛЕФОНІЇ З ЗАБЕЗПЕЧЕННЯМ КОНФІДЕНЦІЙНОСТ

У статті розроблено програмне забезпечення, яке призначено для системи IP-телефонії з забезпеченням конфіденційності. Метою розробки є дослідження та програмна реалізація системи IP-телефонії з забезпеченням конфіденційності. Об'єктом дослідження є процес IP-телефонії з забезпеченням конфіденційності. Предметом дослідження є методи IP-телефонії з забезпеченням конфіденційності. Методи дослідження базуються на методах теорії передачі мультимедійних даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи IP-телефонії з забезпеченням конфіденційності. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерні науки, IP-телефонія

Постановка проблеми. З початком ери комп'ютеризації стали бурхливо розвиватися системи передачі даних (СПД) на базі IP [1-3]. Організувавши високошвидкісний доступ до СПД по наземних каналах або з використанням доступної бездротової технології, оператор може надати клієнтові й послуги телефонного зв'язку – досить лише підключити телефонні апарати або персональну автоматичну телефону мережу (ПАТМ) клієнта через мережу IP до платформи VoIP оператора. Аналогічні підходи застосовні й при побудові корпоративної мережі зв'язку (КМЗ) [5]. Шлях побудови корпоративної мережі зв'язку на базі VoIP припускає відмову від традиційної комутації (тобто від комутації каналів) за допомогою ПАТМ і впровадження IP-PBX (IP-ПАТМ), які є новим поколінням систем зв'язку, орієнтованим на VoIP [1-10]. Замість IP-ПАТМ у КМЗ для комутації трафіку VoIP можна скористатися послугами операторів зв'язку Hosted IP-PBX (віртуальна IP-ПАТМ) або IP-Centrex (оренда комутаційної ємності). Більша частина середніх і великих підприємств має офіси в декількох районах і містах. Організація зв'язку із центральним офісом коштує чималих грошей. Тим часом діяльність всіх перерахованих компаній і підприємств не можна уявити без доступу співробітників до мережі Internet і/або корпоративної обчислювальної мережі. Однак однією з умов придатності приміщення для розміщення філії є найчастіше наявність мережі передачі даних і телефонної мережі. Тільки от чи не так уже необхідно сьогодні окреме підключення до ТфОП? Або, скажемо інакше, чи багато потрібно далеко не дешевих телефонних ліній і чи потрібна окрема ПАТМ, яку доводиться обслуговувати на місці? Використання у філіях електронної пошти, корпоративного електронного документообігу й внутрішніх ресурсів Web (Intranet), довідкових систем і баз даних, систем обліку товарно-фінансових потоків і керування ресурсами підприємства вимагають організації надійного доступу до корпоративної мережі по виділених каналах або через мережу передачі даних за допомогою VPN. Але якщо такий доступ реалізований, то ці ж канали придатні й для телефонного зв'язку – досить реалізувати підтримку технологій VoIP. Завдяки шлюзам VoIP сьогодні можна створювати налагоджену КМЗ з можливістю доступу до будь-якого співробітника без виходу до ТфОП. Для цього абоненти філій підключаються до ПАТМ центрального офісу (яка, як правило, уже є) за допомогою абонентських місць побудованих на основі шлюзів VoIP [9-10].

Основна перевага використання технології VoIP у корпоративній мережі зв'язку – це впровадження з метою економії на капітальних і операційних витратах, пов'язаних з побудовою (на підготовці приміщень і трас, покупці встаткування і його монтажі, будівництві ліній зв'язку, придбанні портової й номерної ємності операторів і т.і.) і експлуатацією (на зарплаті власному сервісному персоналу, сервісних послугах сторонніх організацій, оренді портової й номерної ємності, витратах на трафік і т.і.).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи IP-телефонії з забезпеченням конфіденційност

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи IP-телефонії з забезпеченням конфіденційності.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем IP-телефонії з забезпеченням конфіденційності.
– Дослідження системи IP-телефонії з забезпеченням конфіденційності.
– Програмна реалізація системи IP-телефонії з забезпеченням конфіденційності.

Об'єктом дослідження є процес IP-телефонії з забезпеченням конфіденційності.

Предметом дослідження є методи IP-телефонії з забезпеченням конфіденційності.

Методи дослідження базуються на методах теорії передачі мультимедійних даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Опис функцій, що автоматизуються

Структура програмного забезпечення в першу чергу визначається тими функціями, які повинна виконувати програма. В даній роботі автоматизується система керування корпорацією, за рахунок впровадження IP-зв'язку. Для корпоративної мережі зв'язку можливо виділити наступні функції:

реалізація IP-зв'язку між підрозділами корпорації;
реалізація селективного зв'язку між підрозділами та структурами;
реалізація режиму конференції;
при наявності відповідного устаткування реалізація режиму відеоконференцій;
реалізація можливості створення бази корпоративних номерів;
можливість коригування інформації в базі корпоративних номерів.

Розроблюване програмне забезпечення повинне виконувати всі вказані вище функції, але в різному об'ємі. Головне призначення системи організації зв'язку в корпорації, в даному випадку – поліпшити оперативність прийняття рішень, підвищити продуктивність праці, знизити кількість обчислювальних помилок за допомогою автоматизації процесу обробки інформації, сприяти ефективному і безпечному збереженню і доступу до інформації.

Метою корпоративної мережі зв'язку є створення єдиної мережі, що дозволяє ефективно здійснювати керування за рахунок застосування IP-телефонії.

Опис інформаційного забезпечення системи

Під IP-телефонією розуміється технологія, що дозволяє використовувати IP-мережу як засіб організації й ведення міжнародних і міжміських телефонних розмов і передачі факсів у режимі реального часу. Зараз в IP-телефонії існує два основних способи передачі голосових пакетів по IP-мережі: через публічний Інтернет і використовуючи виділені канали. У першому випадку смуга пропущення прямо залежить від завантаженості IP-мережі пакетами, що містять дані, голос, тощо, а значить затримки при проходженні пакетів можуть бути самими різними. При використанні виділених каналів винятково для голосових пакетів можна гарантувати фіксовану (або майже фіксовану) швидкість передачі. Виходячи зі схеми, реалізованої провайдером IP-телефонії, принцип роботи мережі IP-телефонії наступний (розглянутий найпоширеніший випадок – дзвінок з телефону на телефон або з факсимільного апарата на факсимільний апарат).

Необхідно зробити дзвінок на міський телефонний номер телефонного шлюзу, користуючись будь-яким телефонним апаратом або таксофоном, що переходить у тоновий

режим. Дзвінок по цифрових або аналогових лініях приходить на телефонний шлюз. Шлюз звертається до сервера голосових повідомлень для видачі голосових підказок і повідомлення залишку на рахунку. Після ідентифікації й автентифікації, пропонується ввести код країни, міста й телефонний номер викликуваного абонента. Все спілкування з телефонним шлюзом відбувається в голосовому каналі. Далі телефонний шлюз встановлює зв'язок з віддаленим телефонним шлюзом по виділеному каналі. Віддалений шлюз робить таке ж з'єднання з викликуваним абонентом, але у зворотному порядку. Після установки з'єднання шлюзи починають обмін IP-Пакетами, у які впакований голос.

Апаратне забезпечення. У якості інтерфейсної плати ISDN використовуються плати для роботи з голосом, які з'єднані послідовно з інтерфейсною платою шиною SCBus. При використанні переривання відлуння одна плата підтримує до 8 ліній, а при використанні знищення ефекту відлуння до 4-х ліній. Зовні шлюз являє собою комп'ютер у промисловому виконанні, що монтується в 19-дюймову стійку. В одній мережі зі шлюзом розташовується голосовий сервер, що відповідає за голосові підказки й повідомлення про залишок на рахунку. Являє собою звичайний IBM-сумісний комп'ютер із ПЗ.

Програмне забезпечення. Для кодування використовується стандарт GSM. В IP-мережі голос займає 13,5 Кбіт/сек по протоколу UDP, що також значно зменшує затримки при передачі пакетів. При передачі факсу використовується та ж швидкість, причому використовується протокол гарантованої доставки TCP/IP. Таким чином, при використанні 30 ліній, потрібний канал із шириною пропущення не більше 512 Кбіт/сек, з яких тільки 405 Кбіт/сек будуть задіяні для IP-телефонії. Іншу ширину каналу можна використовувати під Інтернет, причому ніяк не погіршуючи якість передачі голосу. Шлюз підключається до мережі Ethernet, яка підключена до маршрутизатора. Максимально припустима затримка в каналі – 400 мс. При більших затримках недоцільне застосування функцій, що знищують ефект відлуння, тому на програмному рівні відлуння подавлення використовує буферізацію (за замовчуванням в 80 мс).

Рівні архітектури IP-телефонії

Архітектура технології VoIP може бути спрощено представлена у вигляді двох площин. Нижня площина – це базова мережа з маршрутизацією пакетів IP, верхня площина – це відкрита архітектура керування обслуговуванням викликів.

Нижня площина являє собою комбінацію відомих протоколів Інтернет: це – RTP, що функціонує поверх протоколу UDP, розташованого, у свою чергу, у стеці протоколів TCP/IP над протоколом IP. Таким чином, ієрархія RTP/UDP/IP являє собою свого роду транспортний механізм для мовного трафіку. У мережах з маршрутизацією пакетів IP для передачі даних завжди передбачаються механізми повторної передачі пакетів у випадку їхньої втрати. Рекомендації ITU-т допускають затримки в одному напрямку не перевищуючі 150 мс.

Розглянемо протокол TCP/IP. Transmission Control Protocol/Internet Protocol – це промисловий стандарт стеку протоколів, розроблений для глобальних мереж:

це найбільш завершений стандартний і водночас популярний стек мережних протоколів, що має багаторічну історію.

майже усі великі мережі передають основну частину свого трафіка за допомогою протоколу TCP/IP.

це метод одержання доступу до мережі Internet.

стек TCP/IP є основою для створення intranet-корпоративної мережі, що використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet.

усі сучасні операційні системи підтримують стек TCP/IP.

це гнучка технологія для з'єднання різнорідних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів.

це масштабована міжплатформенна середа для додатків клієнт-сервер.

Протоколи TCP/IP поділяються на 4 рівні.

Найнижчий IV рівень відповідає фізичному і канальному рівням моделі OSI. Цей рівень у протоколах TCP/IP підтримує всі популярні стандарти фізичного і канального рівня:

для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальних мереж – протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж із комутацією пакетів X. 25, frame relay. Звичайно тільки з'являється нова технологія локальних або глобальних мереж вона швидко включається в стек TCP/IP за рахунок розробки відповідного стандарту, що визначає метод інкапсуляції пакетів IP у її кадри.

Наступний III рівень – це рівень міжмережної взаємодії, що займається передачею пакетів із використанням різноманітних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку тощо. У якості основного протоколу мережного рівня використовується протокол IP.

Наступний II рівень називається основним. На цьому рівні функціонує протокол керування передачею TCP і протокол дейтаграм користувача UDP. Протокол TCP забезпечує надійну передачу повідомлень між віддаленими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним засобом, як і IP, і виконує тільки функції сполучного ланка між мережним протоколом і численними прикладними процесами.

Верхній I рівень називається прикладним. За довгі роки використання в мережах різноманітних країн і організацій стек TCP/IP накопичив велику кількість протоколів і сервісів прикладного рівня. До них відносять такі широко використовувані протоколи, як протокол копіювання файлів FTP, протокол емуляції термінала telnet, поштовий протокол SMTP, використовуваний в електронній пошті мережі Internet, гіпертекстові сервіси доступу до віддаленої інформації, такі як WWW і багато інших.

Основу транспортних засобів стека протоколів TCP/IP складає протокол міжмережної взаємодії – Internet Protocol (IP). Основні функцій протоколу IP:

перенос між мережами різноманітних типів адресної інформації в уніфікованій формі,

складання і розбирання пакетів при передачі їх між мережами з різноманітним максимальним значенням довжини пакета.

Пакет IP складається з заголовка і поля даних. Максимальна довжина поля даних пакета обмежена розрядністю поля, що визначає цей розмір, і складає 65535 байтів, проте при передачі по мережах різноманітного типу довжина пакета вибирається з урахуванням максимальної довжини пакета протоколу нижнього рівня, що несе IP-пакети. Якщо це кадри Ethernet, то вибираються пакети з максимальною довжиною в 1500 байтів, що поміщаються в поле даних кадру.

Задачею протоколу транспортного рівня UDP є передача даних між прикладними процесами без гарантій доставки, тому його пакети можуть бути загублені, продубльовані або прийти не в тому порядку, у якому відправлені.

У стеку протоколів TCP/IP протокол TCP працює так само, як і протокол UDP, на транспортному рівні. Він забезпечує надійне транспортування даних між прикладними процесами шляхом установлення логічного з'єднання.

У протоколі TCP для зв'язку з прикладними процесами використовуються порти. Номера портам присвоюються. Є стандартні, зарезервовані номера (наприклад, номер 21 закріплений за сервісом FTP, 23 – за telnet), а менше відомі додатки користуються довільно обраними локальними номерами.

Перейдемо до верхньої площини керування обслуговуванням запитів зв'язку. Керування обслуговуванням виклику передбачає прийняття рішень про те, куди виклик повинен бути спрямований, і яким образом повинне бути встановлене з'єднання між абонентами. Інструмент такого керування – телефонні системи сигналізації, починаючи із систем, підтримуваних декадно-кроковими АТС і функцій, що передбачають об'єднання, маршрутизації й функцій створення розмовного каналу, що комутирується, у тих самих декадно-крокових шукачах. Далі принципи сигналізації еволюціонували до систем сигналізації по виділених сигнальних каналах, до багаточастотної сигналізації, до протоколів загальканальної сигналізації [6, 7] і до передачі функцій маршрутизації у відповідні вузли обробки послуг мережі [8].

У мережах з комутацією пакетів ситуація більше складна. Мережа з маршрутизацією пакетів IP принципово підтримує одночасно цілий ряд різноманітних протоколів маршрутизації. Такими протоколами на сьогодні є: RIP, IGRP, EIGRP, IS-IS, OSPF, BGP і ін. Точно так само й для IP-телефонії розроблений цілий ряд протоколів

Найпоширенішим є протокол H.323, зокрема, тому, що він став застосовуватися раніше інших протоколів. Інший протокол площини керування обслуговуванням виклику - SIP – орієнтований на те, щоб зробити кінцеві пристрої й шлюзи більш інтелектуальними й підтримувати додаткові послуги для користувачів. Ще один протокол – SGCP – розроблявся, для того, щоб зменшити вартість шлюзів за рахунок реалізації функцій інтелектуальної обробки виклику в централізованому встаткуванні. Протокол IPDC дуже схожий на SGCP, але має більше, ніж SGCP, механізмів експлуатаційного керування (OAM&P). Існує більш функціональний, ніж MGCP, протокол MEGACO. Його адаптований до H.323 варіант в рекомендації H.248.

Щоб стало зрозуміло, чим конкретно відрізняються один від одного перераховані в попередньому параграфі протоколи, розглянемо архітектуру мереж, побудованих на базі цих протоколів, і процедури встановлення й завершення з'єднання з їхнім використанням.

Мережі на базі протоколів H.323 орієнтовані на інтеграцію з телефонними мережами й можуть розглядатися як мережі ISDN, накладені на мережі передачі даних. Рекомендація H.323 передбачає досить складний набір протоколів, що призначений не просто для передачі мовної інформації з IP-мереж з комутацією пакетів. Його мета – забезпечити роботу мультимедійних додатків у мережах з негарантованою якістю обслуговування. Мовний трафік – це тільки один з додатків H.323, поряд з відеоінформацією й даними. Варіант побудови мереж IP-телефонії в рекомендації H.323, добре підходить тим операторам місцевих телефонних мереж, які зацікавлені у використанні мережі з комутацією пакетів (IP-мережі) для надання послуг міжміського й міжнародного зв'язку.

Основними пристроями мережі є: термінал (Terminal), шлюз (Gateway), воротар (Gatekeeper) і пристрій керування конференціями (MCU).

У сценарії встановлення з'єднання між двома користувачами передбачається, що кінцеві користувачі вже знають IP-адреси один одного. У звичайному випадку етапів буває більше, оскільки у встановленні з'єднання беруть участь gatekeeper і й шлюзи.

Розглянемо крок за кроком цей спрощений сценарій.

1. Кінцевий пристрій користувача А надсилає запит з'єднання – повідомлення SETUP – до кінцевого пристрою користувача В.

2. Кінцевий пристрій викликуваного користувача В відповідає на повідомлення SETUP повідомленням ALERTING, що означає, що пристрій вільний, а викликуваному користувачеві подається сигнал про вхідний виклик.

3. Після того, як користувач У приймає виклик, до зухвалої сторони А передається повідомлення CONNECT з номером Tcp-порту каналу H.245.

4. Кінцеві пристрої обмінюються по каналі H.245 інформацією про типи використовуваних мовних кодеків та про інші функціональні можливості встаткування, і сповіщають один одного про номери портів RTP, на які варто передавати інформацію.

5. Відкриваються логічні канали для передачі мовної інформації.

6. Мовна інформація передається в обидва боки в повідомленнях протоколу RTP; крім того, ведеться контроль передачі інформації за допомогою RTCP.

Наведена процедура обслуговування виклику базується на протоколі H.323 версії 1. Версія 2 протоколи H.323 дозволяє передавати інформацію, необхідну для створення логічних каналів, безпосередньо в повідомленні SETUP протоколу H.225.0 без використання протоколу H.245. Така процедура називається «швидкий старт» (Fast Start) і дозволяє скоротити кількість циклів обміну інформацією при встановленні з'єднання. Крім організації базового з'єднання, у мережах H.323 передбачене надання додаткових послуг відповідно до рекомендацій ITU H.450.X. Моніторинг якості обслуговування забезпечується протоколом

RTCP, однак обмін інформацією RTCP відбувається тільки між кінцевими пристроями, що беруть участь у з'єднанні.

Другий підхід до побудови мереж IP-телефонії заснований на використанні протоколу SIP – Session Initiation Protocol. SIP являє собою текст – орієнтований протокол, що є частиною глобальної архітектури мультимедіа. Ця архітектура також містить у собі протокол резервування ресурсів (RSVP, RFC 2205), транспортний протокол реального часу (RTP, RFC 1889), протокол передачі потоків у реальному часі (RTSP, RFC 2326), протокол опису параметрів зв'язку (SDP, RFC 2327), протокол повідомлення про зв'язок (SAP). Однак функції протоколу SIP не залежать від кожного із цих протоколів.

Третій підхід до побудови мереж IP-телефонії, заснована на використанні протоколу MGCP. При розробці цього протоколу робоча група MEGACO опиралася на мережну архітектуру, що містить основні функціональні блоки трьох видів:

шлюз – Media Gateway (MG), що виконує функції перетворення мовної інформації, що надходить із боку ТфОП з постійною швидкістю передачі, у вид, придатний для передачі по мережах з маршрутизацією пакетів IP (кодування й упакування мовної інформації в пакети RTP/UDP/IP, та зворотнє перетворення);

контролер шлюзів – Call Agent, що виконує функції керування шлюзами;

шлюз сигналізації – Signaling Gateway (SG), що забезпечує доставку сигнальної інформації, що надходить із боку ТфОП, до контролера шлюзів і перенос сигнальної інформації у зворотному напрямку.

Таким чином, весь інтелект функціонально розподіленого шлюзу зосереджений у контролері, функції якого можуть бути розподілені між декількома комп'ютерними платформами.

Для побудови добре функціонуючих і сумісних із ТфОП мереж IP-телефонії підходять протоколи H.323 і MGCP. Як вже відзначалось, протокол SIP трохи гірше взаємодіє із системами сигналізації, використовуваними в ТфОП. Підхід, заснований на використанні протоколу MGCP, має досить важливу перевагу перед підходом H.323: підтримка контролером шлюзів сигналізації ОКС7 і інших видів сигналізації, а також прозора трансляція сигнальної інформації з мережі IP-телефонії. У мережі, побудованої на базі рекомендації H.323, сигналізація ОКС7, як і будь-яка інша сигналізація, конвертується шлюзом у сигнальні повідомлення H.225.0 (Q.931). Основним недоліком третього з наведених у даному параграфі підходів є незакінченість стандартів. До недоліків можна віднести також відсутність стандартизованого протоколу взаємодії між контролерами. Крім того, протокол MGCP є протоколом керування шлюзами, але не призначений для керування з'єднаннями за участю термінального встаткування користувачів (IP-телефонів). Це означає, що в мережі, побудованої на базі протоколу MGCP, для керування термінальним устаткуванням повинен бути присутнім gatekeeper або сервер SIP. Варто також відзначити, що в існуючих додатках IP-телефонії, таких як надання послуг міжнародного й міжміського зв'язку, використовувати протокол MGCP (також, як і протокол SIP) недоцільно у зв'язку з тим, що основна кількість мереж IP-телефонії сьогодні побудована на базі протоколу H.323. В останньому зі згаданих підходів (у проекті версії 4 рекомендації H.323) введено принцип декомпозиції шлюзів, використаний у третьому підході. Керування функціональними блоками розподіленого шлюзу буде здійснюватися контролером шлюзу – MGC (Media Gateway Controller) за допомогою протоколу MEGACO/H.248.

Опис протоколу обміну інформацією

Як було обґрунтовано раніше, сучасна IP-телефонія будується на основі протоколу H.323. Розглянемо більш докладно цей протокол. У рекомендаціях, що входять у сімейство H.323, визначені протоколи, методи й мережні елементи, необхідні для організації мультимедійного зв'язку між двома або більше користувачами [15-22].

Найбільш затребуваною з послуг, специфікованих у рекомендації H.323, є послуга передачі мовної інформації з мереж з маршрутизацією пакетів IP. Найпоширенішим

підходом до побудови мереж IP-телефонії сьогодні є саме підхід, запропонований ITU-T у рекомендації H.323.

Сімейство протоколів H.323 містить у собі три основних протоколи: протокол взаємодії кінцевого устаткування з gatekeeper – RAS, протокол керування з'єднаннями – H.225 і протокол керування логічними каналами – H.245. Ці три протоколи, разом з Інтернет-протоколами TCP/IP, UDP, RTP і RTCP, а також з описаним в [6] протоколом Q.931 складають основу технології IP-телефонії. Суть ієрархії цих протоколів полягає в наступному. Для переносу сигнальних повідомлень H.225 і керуючих повідомлень H.245 використовується протокол з встановленням з'єднання й з гарантованою доставкою інформації – TCP. Сигнальні повідомлення RAS переносяться протоколом з негарантованою доставкою інформації – UDP. Протокол RAS забезпечує контроль використання мережних ресурсів, підтримує автентифікацію користувачів і може забезпечувати нарахування плати за послуги. Для переносу мовної і відеоінформації використовується протокол передачі інформації в реальному часі – RTP. Контроль переносу користувальницької інформації виробляється протоколом RTCP. Процедура встановлення з'єднання в таких мережах IP-телефонії базується на рекомендації Q.931 [15] і аналогічна процедурі, використовуваної в ISDN.

Основними пристроями мережі є: термінал, шлюз, gatekeeper і пристрій керування конференціями.

Термінал H.323 – це кінцевий пристрій мережі IP-телефонії, що забезпечує двосторонній мовний або мультимедійний зв'язок з іншим терміналом, шлюзом або пристроєм керування конференціями. Користувальницький інтерфейс керування системою дає користувачеві можливість створювати й приймати виклики, а також конфігурувати систему й контролювати її роботу.

Таблиця. 1 – Сімейство протоколів H.323

<table>
<tr><td colspan="3">Гарантована доставка інформації із протоколу TCP</td><td colspan="3">Негарантована доставка інформації із протоколу UDP</td></tr>
<tr><td rowspan="2">H.245</td><td colspan="2">H.225</td><td colspan="3">Потоки мови й відеоінформації</td></tr>
<tr><td>Керування з'єднанням (Q.931)</td><td>RAS</td><td>RTCP</td><td>RTP</td></tr>
<tr><td colspan="3">TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="6">IP</td></tr>
<tr><td colspan="6">Канальний рівень</td></tr>
<tr><td colspan="6">Фізичний рівень</td></tr>
</table>

Модуль керування підтримує три види сигналізації: H.225, H.245 і RAS. Цей модуль забезпечує реєстрацію термінала у gatekeeper, установлення й завершення з'єднання, обмін інформацією, необхідної для відкриття мовних каналів, надання додаткових послуг і техобслуговування.

Телематичні додатки забезпечують передачу користувальницьких даних, нерухливих зображень і файлів, доступ до баз даних і т.п. Стандартним протоколом для підтримки таких додатків є протокол T. 120.

Модуль H.225.0 відповідає за перетворення відеоінформації, мови, даних і сигнальної інформації у вид, придатний для передачі по мережах з маршрутизацією пакетів IP, і за зворотне перетворення. Крім того, функціями модуля є розбивка інформації на логічні кадри, нумерація послідовно переданих кадрів, виявлення й корекція помилок.

Мережний інтерфейс забезпечує гарантовану передачу керуючих повідомлень H.245, сигнальних повідомлень H.225.0 (Q.931) і користувальницьких даних за допомогою протоколу TCP і негарантовану передачу мовної й відеоінформації, а також повідомлень RAS, за допомогою протоколу UDP.

Блок синхронізації вносить затримку на прийомній стороні з метою забезпечити синхронізацію джерела інформації з її приймачем, узгодження мовних і відеоканалів або згладжування варіації затримки інформації.

Відеокодеки кодують відеоінформацію, що надходить від зовнішнього джерела відеосигналів (відеокамери або відеомагнітофона), для її передачі по мережі з маршрутизацією пакетів IP і декодують сигнали, що надходять із мережі, для наступного відображення відеоінформації на моніторі або телевізорі.

Аудіокодеки кодують аудіоінформацію, що надходить від мікрофона (або інших джерел аудіоінформації), для її передачі по мережі з маршрутизацією пакетів IP і декодують сигнали, що надходять із мережі, для відтворення.

Слід зазначити, що при організації децентралізованої конференції термінал H.323 може приймати більш ніж один потік мовної інформації. У цьому випадку термінал повинен уміти змішувати або перемикати пакетовану мову, що надходить від інших учасників конференції.

Основною функцією шлюзу H.323 є перетворення мовної (мультимедійної) інформації, що надходить із боку ТфОП з постійною швидкістю, у вид, придатний для передачі по IP-мережах.

При відсутності в мережі gatekeeper повинна бути реалізована ще одна функція шлюзу – перетворення номера ТфОП у транспортну адресу IP-Мережі.

З боку мереж з маршрутизацією пакетів IP, так само, як і з боку ТфОП, шлюз може брати участь у з'єднаннях як термінал або пристрій керування конференціями. У випадку, коли термінал H.323 зв'язується з іншим терміналом H.323, розташованим у ті ж самій IP-мережі, шлюз у цьому з'єднанні не бере участь.

Шлюз, у сукупності з gatekeeper мережі IP-телефонії, утворить універсальну платформу для надання всього спектра послуг зв'язку.

У gatekeeper зосереджений весь інтелект мереж IP-телефонії, що базуються на рекомендації ITU H.323. Мережа H.323 має зонну архітектуру. Gatekeeper виконує функції керування зоною мережі IP-телефонії, у яку входять термінали, шлюзи й пристрої керування конференціями, зареєстровані в цього gatekeeper. Різні ділянки зони мережі H.323 можуть бути територіально рознесені й з'єднуватися один з одним через маршрутизатори. Варто звернути увагу на те, що комутатори кадрів Ethernet і маршрутизатори пакетів IP не є мережними елементами H.323, тому що вони працюють на ланковому або мережному рівнях відповідно, у той час як устаткування H.323 працює на прикладному рівні стека протоколів TCP/IP.

У число найбільш важливих функцій, виконуваних gatekeeper, входять:

перетворення так званої alias-адреси (ім'я абонента, телефонного номера, адреси електронної пошти й ін.) у транспортну адресу мережі з маршрутизацією пакетів IP (IP адреса й номер порту TCP);

контроль доступу користувачів системи до послуг IP-телефонії за допомогою сигналізації RAS (використовуються повідомлення ARQ/ACF/ARJ);

контроль, керування й резервування пропускної здатності мережі;

маршрутизація сигнальних повідомлень між терміналами, розташованими в одній зоні; gatekeeper може організовувати сигнальний канал безпосередньо між терміналами або ретранслювати сигнальні повідомлення від одного термінала до іншого.

У тому випадку, коли абонент, який викликає, знає IP-адресу термінала абонента, який викликається, з'єднання між двома пристроями може бути встановлене без допомоги gatekeeper. Але, при наявності gatekeeper я забезпечується мобільність абонентів, тобто здатність користувача одержати доступ до послуг з будь-якого термінала в будь-якому місці мережі й здатність мережі ідентифікувати користувачів при їхньому переміщенні з одного місця в інше. При відсутності в мережі gatekeeper перетворення адреси викликуваного абонента, що надходить із боку ТфОП у форматі E. 164, у транспортну адресу IP-мережі повинне виконуватися шлюзом. В одній мережі може перебувати декілька gatekeeper, які

повинні взаємодіяти між собою. Слід особливо зазначити, що хоча gatekeeper є окремим логічним елементом мережі, він може бути реалізований у терміналі, у шлюзі, у пристрої керування конференціями або в пристроях, не специфікованих у рекомендації Н.323.

Рекомендація Н.323 передбачає три види конференцій.

Перший вид – централізована конференція, у якій кінцеві пристрої з'єднуються в режимі точка-точка із пристроєм керування конференціями (MCU), що контролює процес створення й завершення конференції, а також обробку потоків користувацької інформації.

Другий вид – децентралізована конференція, у якій кожний її учасник з'єднується з іншими учасниками в режимі точка – група точок, і кінцеві пристрої самі обробляють потоки інформації, що надходять від інших учасників.

Третій вид – змішана конференція, тобто комбінація двох попередніх видів.

Перевага централізованої конференції – порівняно прості вимоги до термінального встаткування, недолік – більша вартість пристрою керування конференціями.

Для децентралізованої конференції потрібно більше складне термінальне встаткування, крім того, бажано, щоб у мережі підтримувалася передача пакетів IP у режимі багатоадресного розсилання (IP multicasting). Якщо мережа не підтримує цей режим, термінал може передавати інформацію до кожного з інших терміналів, що беруть участь у конференції, у режимі точка-точка, але це стає неефективним при числі учасників більше чотирьох. Пристрій керування конференціями MCU містить один обов'язковий елемент – контролер багатоточкових з'єднань – Multipoint controller (MC). Крім того, MCU може містити один або більше процесорів для обробки інформації користувачів при багатоточкових з'єднаннях – Multipoint processor (MP). Слід зазначити, що контролер MC і процесор MP є самостійними логічними пристроями Н.323 і що контролер може існувати незалежно від процесора (зворотне невірно). Контролер може бути фізично сполучений з gatekeeper, зі шлюзом або з MCU, а MCU, у свою чергу, може бути сполучене зі шлюзом або з gatekeeper.

Контролер конференцій повинен використовуватися для організації конференції будь-якого виду. Він організує обмін між учасниками конференції даними про функціональні можливості їхніх терміналів, указує, у якому режимі (з використанням яких кодеків) учасники конференції можуть передавати інформацію, причому цей режим може змінюватися в ході конференції, наприклад, при підключенні до неї нового учасника. Таким чином, контролер MC визначає режим конференції, що може бути загальним для всіх учасників конференції або окремим для кожного з них. В зв’язку з тим, що в мережі може бути кілька контролерів MC, то для кожної знову створюваної конференції повинна проводитися процедура визначення встаткування, для того, щоб виявити той з контролерів MC, що буде управляти даною конференцією. При організації централізованої конференції, крім контролера MC, повинен використовуватися процесор MP, що обробляє користувальницьку інформацію й відповідає за перемикання або змішування мовних потоків, відеоінформації й даних. При організації децентралізованої конференції процесор MP не використовується.

Розробка структурної схеми

Для перевірки коректності реалізації даної задачі було виконано багато розрахунків та експериментальних матеріалів. Цьому питанню приділялась особлива увага тому, що помилка при розрахунку привела б до ряду негативних наслідків. Відлагодження та перевірка, що підтверджує вірність програмних рішень відбувалась за декількаами етапами:

- математична перевірка окремих модулів;
- математична перевірка всієї системи (з допомогою математичної логіки будується логічна схема всієї системи);
- практична перевірка підпрограм (перевіряється процедурна частина кожної підпрограми окремо);

– практична перевірка всієї системи у дії (перевіряється ситема в цілому за допомогою вводу різних даних у програму, потім на виході з програми перевіряємо отриману інформацію з очікуваною).

Для підтвердження правильності розрахунку програми були використані експерементальні дані різних аудіо форматів, були проведені консультації з даного питання зі спеціалістами.

Простота мови проектування та маніпулювання даними, зручність спілкування користувача з системою до мінімума вивчення цієї програми. Користувач програми – це людина, яка повинна володіти азами програмування. При написанні програми я намагалася, щоб програма відповідала наступним параметрам:

– Швидкодія. Програма працює постійно з великою кількістю кінцевих абонентів (селективний зв'язок).

– Захист. Забезпечити надійний захишенний канал зв`язку.

– Відсутність проблеми дороговизни сучасних персональних комп'ютерів. Система, що написана може встановлюватись на будь-якому персональному комп'ютері – використовувати відносно швидкі алгоритми захисту зв'язку.

– Можливість зручно і швидко формувати приклади і теорію для користувача.

– Можливість звертання до системних ресурсів. Користувача системи цікавить її інформаційний та сенсовий зміст. Подробиці організації фізичного зберігання даних його не цікавлять.

Перш за все перед розробкою системи слід одержати уявлення на наступні моменти:

- на які частини можна розбити систему;
- одержати уявлення про кожну частину (фрагмент);
- яка інформація і з якою детальністю необхідна користувачу кожного фрагменту;
- які процеси передачі і обробки даних знаходяться в кожному фрагменті;
- технологія накопичування і обробки аудіо інформації системи;
- на якому обладнанні планується реалізувати систему;
- технологія функціюваня системи;
- чи необхідна адаптація і налаштування системи при змінах деяких умов.

Для розробки програми були попередньо збудовані функціональна схема, структурна схеми, структурна схема системи керування, схема процесів, а також блок-схеми алгоритму програми, розглянемо їх детально.

В процесі практичної реалізації теоретичних принципів розробки системи, додатково розглянутих вище, була розроблена структурна схема системи, яка зображена на рисунку 1.

Завдяки структурній схемі можна чітко побачити основні структурні блоки системи та взаємозв'язки між ними. При розробці структурної схеми основний упор робився на існуючи розробки ПЗ і їх модулі допомоги. Аналіз рисунка 1 дозволяє чітко прослідити як працює програма.

Розглянемо схему зверху вниз, в напрямку від пристрою до кінцевої програми – за допомогою внутрішнього пула доступу що забезпечує закриті канали зв'язку абоненти генеральний директор, відділи бухгалтерії, логістики, складу, збуту, економічної безпеки – можуть взаємодіяти з дочірніми виробниками з використанням внутрішньої АТМ. і чітко налагодженої технічної системи взаємодії. Технічна частина взаємодії забезпечується VoIP та воротарем з використанням маршрутизатора.

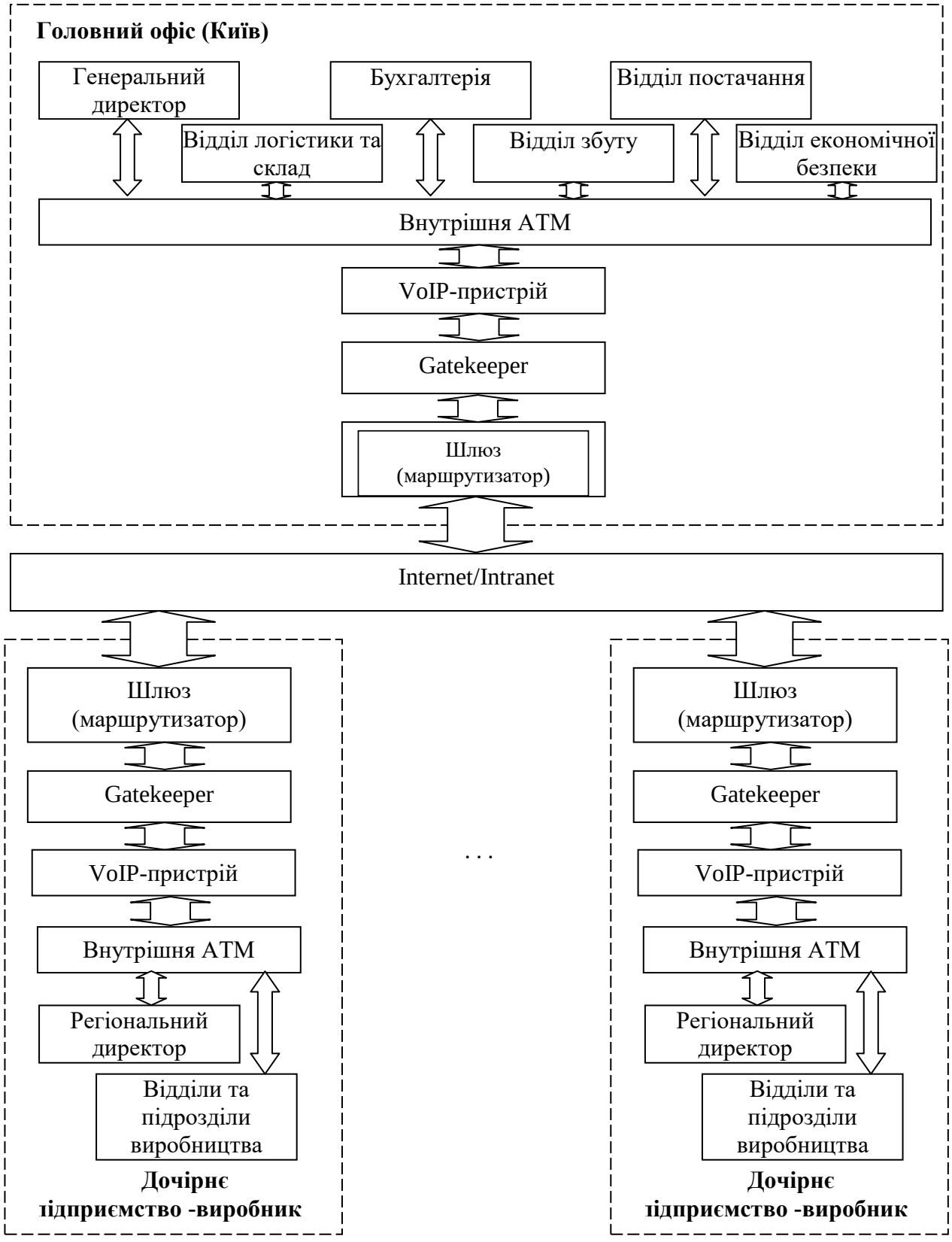


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів IP-телефонії з забезпеченням конфіденційності. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем IP-телефонії з забезпеченням конфіденційності. Досліджена система IP-телефонії з

забезпеченням конфіденційності. На основі отриманих результатів досліджень створена програмна реалізація системи IP-телефонії з забезпеченням конфіденційності. Розроблені алгоритми дозволяють успішно вирішувати завдання IP-телефонії з забезпеченням конфіденційності. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
2. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
3. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
4. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 15-16 жовтня 2010 р. – Кіровоград – С. 58
5. Дрєєв О.М. Узагальнення вейвлету Хаара / О.М. Дрєєв // Матеріали науково-практичної конференції, присвяченої 80-річчю фізико-математичного факультету КДПУ ім. В. Винниченка 26 листопада 2010 р. – Кіровоград – С. 12
6. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.В. Коваленко // Тези доповідей Новітні технології – для захисту повітряного простору. Дев'ята наукова конференція. 18-19 квітня 2011 р. – Х.: ХУПС. – 2012. – С. 206
7. Дрєєв О.М. Метод довгострокового прогнозування навантаження серверу телекомунікаційної мережі / О.М. Дрєєв, Г.М. Дрєєва // Комбінаторні конфігурації та їх застосування. Кіровоград. 13-14 квітня 2012 р. – Кіровоград: "Екслюзів-систем". – 2012. – С. 50
8. Дрєєв О.М. Вдосконалення стиснення зображень SPIHT методу шляхом додаткового кодування та відкладеної передачі уточнення вейвлет коефіцієнтів / О.М. Дрєєв // Дискретна математика та її застосування у економіко-математичному моделюванні та інформаційних технологіях. 11-13 жовтня 2012 р. – Запоріжжя: ЗНУ – 2012. – С. 22-23.
9. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19
10. Дреев А.Н. SPIHT кодирование с отложенной передачей значимых битов / А.Н. Дреев // Тези доповідей. Новітні технології – для захисту повітряного простору. Дев'ята наукова конференція 17 квітня 2013 р. – Х.: ХУПС. – 2013. – С. 206

УДК 004

Б. Панасюк, магістр гр. КІ-20М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ОБМІНУ ІНФОРМАЦІЄЮ У КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ DMVPN

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Метою розробки є дослідження та програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Об’єктом дослідження є процес забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Предметом дослідження є методи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Методи дослідження базуються на методах теорії інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, корпоративна мережа, DMVPN

Постановка проблеми. DMVPN (Dynamic Multipoint Virtual Private Network) – динамічна багатоточкова віртуальна приватна мережа. Ця технологія є подальшим розвитком VPN компанією Cisco Systems. Якщо коротко, то вона дозволяє створити віртуальну приватну мережу з можливістю динамічного створення тунелів між вузлами. Припустимо, що є якесь підприємство із центральним офісом і декількома філіями, територіально рознесеними по декількох площадках (одна з них в іншому місті або навіть державі), які потрібно об'єднати в одну мережу. Підприємство не дуже багате й не може дозволити собі використовувати для зв'язку між офісами орендовані канали. Зате на кожній площадці є вихід в Інтернет. Це може бути мережа одного конкретного провайдеру або різних, не важливо.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

– Дослідження системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

– Програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Об’єктом дослідження є процес забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Предметом дослідження є методи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Методи дослідження базуються на методах теорії інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У цей час існують сотні VPN-сервісів, і всі заявляють про себе як про лідерів. У таких умовах стає складно знайти по-справжньому кращий VPN. Наші рекомендації опираються на найважливіші критерії, що дозволить вам найбільш зваженим образом вибрати кращий VPN для роботи в Україні.

Безпека

Двома найважливішими аспектами будь-якого гарного VPN-сервісу є конфіденційність і безпека. Вам необхідно знайти сервіс, що пропонує все це не тільки на папері, але й у реальності.

VPN-сервіс із підтвердженою безлоговою політикою зможе надійно сховати всі ваші цифрові сліди від сторонніх. Безлогова політика означає, що сервіс не збирає, не зберігає й не передає дані про те, що ви робили в Мережі. Такий сервіс захистить ваші дані від сторонніх і забезпечить вам можливість працювати в Інтернеті конфіденційно. Як наслідок, наявність безлогової політики – це один з головних критеріїв, які лягли в основу VPN-рейтингів.

Швидкість

Але не можна назвати кращим VPN-сервіс без гідної швидкості підключення. Використання технології VPN означає, що ваш трафік буде перенаправлятися через додаткові сервери, що за замовчуванням сповільнює обмін даними. Будь-який VPN буде в тому або іншому ступені знижувати швидкість підключення; так що правильно буде порушити питання «наскільки?». Найшвидші VPN-сервіси впливають на якість підключення мінімальним образом. З ними ви зможете переглядати сайти, завантажувати торренти й дивитися потокові трансляції без лагів і буферизації.

По-справжньому швидкий VPN навіть допоможе вам обійти обмеження швидкості підключення, установлені інтернет-провайдером. Цілком можливо, що так ваша швидкість виявиться навіть вище, ніж була!

Потоковий контент

До слова про стріми: VPN-сервіси – це популярне рішення для тих, хто хоче мати вільний доступ до всьому контенту таких платформ, як Netflix, Hulu, BBC iPlayer і DAZN. Ці сервіси обмежують доступність контенту залежно від регіону, звідки приходить користувач. На щастя, підключення до підходящого VPN-серверу дозволить вам одержати доступ до улюблених фільмів і серіалів.

Торренти

VPN-сервіси придадуться й для аматорів торрентів, особливо в країнах, де такий формат обміну даними заборонений. Навіть якщо ви дотримуєте всі правила (а саме це у даній роботі й рекомендуємо), завантаження торрентів без додаткових заходів захисту можуть поставити вас під удар з боку хакерів і жадібних копірайтних тролів.

P2P-підключення не захищені самі по собі, але виправити цей недолік можна за допомогою гарного VPN для торрентів. Сховавши свій вихідна IP-адресу й сховавши трафік за шаром шифрування, ви відгородите себе від всіх погроз, пов'язаних із завантаженням торрентів, зберігаючи їхньої переваги. Становлячи цей VPN-рейтинг, у даній роботі проаналізували всі важливі особливості сервісів у плані торрентів: P2P-режими роботи, SOCKS 5-проксі й легке налаштування торрент-клієнтів.

Цензура

Нарешті, давайте поговоримо про цензуру. Ви зрозумієте, що знайшли надійний сервіс, коли обраний вами VPN буде працювати в країні, незважаючи на активні спроби її влади заблокувати такого роду ресурси. Проводячи наше дослідження, у даній роботі звертали особливу увагу на спеціальні функції й налаштування, що забезпечують додаткову обфускацію (приховання) трафіку. Кращі VPN-сервіси в цьому рейтингу довели, що можуть працювати навіть у таких складних країнах, як Китай, Іран й т.і. Є й інші фактори, що визначають місця в нашому рейтингу: розмір серверної мережі, шифрування, функції безпеки, простота роботи й, звичайно ж, ціна. У даній роботі не поспішали, уважно вивчаючи й перевіряючи всі аспекти роботи VPN-сервісів для складання наших оглядів.

Є думка, що конфіденційність у Мережі – це базове право людини й платити за це не можна. У теорії у даній роботі дотримуємося тих же поглядів, однак не можна забувати про те, як обстоять справи на практиці.

VPN-сервіси пропонують своїм послуги в обмін на щось. І якщо мова йде не про гроші, варто насторожитися! Навіть сир у мишоловці не буває безкоштовним: якщо ви не платите за товар, те самі стаєте товаром.

На жаль, але більшість безкоштовних VPN-сервісів надають свої послуги з величезними обмеженнями, а іноді й прямо загрожують безпеці й конфіденційності користувальницьких даних. Низька швидкість, обмежена пропускна здатність каналу, що дратує реклама й навіть продаж користувальницьких даних – це далеко не повний список того, із чим можна зштовхнутися, вибравши безкоштовний VPN.

Відмінним прикладом служить Hola. Цей безкоштовний VPN-сервіс по суті являє собою проксі-сервіс, заснований на протоколі P2P і перенаправляючий трафік одних користувачів через пристрої інших. Таким чином, сервіс не тільки використовує інтернет-

канали своїх користувачів, але й збирає й записує практично всієї їхньої дії. В «політику конфіденційності» прямо зазначено, що Hola буде надавати ці дані третім сторонам, партнерам і рекламодавцям.

Звичайно, не всі безкоштовні VPN погані. У даній роботі ретельно протестували десятки таких сервісів і знайшли декілька безкоштовних і безпечних VPN. Але чи буде їх досить?

Вивчивши все, що можуть запропонувати вам платні VPN, ви навряд чи захочете користуватися безкоштовними сервісами. Все просто – якщо ви шукаєте спосіб надійно захистити свою конфіденційність і одержати стабільний і швидкий доступ до необхідних ресурсів і серверів, краще заплатити пари сотень рублів, чим знову й знову разочаровуватися в роботі безкоштовних VPN.

Помнете, що оформити передплату на VPN-сервіс можна на куди більше вигідних умовах, якщо скористатися знижками й купонами. Ви зможете одержати послуги сервісу преміум-класу за відносно невеликі гроші. Вигода отут незаперечна!

Кращі VPN-сервіси, упевнені як своя пропозиція, пропонують потенційним клієнтам скористатися безкоштовними пробними періодами на свої послуги. Також більшість сервісів дають гарантію повернення грошей, так що ви можете детально протестувати сервіс і не боятися викинути гроші на вітер.

VPN-сервіси часто використовують у незаконних цілях, тому багато хто вважають, що й самі ці сервіси незаконні. Це далеко від істини.

Використання VPN зовсім законно в 95,9% країн. Поза законом (або в так званій «сірій зоні») VPN-сервіси в наступних країнах:

Китай.

Ірак.

Іран.

Росія.

Білорусія.

Туреччина.

Оман.

ОАЕ.

Робота з VPN – це зовсім повсякденна справа. Багато компаній використовують VPN, щоб захистити свої дані, що представляють комерційну цінність, від хакерів, а також для проведення маркетингових досліджень у різних країнах миру.

Ховатися за VPN заради здійснення злочинів – от що незаконно. Але погодитеся, це не проблема VPN, особливо якщо врахувати, що мільйони користувачів вибирають ці сервіси заради захисту.

Спокійно використовувати VPN можна в більшості країн. Втім, дотримувати правил і не вплутуватися в сумнівні авантюри – це вже ваш обов'язок.

Крім того, ви можете зштовхнутися з певним ризиком у наступних ситуаціях:

Ви працюєте з VPN, що не має урядової ліцензії, на території країни, де дозволені тільки мають цю ліцензію сервіси;

Ви скачуєте торрент-файли з добутками, захищеними авторськими правами, через VPN-сервіс, ведучий логи або не вміє негайно обривати з'єднання.

У наші дні для роботи з VPN досить скачати застосунок із сайту сервісу й установити його, що займе від сили пари мінут.

Багато які VPN-сервіси можна назвати дуже зручними у використанні: у них інтуїтивно зрозумілі інтерфейси й прості інструкції. Вам потрібно буде тільки вибрати безпечний сервер зі списку або дозволити VPN-Додатку автоматично підключати вас до найбільш підходящої локації. Для цього в ньому повинна підтримуватися функція швидкого підключення.

Якщо ви ніколи не працювали з VPN, не переживайте! Всі набагато простіше, ніж здається, особливо якщо ви прочитаєте наше докладне керівництво для починаючих користувачів.

На щастя, VPN-сервіси преміум класу коштують зовсім не космічних грошей. Якщо купувати місячну підписку, ціни вигляд переконливо. А от якщо заплатити відразу за рік-два, то в перерахуванні вийде близько 3-7$ на місяць.

По факту, ви можете оформити передплату на високоякісний VPN-сервіс менше ніж за 3 долари на місяць!

Також варто відзначити, що в багатьох VPN-сервісів є безкоштовні пробні періоди, що допоможе вам перевірити їх на практиці й зрозуміти, чи відповідають їхні послуги вашим вимогам у плані швидкості, безпеки й так далі.

Багато сервісів також дають гарантію повернення грошей: у вас буде від 7 до 45 днів (залежить від самого сервісу), щоб встигнути скасувати підписку й одержати свої гроші назад, якщо щось вам не сподобається.

Також ви зможете заощадити на вартості підписки, скориставшись нашими акціями й знижковими купонами.

Tor, проксі й VPN – це три зовсім різних типи сервісів. Втім, часом вони використовуються заради однієї й тої ж мети. Давайте уважніше розглянемо цей момент.

Tor (скорочення The Onion Router) – це анонімна мережа, де ваше підключення перенаправляється через ланцюжок серверів, підтримуваних або надаваних волонтерами. Як наслідок, вас і ваші дані стає набагато складніше відстежити. При цьому швидкість з'єднання падає. Це досить складна тема, так що почитайте наш повний посібник з мережі Tor, якщо ви хочете краще в ній розібратися.

Що й говорити, на тлі VPN в Tor є чимало недоліків. Так, це безкоштовна мережа, однак шифрування тут використовується менш просунуте, а підключення виходять більше повільними. Найкраще буде використовувати Tor і VPN разом – так ви зможете скористатися перевагами обох технологій. Стабільне VPN-підключення зведе до 0 уразливості Tor, а Tor зробить ваше перебування в Мережі ще більш конфіденційним.

От тільки не будь-який VPN можна використовувати з Tor. Щоб фокус удався, вам потрібний VPN типу NordVPN, у якого є спеціальні сервери для підключення Tor-через-VPN.

Проксі-сервіси мають єдина перевага перед VPN: вони забезпечують за замовчуванням високу швидкість підключення й приховують користувальницька IP-адресу. От тільки ніяких захисних функцій у них ні, трафік вони не шифрують, а в багатьох і якогось окремого інтерфейсу немає.

Все це значить, що проксі-сервіси й не безпечні, і не зручні. Втім, якщо конфіденційність підключення для вас не пріоритетна, то можна скористатися й ними.

Є сотні й тисячі проксі-сервісів, тому важливо не помилитися з вибором. Але краще буде оформити недорогу передплату на швидкий VPN і насолоджуватися відмінною швидкістю підключень, бездоганним захистом і повною конфіденційністю.

Примітка. В vpnMentor є власний безкоштовний проксі! Скористайтеся ним, якщо поспішаєте й не можете дозволити собі вибирати.

Той самий VPN може надавати своїм клієнтам застосунки для самих різних платформ. Втім, отут не всі так однозначно! Наприклад, навіть якщо ваш VPN бездоганно працює на Windows, його мобільний застосунок може працювати нестабільно й ненадійно.

По правді сказати, немає такого VPN-сервісу, що був би однозначно кращим для всіх пристроїв, версій ПЗ й ОС. Щоб зробити правильний вибір, вам необхідно провести невелике дослідження, вибираючи краще рішення для ваших потреб із числа перевірених VPN .

Нижче ви знайдете наші регулярно обновлювані рейтинги кращих VPN для всіх основних платформ:

Windows.

Mac.

iOS, iPhone, iPad.

Android.
Chrome.
Firefox.
Safari.
Apple TV.
Smart TVs.
Kodi.
Fire TV Stick.
PS4.
Роутери.
Roku.

Покажемо приклад налаштування DMVPN – Dynamic Multipoint VPN, що є VPN рішенням компанії Cisco. Дане рішення використовується, коли потрібна висока масштабованість і легкість налаштування при підключенні філій до головного офісу.

DMPVN одне із самих масштабованих і ефективних рішень VPN підтримуваних компанією Cisco. В основному воно використовується при топології Hub-and-Spoke, де ви хотіли б бачити прямі VPN тунелі Spoke-to-Spoke на застосунок до звичайних Spoke-to-Hub тунелям. Це означає, що філії зможуть спілкуватися з один одним прямо, без необхідності проходження трафіку через HQ. Як уже згадували, ця технологія є пропрієтарною технологією Cisco.

Якщо вам необхідно підключити більше десяти сайтів до головного офісу, то DMPVN буде ідеальним вибором. Крім того, DMPVN підтримує не тільки Hub-and-Spoke, але й Full-Mesh топологію, так як всі сайти мають між собою зв’язність без необхідності налаштування статичних VPN тунелів між сайтами.

Для початку перелічимо важливі характеристики даного способу організації Site-to-Site VPN для кращого розуміння:

Центральний маршрутизатор (HUB) – даний роутер працює як DMVPN сервер, і Spoke маршрутизатори працюють як DMVPN клієнти.

У даного маршрутизатора є публічна статична IP-адреса на WAN інтерфейсі.

В Spoke маршрутизаторів на WAN інтерфейсах може як статична, так і динамічна публічна IP-адреса.

У кожної філії (Spoke) є IPSEC тунель до головного офісу (Hub).

Spoke-to-Spoke – тунелі встановлюються при виникненні необхідності, коли є рух трафіку між філіями. Таким чином, трафік може не ходити через головний офіс, а використовувати прямі тунелі між філіями.

Всі тунелі використовують Multipoint GRE с IPSEC.

NHRP (Next Hop Resolution Protocol) – даний протокол використовується для встановлення відповідностей між приватними IP тунельних інтерфейсів з публічними WAN адресами

Описані вище NHRP відповідності будуть зберігатися на NHRP сервері, чим у нашім випадку є HUB роутер. Кожна філія встановлює з'єднання з головним офісом і реєструє свою публічну IP-адресу і його приватну IP-адресу тунеля.

Коли філії необхідно відправити пакети в підмережу іншої філії, він запитує NHRP сервер для одержання інформації про зовнішню публічну адресу цільової філії.

Для кращої масштабованості радимо використовувати один із протоколів динамічний маршрутизації між всіма роутерами – наприклад, EIGRP.

Ще раз коротко про технології, які використовує DMVPN:

Multipoint GRE.
IPSEC.
NHRP – Next Hop Resolution Protocol.
Статична або динамічна маршрутизація.

Dynamic Multipoint VPN (DMVPN) – віртуальна приватна мережа з можливістю динамічного створення тунелів між вузлами.

На цій сторінці детально описується процедура організації мережі DMVPN на маршрутизаторах Cisco. Розглядаються варіанти налаштування проколовши динамічної маршрутизації OSPF і EIGRP, автентифікація маршрутизаторів по сертифікатах і pre-shared key.

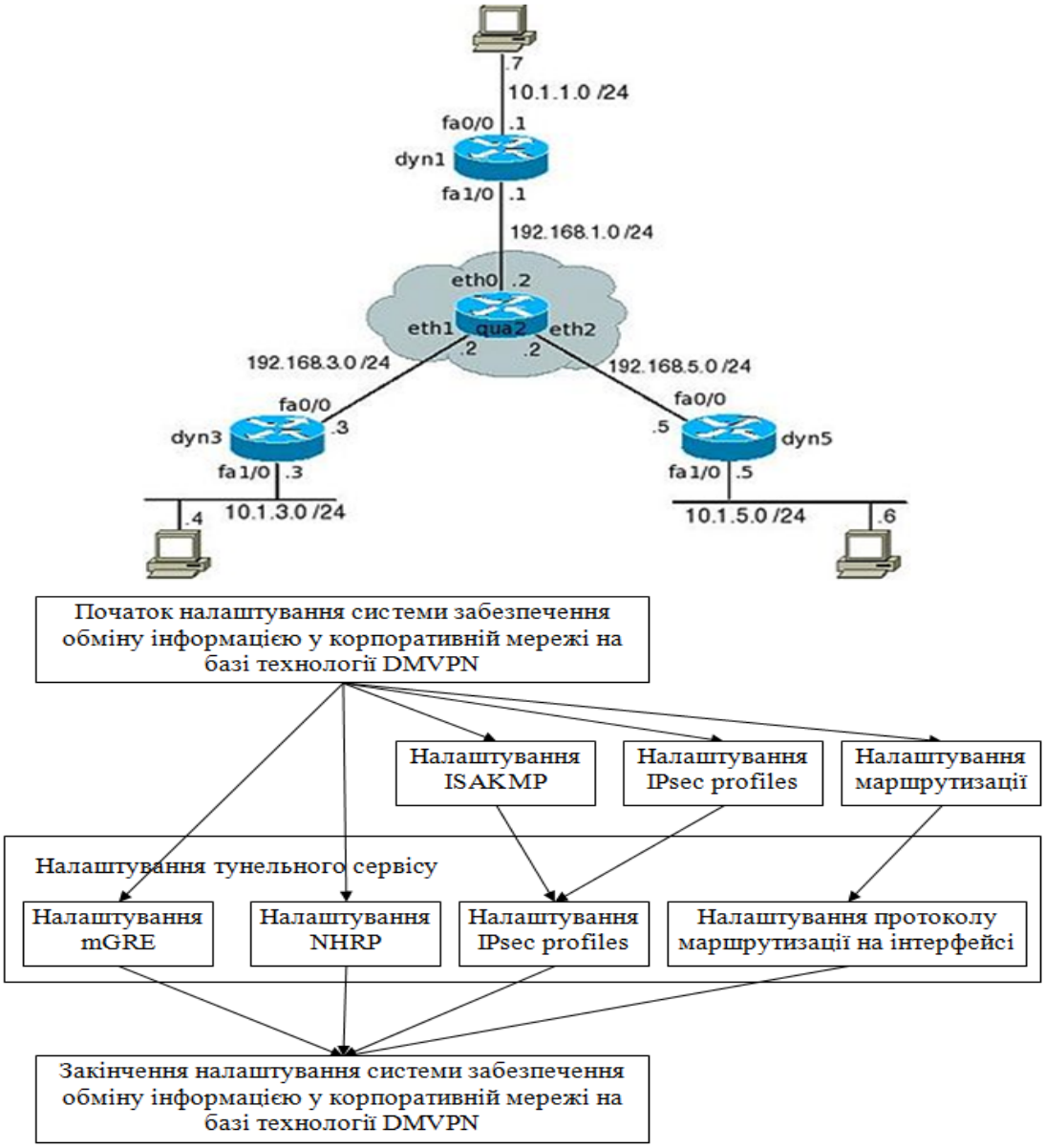


Рисунок 1 – Структурна схема системи

На сторінці dmvpn/config представлені схема й конфігураційні файли для віртуальної мережі Xentaur, що розглядається на цій сторінці.

Центральний офіс (що перебуває за dyn1) з'єднаний з декількома віддаленими (що перебувають за dyn3 і dyn5). Необхідно забезпечити зв'язок віддалених офісів із центральним і, при необхідності, установлювати тунель між віддаленими офісами.

Маршрутизація між мережами офісів буде виконуватися за допомогою протоколів динамічної маршрутизації.

Зображена топологія називається – зірка (hub-and-spoke), де:

- dyn1 – центр зірки, hub-маршрутизатор;
- dyn3 і dyn5 – вершини зірки, spoke-маршрутизатори.

Рішення

Якщо в даній схемі використовувати звичайну віртуальну приватну мережу, що з'єднує мережі (site-to-site VPN), то на маршрутизаторах, які перебувають у віддалених офісах, необхідно буде налаштувати тунель для зв'язку із центральним офісом і тунелі для зв'язку з іншими віддаленими офісами. Для того щоб всі віддалені офіси могли працювати між собою прямо, необхідно буде налаштувати тунелі з усіма офісами, що приведе до створення повнозв'язної топології (full mesh). Як наслідок, кількість налаштувань на маршрутизаторах, як у центральному офісі, так і у віддалені істотно збільшується.

Технологія DMVPN дозволяє вирішити це завдання більше масштабованим методом, чим створення зв'язків точка-точка між всіма офісами й об'єднання їх у повнозв'язну топологію:

При додаванні нових маршрутизаторів в існуючу мережу DMVPN, необхідно налаштувати тільки новий маршрутизатор, змін на вже існуючих маршрутизаторах не потрібно.

DMVPN дозволяє використовувати динамічно призначені IP-адреси на spoke-маршрутизаторах.

Якщо двом spoke-маршрутизаторам необхідно встановити тунель прямо, то він установлюється динамічно.

В основі DMVPN лежать кілька технологій:

mGRE-тунелі;

Протокол NHRP (Next Hop Resolution Protocol);

Протоколи динамічної маршрутизації;

Так як DMVPN використовує кілька технологій, то пошук несправностей у його налаштуваннях може займати досить багато часу. Для того щоб уникнути помилок, бажано пошагово перевіряти виконані налаштування, роботу відповідних протоколів і доступність мереж.

Нижче опишемо послідовність дій при налаштуванні системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.

Базові налаштування мережі

Налаштування мережі DMVPN будемо виконувати на умовному прикладі, що відбиває ключові особливості мереж, у яких доцільно використовувати цю технологію.

За кожним маршрутизатором перебуває мережа, що імітує локальну мережу офісів:

- dyn1 – 10.1.1.0/24;
- dyn3 – 10.1.3.0/24;
- dyn5 – 10.1.5.0/24.

Для зовнішніх інтерфейсів обрані мережі:

- dyn1 – 192.168.1.0/24;
- dyn3 – 192.168.3.0/24;
- dyn5 – 192.168.5.0/24.

Налаштування маршрутизації між зовнішніми інтерфейсами маршрутизаторів

У даній тестовій мережі на кожному маршрутизаторі прописані статичні маршрути до мереж зовнішніх інтерфейсів інших маршрутизаторів.

Статичні маршрути на hub-маршрутизаторі (dyn1).

Але можна зробити простіше – прописати default GW.

mGRE-тунелі

У топології зірка (hub-n-spoke) використання GRE-тунелів точка-точка приведе до великої кількості налаштувань, так як IP-адреси всіх spoke-маршрутизаторів повинні бути відомі й настроєні на центральному маршрутизаторі (hub).

Альтернативою GRE-тунелів точка-точка є multipoint GRE (mGRE) тунель, що дозволяє термінувати на собі декілька GRE-тунелів. mGRE-тунель дозволяє одному GRE-інтерфейсу підтримувати декілька IPsec-тунелів і спрощує кількість і складність налаштувань, у порівнянні з GRE-тунелями точка-точка.

Крім того, mGRE-інтерфейс дозволяє використовувати динамічно призначені IP-адреси на spoke-маршрутизаторах.

Налаштування mGRE-тунелів

Для адресації тунелів виділена мережа 10.10.10.0/24, всі тунелі перебувають в одній мережі. На hub-маршрутизаторі й spoke-маршрутизаторах mGRE-тунелі настроюються аналогічно (далі приклад для hub-маршрутизатора).

Створення тунельного інтерфейсу.

Завдання IP-адреси на інтерфейсі.

Так як GRE додає додаткові заголовки до IP-пакета, необхідно змінити значення MTU на інтерфейсі.

Як адреса відправника в пакеті вихідному з mGRE-інтерфейсу буде використовуватися IP-адреса фізичного інтерфейсу, а адреса одержувача буде виучений динамічно за допомогою протоколу NHRP.

Налаштування відповідності між тунельним інтерфейсом і фізичним.

Включення mGRE-тунелю.

(Опціонально) Завдання ключа, що ідентифікує тунель.

Якщо буде використовуватися топологія із двома hub-маршрутизаторами й, відповідно, двома мережами DMVPN, то ключ указує на приналежність інтерфейсу однієї з мереж DMVPN.

Next Hop Resolution Protocol (NHRP)

Next Hop Resolution Protocol (NHRP) – клієнт-серверний протокол перетворення адрес, що дозволяє всім хостам, які перебувають в NBMA(Non Broadcast Multiple Access)-мережі, динамічно вивчити NBMA-адреси (фізичні адреси) один одного звертаючись до next-hop-сервера (NHS). Після цього хости можуть обмінюватися інформацією один з одним прямо.

У мережі DMVPN:

Hub-маршрутизатор буде працювати як NHS, а spoke-маршрутизатори будуть клієнтами.

Hub-маршрутизатор зберігає й обслуговує базу даних NHRP, у якій зберігаються відповідності між фізичними адресами й адресами mGRE-тунелів spoke-маршрутизаторів.

На кожному spoke-маршрутизаторі hub-маршрутизатор статично зазначений як NHS і задан відповідність між фізичною адресою й адресою mGRE-тунелю hub-маршрутизатора.

При включенні кожний spoke-маршрутизатор реєструється на NHS і, при необхідності, запитує в сервера інформацію про адреси інших spoke-маршрутизаторів для побудови spoke-to-spoke тунелів.

Network ID – характеристика локальна для кожного маршрутизатора (аналогія – OSPF process ID). Різні інтерфейси можуть брати участь у різних NHRP сесіях; це просто розмежувач того, що сесія NHRP на одному інтерфейсі не та що на іншому. Відповідно, зовсім не обов'язково, щоб Network ID збігалися на різних маршрутизаторах.

Налаштування NHRP

Налаштування NHRP на hub-маршрутизаторі

Включення NHRP на інтерфейсі.

Hub-маршрутизатор буде автоматично додавати відповідності між адресами spoke-маршрутизаторів.

(Опціонально) налаштування автентифікації.

Налаштування NHRP на spoke-маршрутизаторах

Включення NHRP на інтерфейсі.

Адреса тунельного інтерфейсу hub-маршрутизатора вказується як next-hop-сервер.

Статична відповідність між адресою mGRE-тунелю й фізичною адресою hub-маршрутизатора (перша адреса – адреса тунельного інтерфейсу, друга – адреса зовнішнього фізичного інтерфейсу).

Адреса зовнішнього фізичного інтерфейсу hub-маршрутизатора вказується як одержувач multicast-пакетів від локального маршрутизатора.

(Опціонально) Налаштування автентифікації.

(Опціонально) Налаштування прапора неунікальності ip-адреси тунелю в базі nhrp на hub-маршрутизаторі.

Якщо зміниться зовнішня адреса spoke-маршрутизатора й цієї команди не буде, то hub-маршрутизатор не обновить свою базу nhrp через помилку: unique address registered already

Перевірка роботи mGRE-тунелів і протоколу NHRP

Перевірка тунельних інтерфейсів

Після того, як на маршрутизаторах настроєні mGRE-тунелі й настроєний протокол NHRP, тунелі перебувають у стані up і всі IP-адреси тунелів доступні.

На dyn5.

Перегляд інформації про тунельний інтерфейс.

З dyn5 пінгується й dyn1 і dyn3.

Перевірка NHRP на spoke-маршрутизаторі

Інформація про NHS.

Сумарна інформація NHRP (уже встановлена динамічний тунель із dyn3).

Докладна інформація про інші маршрутизатори отримана по NHRP.

Одержувач multicast-трафіку.

Сумарна інформація про записи NHRP.

Статистика по пакетах NHRP.

Перевірка NHRP на hub-маршрутизаторі

Сумарна інформація NHRP.

Докладна інформація про інші маршрутизатори отримана по NHRP.

Одержувачі multicast-трафіку.

Сумарна інформація про записи NHRP.

Статистика по пакетах NHRP.

Налаштування маршрутизації

Розглядається використання протоколів EIGRP і OSPF для налаштування маршрутизації між мережами офісів. Для реального використання досить вибрати один із цих протоколів, і виконати відповідні йому налаштування.

Налаштування EIGRP

Якщо як протокол маршрутизації буде використовуватися EIGRP, то необхідно.

- Включити EIGRP для мереж mGRE-інтерфейсів і локальних мереж;
- Відключити автоматичне підсумовування мереж по класовій ознаці;
- Налаштувати EIGRP на mGRE-інтерфейсі.

Включення EIGRP для мереж mGRE-інтерфейсів і локальних мереж.

Відключення автоматичного підсумовування мереж.

Налаштування EIGRP на mGRE-інтерфейсах

Для роботи в мережі DMVPN необхідно додатково налаштувати EIGRP.

На hub-маршрутизаторі необхідно відключити правило розщеплення обрію (split horizon), інакше EIGRP не буде анонсувати маршрути, виучені через mGRE-інтерфейс назад у цей же інтерфейс.

За замовчуванням EIGRP буде підставляти IP-адреса hub-маршрутизатора в якості next-hop для маршрутів які він анонсує, навіть коли анонсує маршрути назад через той же інтерфейс, на якому вони були виучені. Для мережі DMVPN необхідно щоб EIGRP використовував у якості next-hop адреси spoke-маршрутизаторів. Тому на hub-маршрутизаторі необхідно відключити це правило:

При використанні DMVPN у більших мережах час збіжності мережі може збільшуватися. Для того щоб уникнути можливих проблем з маршрутизацією, на маршрутизаторах необхідно змінити hold time (за замовчуванням 15 секунд).

Якщо на одному з маршрутизаторів цей параметр змінений, то сусіди цього маршрутизатора будуть використовувати цей таймер. Для того щоб маршрутизатор сам використовував певне значення таймера, необхідно змінити таймер на відповідному інтерфейсі сусіда.

Перевірка роботи EIGRP

Сусіди EIGRP на dyn1.

Сусіди EIGRP на dyn5.

Таблиця маршрутизації dyn1.

Таблиця маршрутизації dyn3 (мережа 10.1.5.0 доступна через dyn5, а не через dyn1).

Налаштування OSPF

Для OSPF обрана топологія в якій mGRE-інтерфейси перебувають у зоні 0, а локальні мережі – кожна у своїй зоні. Мережа розбита на зони, так як це дозволяє підсумувати мережі усередині зони й не передавати в інші офіси докладну інформацію про мережі (для даного приклада це не актуально, але в реальній мережі може істотно зменшити таблицю маршрутизації й кількість обчислень найкоротшого шляху).

На маршрутизаторах необхідно.

- Включити OSPF для мереж mGRE-інтерфейсів у зоні 0;
- Включити OSPF для локальних мереж у відповідній зоні;
- Налаштувати OSPF на mGRE-інтерфейсі.

Включення OSPF для мереж mGRE-інтерфейсів у зоні 0.

Включення OSPF для локальних мереж у відповідній зоні (офісу за dyn1 відповідає зона 1).

Налаштування OSPF на mGRE-інтерфейсі

Так як mGRE-інтерфейси утворять NBMA-мережа, то на цих інтерфейсах необхідно змінити налаштування OSPF. Докладніше про роботу OSPF в NBMA-мережах на сторінці OSPF в Cisco.

На hub-маршрутизаторі й spoke-маршрутизаторах відрізняються налаштування пріоритетів, інші налаштування збігаються.

Пріоритет інтерфейсу впливає на те, який маршрутизатор буде обраний виділеним маршрутизатором (DR) для мережі. У топології "зірка" роль DR повинен взяти на себе центральний маршрутизатор.

На hub-маршрутизаторі пріоритет установлюється 10.

На spoke-маршрутизаторах пріоритет установлюється 0 для того щоб маршрутизатори не могли брати участь у виборах DR.

Вказівка типу мережі OSPF на mGRE-інтерфейсі.

Зміна інтервалу між відправленням hello-пакетів.

Перевірка роботи OSPF

Сусіди OSPF на dyn1.

Сусіди OSPF на dyn3.

Таблиця маршрутизації на dyn1.

Таблиця маршрутизації на dyn3.

Фази DMVPN

В DMVPN розрізняють три фази або версії: першу, другу й третю. Розглянемо докладніше кожну з них. Як протокол динамічної маршрутизації для наочності будемо використовувати EIGRP.

Перша фаза

У першій фазі допускається динамічне підключення spoke-маршрутизаторів до hub, при цьому вся взаємодія між мережами, розташованими за spoke, ведеться через центр – через hub-маршрутизатор. Тобто в першій фазі неможливо пряма взаємодія між spoke-маршрутизаторами. Всі spoke-маршрутизатори в даній фазі використовують тільки point-to-point тунелі.

До переваг першої фази можна віднести можливість значного скорочення кількості маршрутів, що перебувають у таблицях маршрутизації spoke-пристроїв за рахунок агрегації або фільтрації маршрутів, анонсуємих hub-маршрутизатором. Вирожденим прикладом є анонсування лише дефолтного маршруту з боку hub.

У цьому випадку на spoke-пристроях по EIGRP буде відомий тільки один маршрут.

Перевіримо, що трафік між spoke-маршрутизаторами передається через hub.

До недоліків першої фази ставиться неоптимальний маршрут проходження трафіку між spoke-маршрутизаторами.

Друга фаза

Друга фаза містить у собі оптимізацію шляху проходження трафіку, переданого між spoke-пристроями, за рахунок динамічної побудови тунелів між кінцевими маршрутизаторами, що стає можливим, якщо spoke-маршрутизатори мають повну інформацію про всі префікси в мережі.

Налаштування hub-маршрутизатора повинна задовольняти трьом основним правилам:

– Агрегація мереж або не повинна вироблятися зовсім, або не повинна приховувати реального розташування префіксів;

– На hub-пристрої повинне бути відключене розщеплення обрію;

– Hub-маршрутизатор не повинен підмінювати адресу next-hop, отриманий від spoke-пристрою.

Ніяке додаткове налаштування, що включає підтримку другої фази, не потрібно.

Таблиця маршрутизації spoke-маршрутизатора представлена нижче й містить у собі всі префікси в мережі.

Незважаючи на те, що таблиця маршрутизації містить у собі всі префікси, в CEF не втримується повної інформації про кожну підмережу до моменту передачі першого пакета. Перший пакет убік нової підмережі обробляється процесором і відправляється убік hub-маршрутизатора, після чого завершується формування запису в CEF. До приходу першого пакета запис в CEF позначається як incomplete.

Для завершення формування запису в CEF повинен бути зроблений пошук L2 даних по існуючої L3 інформації. Такий пошук виробляється з використанням протоколу NHRP.

Після завершення роботи протоколу NHRP завершується формування запису в CEF.

Трафік між мережами spoke-маршрутизаторів передається прямо між ними (не через hub).

Перевагом використання другої фази є оптимізація шляхів передачі трафіку між spoke-пристроями. До недоліків можна віднести ріст таблиці маршрутизації на з.

Третя фаза

Третя фаза позбавлена недоліків перших двох фаз, але при цьому володіє їхніми перевагами: трафік передається оптимальним шляхом, при цьому таблиця маршрутизації не зобов'язана містити в собі всі можливі префікси мережі. Домогтися цього вдалося за рахунок приміщення в таблицю маршрутизації тільки тих префіксів, які реально використовуються в цей момент часу. Запис у таблиці маршрутизації з'являється тільки після того, як з'являється трафік, призначений для відповідних одержувачів. Все чарівництво третьої фази стає можливим за рахунок використання опцій redirects і shortcuts. При використанні третьої фази немає необхідності відмовлятися від підсумовування маршрутів (як це було в першій фазі) і не виникає проблеми з адресами next-hop маршрутизаторів (як у другій фазі). По суті hub-маршрутизатор убік spoke-пристроїв може повідомляти єдиний маршрут (наприклад, на мережу 0.0.0.0/0), що відразу ж міститься в CEF. У такий спосіб у третій фазі DMVPN на маршрутизаторах немає частково заповнених записів в CEF, що дозволяє всі пакети (включаючи перший) маршрутизувати із використанням CEF, тобто без використання процесора.

Розглянемо процес передачі даних між двома spoke-маршрутизаторами. Перший пакет передається убік hub-пристрою відповідно до таблиці маршрутизації, після чого hub-маршрутизатор через той же тунельний інтерфейс відправляє пакет убік маршрутизатора

одержувача. Така подія (відправлення пакета через той же інтерфейс, через який він був отриманий) змушує hub-маршрутизатор відправити повідомлення redirect, що означає, що трафік передається не самим оптимальним шляхом. Включення можливості відправлення hub-маршрутизатором повідомлень NHRP redirect включається за допомогою команди ip nhrp redirect, що вводиться в режимі налаштування тунельного інтерфейсу.

Одержавши повідомлення redirect spoke-маршрутизатор відправляє повідомлення NHRP request, за допомогою якого намагається з'ясувати, NBMA адреса пристрою, за яким розташований одержувач. Повідомлення NHRP request передається через hub убік другого spoke-пристрій, що і відповідає на запит. Одержавши відповідь на відповідний запит, spoke-маршрутизатор додає новий запис у таблицю маршрутизації й використовує неї для пересилання трафіку. Для включення опції redirect на тунельних інтерфейсах spoke-пристроїв повинна бути уведена команда ip nhrp shortcut.

Трафік між spoke-пристроями передається прямо, тобто минаючи hub-маршрутизатор.

У виводі debug-повідомлень на spoke-маршрутизаторі одержання пакета nhrp redirect називається «NHRP: Receive Traffic Indication», тоді як відправлення повідомлення nhrp request можна розпізнати по фразі «NHRP: Sending NHRP Resolution Request for dest».

Налаштування IPsec

Перша фаза (налаштування IKE)

Для тестової мережі в політику isakmp використовуються налаштування за замовчуванням.

- Алгоритм шифрування: DES – Data Encryption Standard (56 bit keys).
- Алгоритм хешування: Secure Hash Standard.
- Метод автентифікації: Rivest-Shamir-Adleman Signature.
- Група Diffie-Hellman: #1 (768 bit).
- Час життя SA: 86400 seconds, no volume limit.

Автентифікація по pre-shared key

У політику з автентифікацією по pre-shared key, метод автентифікації змінений, так як за замовчуванням використовується автентифікація по сертифікатах. Інші параметри використовують значення за замовчуванням.

Створити політику isakmp.

Так як адреса peer заздалегідь не відома й може бути отриманий динамічно, те при налаштуванні pre-shared key необхідно вказувати шаблонову адресу (wildcard address).

Налаштувати isakmp pre-shared key.

Автентифікація по сертифікатах

Автентифікацію по pre-shared key не рекомендується використовувати для DMVPN, так як pre-shared key повинен бути зазначений із шаблоновою адресою, і немає прив'язки до адреси маршрутизатора з яким установлюється тунель.

У тестовій мережі hub-маршрутизатор буде виконувати роль центра сертифікатів. Всім маршрутизаторам видані сертифікати.

Більш докладно про налаштування центра сертифікатів на маршрутизаторі Cisco і процедурі видачі сертифікатів маршрутизаторам на сторінці Центр сертифікатів на маршрутизаторі Cisco.

Створити політику isakmp (так як за замовчуванням використовується автентифікаціях по сертифікатах, то в тестових цілях можна залишити всі налаштування політики за замовчуванням).

Друга фаза (налаштування IPsec-профілю)

Так як hub-маршрутизатор не знає заздалегідь IP-адреси spoke-маршрутизаторів, то для другої фази IPsec потрібна динамічна crypto map (dynamic crypto map), але для тунельних інтерфейсів еквівалентом dynamic crypto map є IPSec-profile.

- застосовується на тунельному інтерфейсі;

– після застосування будь-який трафік вихідний з тунельного інтерфейсу ініціює створення IPsec-тунелю (немає необхідності використовувати ACL, як у звичайної crypto map);

– source і destination адреси тунельного інтерфейсу використовуються для створення IPsec-тунелю. Адреси можуть бути прописані в налаштуваннях інтерфейсу або отримані динамічно за допомогою NHRP (не задається адреса peer, як у звичайної crypto map);

Створюємо transform set.

Так як mGRE-інтерфейс забезпечує створення тунелю, то IPsec можна перевести в транспортний режим (за замовчуванням використовується тунельний режим).

Створити IPSec-профіль.

Застосування IPsec-профілю

Застосування IPsec-профілю на mGRE-інтерфейсі.

Перевірка роботи IPsec

Перевірка роботи IKE з автентифікацією по pre-shared key

Перевірка isakmp SA на dyn1.

Перевірка isakmp SA на dyn3 до установки тунелю spoke-to-spoke.

Перевірка isakmp SA на dyn3 після установки тунелю spoke-to-spoke. Для цього досить просто пропінгувати тунельний інтерфейс сусіднього spoke-маршрутизатора (але пакетів icmp бажано послати штук 10).

Більше докладна інформація про isakmp SA (автентифікація по pre-shared key).

Перевірка роботи IKE з автентифікацією по сертифікатах

Перевірка isakmp SA на dyn1.

Перевірка isakmp SA на dyn3 до установки тунелю spoke-to-spoke.

Перевірка isakmp SA на dyn3 після установки тунелю spoke-to-spoke. Для цього досить просто пропінгувати тунельний інтерфейс сусіднього spoke-маршрутизатора (але пакетів icmp бажано послати штук 10).

Більше докладна інформація про isakmp SA (автентифікація по сертифікатах).

Перевірка роботи IPsec

Перегляд інформації про crypto map на dyn1.

Перегляд інформації про crypto map на dyn3 до створення динамічного тунелю з dyn5.

Перевірка IPsec SA на dyn1.

Перевірка IPsec SA на dyn3 після установки тунелю spoke-to-spoke.

Перегляд інформації про DMVPN мережі

Так як на маршрутизаторі dyn3 запису різних типів – динамічна й статична, те вся інформація перевіряється на ньому.

У деяких версіях IOS може не бути команди show dmvpn. Вона з'явилася в Cisco IOS 12.4(9)T.

Перегляд інформації про DMVPN.

Більше докладна інформація про DMVPN до застосування IPsec profile.

Більше докладна інформація про DMVPN після застосування IPsec profile.

Конфігурації маршрутизаторів

У конфігураційних файлах збережені всі налаштування.

– Різні протоколи динамічної маршрутизації.
– OSPF;
– EIGRP;
– Різні методи автентифікації.
– по pre-shared key;
– по сертифікатах.

Для реального використання досить вибрати один із протоколів маршрутизації й метод автентифікації.

Так як в EIGRP AD (administrative distance) менше, ніж в OSPF, те при використанні обох протоколів, у таблиці маршрутизації будуть маршрути EIGRP.

Так як в політики isakmp, що використовує автентифікацію по сертифікатах, на всіх маршрутизаторах номер менше ніж у політики з pre-shared key, те при використанні обох політик, автентифікація буде проводитися по сертифікатах.

Конфігурація hub-маршрутизатора (dyn1)

Конфігурація spoke1 (dyn3)

Конфігурація spoke2 (dyn5)

DMVPN і crypto-map на одному інтерфейсі

Удалося подружити DMVPN і crypto-map на одному інтерфейсі використовуючи ISAKMP Profile.

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/prod_white_paper0900aecd8034bd59.html

Додаткові налаштування

Описуємо ключі для кожного з бенкетів.

Формуємо новий ISAKMP профіль

Додаємо ще один transform-set

Формуємо crypto map використовуємо crypto isakmp profile MyISaPROF

Заводимо access-list з дозволом на кожну підмережу за кожним бенкетом

І найпростішому підвішуємо crypto map на зовнішній інтерфейс

Не забуваємо маршрути на мережі за VPN

Начебто все. Громіздко, статично, якщо багато бенкетів те й писати багато. Але дозволяє підключити до Cisco будь-яку залозку (dlink, tplink та ін. супербренди).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN.Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Досліджена система забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Розроблені алгоритми дозволяють успішно вирішувати завдання забезпечення обміну інформацією у корпоративній мережі на базі технології DMVPN. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С.

Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

Ю. Окаєвич, магістр гр. КН-20МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО РОЗПОДІЛУ КЛЮЧІВ

У статті розроблено програмне забезпечення, яке призначено для системи централізованого розподілу ключів. Метою розробки є дослідження та програмна реалізація системи централізованого розподілу ключів. Об’єктом дослідження є процес централізованого розподілу ключів. Предметом дослідження є методи централізованого розподілу ключів. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи централізованого розподілу ключів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерні науки, розподіл ключів

Постановка проблеми. На сучасному етапі розвитку систем передачі даних, особливо гостро стоїть питання забезпечення захисту інформації, що передається по каналах зв'язку цих систем. У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти пропонується до розгляду захист інформації в банківській мережі. Для забезпечення захищеності даних, які передаються по даній мережі, у банківських мережах регулярно відбувається зміна ключів. Формуванню системи централізованого розподілу ключів й присвячена випускна кваліфікаційна робота за другим (магістерським) рівнем вищої освіти.

Ця проблема є дуже актуальною та важливою, в зв’язку з тим, що в банківський мережі за день проходить кілька десятків тисяч транзакцій, і якщо зловмисник зможе взломати систему розподілу ключів, то банк понесе колосальні втрати [1]. При цьому виникає питання не тільки фінансових втрат, а й питання втрати іміджу банку. Тобто, якщо з вини служби безпеки банку, яка не зуміла забезпечити необхідний рівень захисту системи розподілу ключів, відбудеться взлом цієї системи, то у банка буде підмочена репутація і

клієнти оберуть інший банк для проведення операцій з готівковими та безготівковими операціями.

Для забезпечення стійкості системи необхідно забезпечити захист наступних компонент цієї системи: центру сертифікації, формування й розподілу ключів (ЦСФРК), серверів розподіленої обробки й користувальницькі пристрої [2].

При цьому необхідно комплексно вирішувати проблему захисту інформації, тобто, враховувати не тільки загрози зі сторони взлому програмного забезпечення, а й забезпечувати фізичний, правовий та технічний рівень захисту вищеперерахованих елементів системи [3-6].

Розроблена в статті система повинна забезпечувати можливість ефективного, з гарантованою надійністю обміну закритою інформацією. Кожний сертифікований користувач, звернувшись до центру сертифікації, формування й розподілу ключів, повинен змогти обмінюватися закритою інформацією з будь-яким сервером або користувачем банківської мережі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні Дослідження та програмна реалізація системи централізованого розподілу ключів”

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи централізованого розподілу ключів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

Огляд існуючих систем централізованого розподілу ключів.

Дослідження системи централізованого розподілу ключів.

Програмна реалізація системи централізованого розподілу ключів.

Об’єктом дослідження є процес централізованого розподілу ключів.

Предметом дослідження є методи централізованого розподілу ключів.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення

Виклад основного матеріалу. Синтез одноразової системи з відкритою передачею ключів

Характерна риса одноразової системи шифрування – одноразове використання ключової послідовності. Така система шифрує вихідний відкритий текст X у шифротекст Y з використанням одноразової випадкової ключової послідовності K. Для її реалізації іноді використовують одноразовий блокнот, складений з відривних сторінок; на кожній з них надрукована таблиця з випадковими числами (ключами) Ki. Блокнот виконується у двох екземплярах: один використовується відправником, а інший – одержувачем. Для кожного символу Xi повідомлення є свій ключ Ki з таблиці одержувача. Після того, як таблиця використана, її необхідно видалити із блокнота й знищити. Шифрування нового повідомлення починається з нової сторінки.

Абсолютна надійність одноразової системи доведена Клодом Шенноном. Одноразові системи нерозкриваємі, оскільки їх шифротекст не містить достатньої інформації для відновлення відкритого тексту. Однак можливості використання одноразових систем на практиці обмежені. Ключова послідовність довжиною не менш довжини повідомлення повинна передаватися одержувачеві повідомлення заздалегідь або окремо по деякому секретному каналі, що практично нездійсненно в сучасних банківських системах, де потрібно шифрувати багато мільйонів символів і забезпечувати засекречений зв'язок для безлічі абонентів. Ці недоліки усунуті в способі синтезу одноразових систем шифрування з відкритим поширенням ключа.

Розглянемо процес передачі інформації з лінії зв'язку, що з'єднує сервер банківської мережі (сторона А) та клієнтську ЕОМ банківської мережі (сторона В). Пропонований спосіб побудови одноразової системи дає можливість передавати практично необмежений обсяг інформації з використанням випадкової перестановки тільки однієї таблиці ключів.

У якості базового елемента, що шифрує, для системи з відкритою передачею ключів розроблений одноразовий багатоалфавитний кодер (ОБК). Система містить ОБК, датчик випадкових чисел, схему формування випадкової перестановки на стороні А и багатоалфавитний декодер на стороні В ОБК реалізується процес стохастичного кодування

До складу ОБК входить базова таблиця одноразових ключів, регістр перестановки інтерфейсу, регістри випадкової й псевдовипадкової перестановок рядків і стовпців базової таблиці. Аналогічний состав має й багатоалфавитний декодер. Регістри випадкових і псевдовипадкових перестановок рядків і таблиці інтерфейсу декодера містять комбінації, зворотні стосовно відповідних перестановок кодера.

Базова таблиця одноразових ключів на стороні A и на стороні B має розмір n x n. Кожний і-ий рядок таблиці містить випадкову ключову комбінацію, у яку входять всі можливі різні значення K_{ij} довжиною m біт. (Для таблиці кодів ASCII $m = 8$, $n = 256$, тому для шифрування тексту використовують таблицю розміром 256 x 256.)

$K_i = K_{i0}, K_{i1}, ..., K_{in-1}$ $(i = 1,...,n)$

У результаті роботи датчика випадкових чисел i схеми формування випадкової перестановки генерується відповідна перестановка. В отриманій перестановці стовпці задають відповідність між вхідними значеннями (верхній рядок) і вихідними (нижній рядок).

Базова таблиця одноразових ключів на стороні A виконує дві функції:

– генерацію віртуальної змінної таблиці одноразових ключів з випадковою перестановкою стовпців і рядків;

– реалізацію логічного виводу, що забезпечує перетворення секретної перестановки в несекретну, застосовувану для відкритої передачі ключа.

Із цією метою кожний стовпець базової таблиці можна представити у вигляді вертикально розташованої перестановки. При цьому регістр псевдовипадкової перестановки, підключений до даної таблиці, у сполученні з попередньою випадковою перестановкою, що передана на сторону В, забезпечує вибір стовпців таблиці для формування їхніх одноразових комбінацій. Названі комбінації стовпців застосовуються в процесі логічного виводу. Усього може бути сформоване $N = n!$ різних комбінацій стовпців.

Логічний вивід реалізує односпрямовану функцію $Y = F(x)$, що дозволяє на основі секретної перестановки, записаної в лівий регістр базової таблиці одноразових ключів, одержати несекретну перестановку, формовану у вихідному блоці ОБК. Тут x – значення секретної перестановки, F – функціональні зв'язки, формовані в процесі логічного виводу з використанням чергової комбінації стовпців-перестановок, Y – відносна несекретна перестановка. Знаючи x і формуючи функціональні зв'язки F, легко одержати Y. Однак за відомим значенням Y, не знаючи всієї схеми функціональних зв'язків базової таблиці, не можна відновити вихідну секретну перестановку. Для цього необхідно зробити повний перебір на безлічі $V = n!$ всіх значень результуючих перестановок, одержуваних у ході логічного виводу, – свого роду ефект лабіринту, у центр якого поміщають людину із зав'язаними очами й, знявши пов'язку, пропонують шляхом випадкового перебору всіх можливих варіантів проходу знайти вихід.

У результаті виконання n процедур логічного виводу буде сформована таблиця несекретної перестановки, яка буде використовуватися в процесі шифрування для відкритої передачі ключа.

Таким чином, одночасно з передачею й шифруванням інформації на стороні користувача A генерується чергова випадкова перестановка. Потім за допомогою описаного алгоритму логічного виводу формується відповідна їй несекретна перестановка. Вона передається на сторону B у початку обміну інформацією й після передачі по лінії зв'язку n блоків шифротексту довжиною n символів кожний. На основі цієї перестановки на стороні B с допомогою базової таблиці, ідентичній базовій таблиці A, виконується процедура зворотного логічного виводу з метою одержання відповідної секретної перестановки (рис. 3.2). Ця процедура описується вираженням $x = F^{-1}(Y)$, де F^{-1} – функція зворотного логічного виводу, реалізованого за допомогою базової таблиці сторони B. Сформована секретна

перестановка записується в регістри випадкових перестановок стовпців і рядків багатоалфавитного декодера. Шляхом використання зазначених регістрів у декодері відбувається утворення віртуальних таблиць одноразових ключів відповідно до отриманої випадкової перестановки. У результаті на сторонах *A* и *B* щораз будуть одночасно сформовані нові випадкові віртуальні таблиці одноразових ключів, ідентичних по змісту. Ці таблиці застосовуються при передачі зашифрованої інформації.

Розглянемо цей процес докладніше. Вихідний текст надходить на вхід регістра перестановки інтерфейсу ОБК, що забезпечує перестановку таблиці кодів ASCII. Так здійснюється перший етап перетворення вихідної інформації. Потім перетворений текст проходить через регістр випадкової перестановки рядків, що у сполученні з випадковою перестановкою стовпців реалізує чергову віртуальну таблицю одноразового ключа. При цьому застосування випадкових і псевдовипадкових перестановок забезпечує для кожної чергової комбінації вихідного тексту $X_i = (X_{i0}, X_{i1}, ..., X_{in-1})$ ($i = 1,...,n$) формування унікальної одноразової ключової послідовності $K_i = K_{i0}, K_{i1}, ..., K_{in-1}$ ($i = 1,..,n$). Усього для даної віртуальної таблиці, обумовленою черговою випадковою перестановкою, може бути утворено n таких ключових послідовностей. У результаті зроблених перестановок і замін у багатоалфавитному кодері символів кожної чергової послідовності X_i, а також циклічних зрушень стовпців таблиці, процес шифрування аналогічний класичній одноразовій системі. У декодері спочатку реалізується процедура ідентифікації символів шифротекста шляхом включення відповідних стовпців базової таблиці, а потім виробляються відповідні циклічні зрушення стовпців і за допомогою регістрів перестановок рядків виконуються зворотні перестановки, що забезпечують перетворення шифротекста у вихідний текст.

Після передачі $i = n$ чергових комбінацій шифротекста реалізується описаний процес відкритої передачі ключа (чергової секретної перестановки). За рахунок цього виробляється постійна (із заданим періодом) випадкова модифікація віртуальної таблиці багатоалфавитних кодера й декодера для одержання нових таблиць одноразових ключів. Потім триває передача, шифрування й дешифрування інформації з використанням нових таблиць одноразових ключів. При цьому передача несекретної перестановки реалізує функцію відкритої передачі ключів, виробленої після видачі кожних n блоків зашифрованої інформації. У результаті забезпечується гарантована надійність шифрування. Дійсно, самі базові таблиці одноразових ключів супротивникові невідомі при будь-яких видах атак на дану систему шифрування (у явному виді вони не беруть участь у процесі шифрування інформації), тому формовані віртуальні таблиці одноразових ключів випадкові й непередбачені. З огляду на односпрямованість функції $Y = F(x)$ одержання несекретної перестановки, безліч варіантів модифікації віртуальних таблиць на сторонах *A* и *B* шляхом випадкової перестановки стовпців і рядків виміряється числом $V = n!$ Так, при використанні таблиці кодів ASCII із зазначеними параметрами m і n одержимо величину $V > 10^{500}$. Для більших значень *n* даний спосіб дозволяє передавати практично необмежені обсяги зашифрованої інформації в режимі одноразового ключа з гарантованим рівнем надійності, обумовленим числом $V = n!$ всіх можливих значень результуючих перестановок, які одержують у ході логічного виводу. Відзначимо, що в цьому випадку застосовується одна таблиця одноразових ключів розміром $n \times n$ і функція відкритої передачі ключів з використанням випадкової несекретної перестановки довжиною *n* байт. Важко навіть указати, скільки часу буде потрібно на перебори всіх варіантів перестановок на реальному комп'ютері. При цьому функція відкритої передачі ключів може періодично використовуватися для відновлення базової таблиці шляхом передачі нових значень її стовпців (перестановок). Зазначені значення стовпців генеруються за допомогою датчика випадкових чисел і схеми формування випадкових перестановок. У результаті після n циклів відновлення на сторонах *A* и *B* будуть отримані нові базові таблиці, використовувані далі при шифруванні.

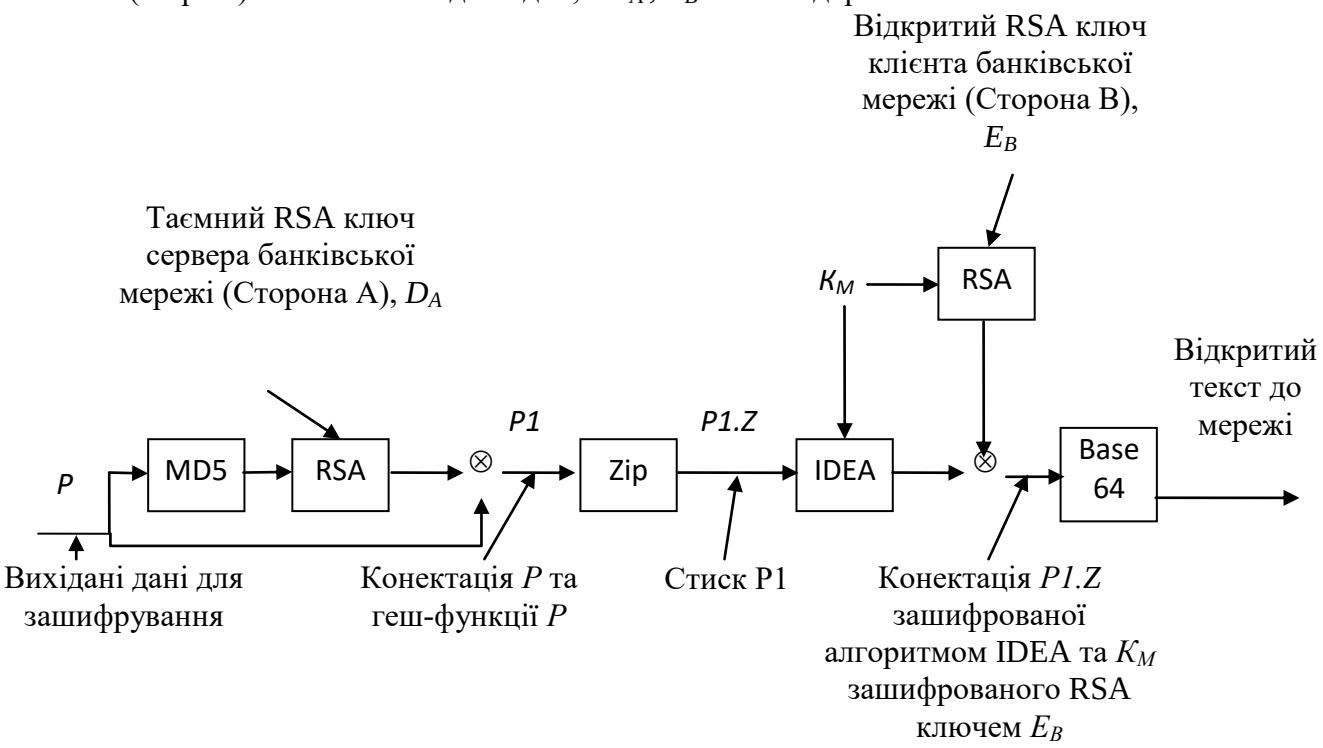
Процес кодування в ОБК практично не знижує швидкість передачі інформації з каналу зв'язку. Це дозволяє реалізувати швидкісні одноразові шифри для роботи в

банковських мережах. Є ефективні технології забезпечення цілісності інформації, а також ідентифікації й автентифікації користувачів, перевірки дійсності повідомлень.

Алгоритм розподілу ключів на основі PGP

На основі алгоритму RSA розроблена програма PGP (Pretty Good Privacy). Це повний пакет безпеки, що включає засобу конфіденційності, установлення дійсності, електронного підпису, стиску й все це в зручній для використання формі. Завдяки цьому система працює як на платформі Unix, так і MS-DOS/Windows, Macintosh і поширюється безкоштовно, тому вона одержала дуже широке поширення.

PGP використовує алгоритми шифрування RSA, IDEA і MD5. PGP підтримує компресію, переданих даних, їхню таємність, електронний підпис і засоби управління доступу до ключів. Схема роботи PGP показана на рисунку 3.3. На цьому рисунку – D_A, D_B особисті (закриті) ключі A и B відповідно, а E_A , E_B – їхні відкриті ключі.



K_M – одноразовий ключ для зашифрування повідомлення IDEA
⊗ – конектація

Рисунок 1 – Алгоритм шифрування при розподілу ключей PGP

Відзначимо, що секретний ключ для IDEA будується автоматично по ходу роботи PGP на стороні A и називається ключем сесії – K_M, що потім шифрується алгоритмом RSA з відкритим ключем користувача B. Так само варто звернути увагу на те, що повільний алгоритм RSA використовується для шифрування коротких фрагментів тексту: 128 біт MD5 і 128 біт IDEA ключа.

PGP підтримує три довжини ключів:

– Звичайний – 314 біт (може бути розкритий за рахунок більших витрат).

– Комерційний – 512 біт (може бути розкритий спеціалізованими організаціями, назви яких, як правило, складається із трьох букв).

– Військовий – 1024 біта (не може бути розкритий поки ніким на землі).

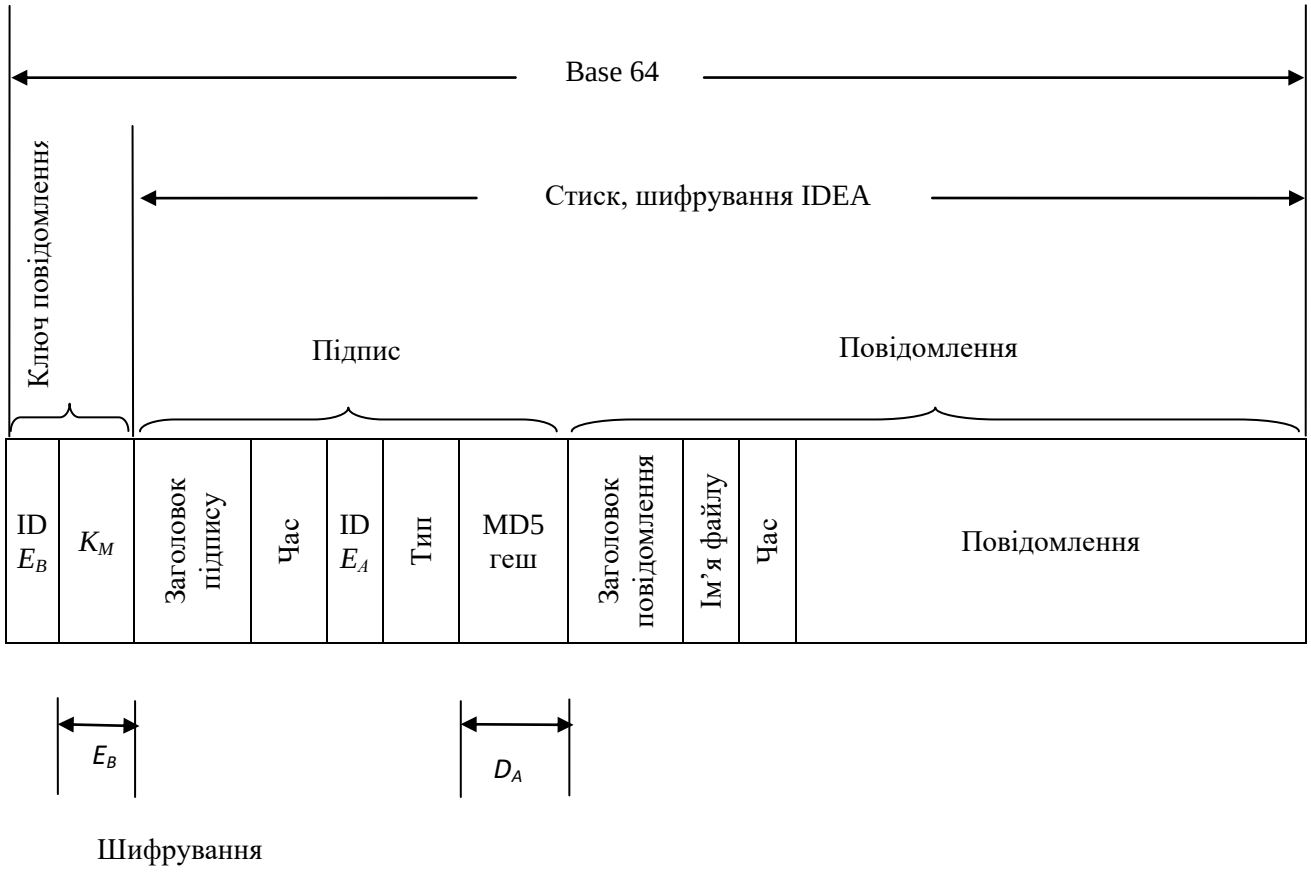


Рисунок 2 – Структурна схема PGP

Розподіл ключів. Web of Trust

Кожний користувач PGP може самостійно згенерувати свій ключ. Кожний користувач може привласнити ключу будь-яке ім'я й будь-який e-mail-адресу. Все це відкриває широкий простір для шахрайства й атак по методу "людина у середині". Щоб переконатися, що конкретний ключ дійсно належить передбачуваному власникові, потрібно якось це перевірити. Це неважко, якщо ви особисто знайомі з людиною, у противному ж випадку може виявитися досить складним. Основний з механізмів, пропонованих PGP для рішення цієї проблеми – це *цифрові сертифікати ключів* і модель відносин довіри *Web of Trust.*

Сертифікат відкритого ключа PGP – це форма посвідчення, що несе ідентифікацію користувача (тобто об'єктивний спосіб його впізнавання), і пов'язана з певним відкритим ключем за допомогою підтверджувального підпису третьої сторони – підпису поручителя. На сьогоднішній день не існує устояного визначення підтверджувального підпису. Такий підпис на сертифікаті ключа може мати приблизно наступне значення: *"Я поручаюся в тім, що підписаний мною ключ дійсно належить особі, зазначеній у відомостях (ідентифікації) сертифіката".* Таке значення, на жаль, не можна вважати достатнім і повним.

Тому більш точне значення підтверджувального підпису звучить так: *"Я поручаюся, ґрунтуючись на своїй особистій безпосередній переконаності й об'єктивних підтверджувальних свідченнях, у тім, що підписаний мною відкритий ключ і пов'язаний з ним закритий ключ дійсно належать особі, чиє ім'я, e-mail і інші ідентифікаційні відомості зазначені в сертифікаті ключа".* Щоб дати такий підтверджувальний підпис, поручитель зобов'язаний упевнитися в наступному (у наведеній послідовності): ключ індивідуальний і унікальний. Для цього власник ключа повинен повідомити його цифровий відбиток; зазначений у сертифікаті ключа людина (ім'я, фото) є тої, за кого себе видає. Звичайно із цією метою перевіряють персональні документи державного зразка або інше надійне посвідчення особи з фотографією; власник відкритого ключа має відповідний закритий

ключ. Якщо він може розшифрувати зашифрований текст даним відкритим ключем і згенерувати цифровий підпис, що звіряється даним відкритим ключем, значить він володіє й відповідним закритим ключем; у сертифікаті зазначені приналежному власникові ключа контактні координати. Він повинен довести, що має повний доступ до цих координат для одержання й відправлення повідомлень.

Але навіть якщо поручитель завірив своїм підписом сертифікат і ключ, маючи на увазі саме таке значення своєго підтведжуючого підпису, однаково ряд питань залишаються відкритими: яким документом власник ключа засвідчив свою особистість, чи надійний цей документ, чи було посвідчення особи справжнім, чи не був закритий ключ скомпрометований і викрадений? Ці питання впритул підводять нас до критерію довіри в середовищі асиметричних криптосистем і до розподіленої моделі довіри PGP *Web of Trust.*

Моделі довіри в криптосистемах з відкритим ключем діляться на два великих види: централізовані й розподілені. У централізованих, або ієрархічних, моделях всі користувачі системи покладаються на довіру до одного кореневого джерела, що підтверджує вірогідність всіх відкритих ключів. Така модель звичайно застосовується в корпоративному середовищі (де єдине джерело довіри обов'язкове) і в системах центрів, що засвідчують, на базі стандарту X.509, хоча бувають і виключення, наприклад, центр, що засвідчує, Thawte Consulting, що реалізує, як схему з єдиним сервером-зберігачем ключів, так і розподілену модель PGP, також називану мережею довіри.

У такій системі немає єдиного джерела сертифікації, навпроти, кожний користувач самостійно вирішує, кому він довіряє, а кому не довіряє в посвідченні інших відкритих ключів, створюючи тим самим особисту мережу поручителів. Такий підхід забезпечує гнучкість і стійкість системи до будь-якого зловмисного впливу: можна вплинути на один вузол розподіленої системи, але тисячі інших вузлів збережуть повну надійність.

Загальна проблема всієї асиммтеричной криптографії – складність перевірки автентичності відкритих ключів. Непросто з достатньою точністю визначити, що конкретний відкритий ключ є справжнім і належить передбачуваному власникові, і ще сутужніше це в середовищі PGP, де немає єдиного джерела сертифікації ключів, як в умовах інфраструктур PKI (Personal Key Infrastructure). З іншого боку, розподілена природа моделі довіри PGP має й свої переваги.

Наведена в PGP схема досить складна й багата на несполучені ланцюжки сертифікації. Несполученими ланцюжками називаються такі, які не мають загальних ланок поручителів. Чим більше таких паралельних шляхів поручництв, тим менше ймовірність, що підозрілий ключ недостовірний: малоймовірно, щоб відразу кілька людей у такому випадку поручилися за його дійсність.

Щоб мати можливість знаходити такі комплексні ланцюжки, дуже важливо, щоб користувачі перевіряли дійсність ключів своїх кореспондентів, завіряли їхніми підписами й обновляли на сервері. В остаточному підсумку це буде благом для всіх. Такі взаємні поручництва утворять свого роду мережа, саме тому модель довіри PGP називається Web of Trust – Мережа довіри.

Усякий відкритий ключ на своєму зв'язуванні ви можете наділити деяким ступенем довіри в сертифікації інших ключів. Це значить, що якщо до вас у руки потрапить ключ *Б*, підписаний ключем А, що підтверджує підпису якого ви цілком довіряєте, ключ *Б* буде розцінений споконвічно достовірним, рятуючи вас від необхідності перевіряти його дійсність самостійно.

Інтегральним показником критеріїв довіри є ранг ключа в Мережі довіри, заснований на індексі MSD. Всім цим процедура наділення довірою істотно відрізняється від сертифікації ключа, коли ви повинні оцінити тільки його взаємозв'язок з передбачуваним власником, але не особистісні якості власника ключа.

Розглядаючи схему несполучених ланцюжків, намагаючись визначити дійсність підозрілого ключа, обов'язково переконаєтесь, що в складі проміжних ланок є хоча б кілька

людей, яким ви довіряєте в сертифікації ключів. Якщо ланцюжок сертифікації не містить довірених поручителів, ви не повинні покладатися на неї як на оцінний критерій.

Чим більше взаємних перехресних підписів, що сертифікують, буде акумульовано в Мережі довіри, тим коротше почнуть ставати ланцюжки сертифікації, і тем вище стане загальна переконаність у дійсності всякого ключа. Ключі, надійно зв'язані безліччю коротких ланцюжків, що засвідчують, називаються міцним набором. Кількість цих ключів у цей час становить приблизно 25 тисяч, і саме вони утворять стрижень і ядро всієї Мережі довіри, або зв'язкового набору – ключів, що мають хоча б один ланцюжок сертифікації від міцного набору. Зв'язний набір вичерпується приблизно 70 тисячами ключів, при цьому в названі 70 тисяч входять 25 тисяч ключів міцного набору. Ключі зі зв'язного набору, що не входять у міцний набір, називають периферійним набором (порядку 45 тисяч).

На суспільних серверах Інтернету зберігається біля двох мільйонів відкритих ключів, які утворять "міцні зв'язування". Більшість із них не має підписів, що сертифікують; деякі мають підпис, але не від ключів, що входять у мережу довіри банку. Такі невеликі групи взаємопідписаних ключів і ключі, що не мають підтверджувальних підписів, називаються ізольованим набором. Вони не враховуються в статистику мережі довіри банку, і визначити їхню дійсність по методу аналізу ланцюжків сертифікації неможливо. Якщо ж будь-який власник ключа зі зв'язного набору (клієнт банку) перевірить надійність одного з ізольованих ключів і підпише його, що підтверджує підпис виявиться сполучною ланкою, що веде до серця міцного набору, і ця група ізольованих ключів відразу увіллється в мережу довіри.

Сервери, або депозитарії, ключів OpenPGP, – це відкриті бази даних, прості сховища сертифікатів. Щоб спростити клієнтським частинам банківських мереж завдання знаходження відкритого ключа, можно завантажити його на сервер. Аналогічно, коли виникне потреба відправити на банківський сервер зашифрований лист, просто користуються формою пошуку для знаходження його відкритого ключа в базі.

Крім завантаження й пошуку ключів, зведена статистика мережі довіри PGP Web of Trust, а також базовані на ній спеціальні механізми відстеження шляхів сертифікації ключів і оцінки "авторитетності" і "ваги" будь-якого ключа в системі Web of Trust. Механізм відстеження шляхи сертифікації дозволяє встановити ланцюжок підписань від ключа банківського сервера до ключа клієнтської частини банківської мережі, виявляючи всі проміжні ланки поручителів. Це один з допоміжних методів визначення дійсності й вірогідності конкретного ключа. Аналіз і оцінка положення ключа в системі Web of Trust також дозволяє визначити, як давно ключ циркулює в банківській мережі, наскільки вагомим можна вважати його підпис, що сертифікує, і т.д.

Розробка структурної схеми

Розглянемо основні положення які реалізовані в даній роботі – структурна схема роботи системи зображена на рисунку 3

До складу системи з відкритим розподілом ключів входять центр сертифікації, формування й розподілу ключів (ЦСФРК), сервери розподіленої обробки й користувальницькі пристрої.

Основними завданнями ЦСФРК є підключення користувальницьких пристроїв і серверів до системи захисту, їхня сертифікація, формування й розподіл закритих і відкритих ключів між користувальницькими пристроями й серверами розподіленої обробки даних.

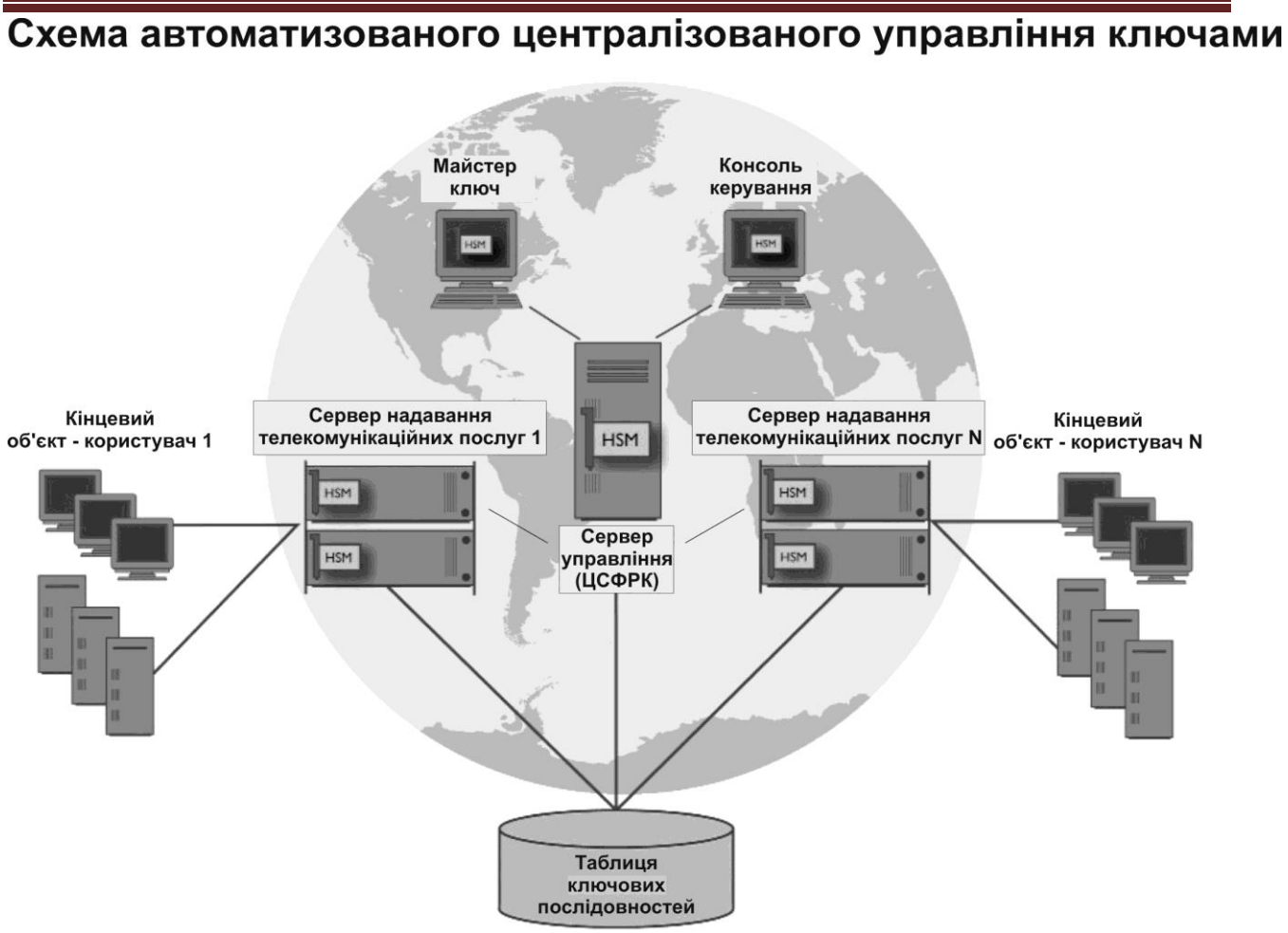


Рисунок 3 – Структурна схема роботи системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів централізованого розподілу ключів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем централізованого розподілу ключів. Досліджена система централізованого розподілу ключів. На основі отриманих результатів досліджень створена програмна реалізація системи централізованого розподілу ключів. Розроблені алгоритми дозволяють успішно вирішувати завдання централізованого розподілу ключів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения

компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

Д. Немировський, магістр гр. КІ-20М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ МЕРЕЖЕВИХ ПРИНТЕРІВ

У статті розроблено програмне забезпечення, яке призначено для системи моніторингу мережевих принтерів. Метою розробки є дослідження та програмна реалізація системи моніторингу мережевих принтерів. Об'єктом дослідження є процес моніторингу мережевих принтерів. Предметом дослідження є методи моніторингу мережевих принтерів. Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи моніторингу мережевих принтерів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, моніторинг, мережеві принтери

Постановка проблеми. Мабуть самими неконтрольованими та невидимими витратами в організаціях, які використовують сучасні комп'ютерні технології та електронний документообіг, є витрати на друк документів (включаючи витрати на папір, апаратне обладнання та тонер). Аналіз цього питання, проведений в період переддипломної практики, виявив наступні результати: вартість виготовлення документів складає біля 40 % трудових витрат відповідних відділів фірми, які використовують документообіг в електронному вигляді та роздруковують документи на паперових носіях інформації.

Багато адміністраторів і керівників неоднократно зіткалися з необхідністю контролю ефективності використання принтерів в організації і намагалися провести такий контроль власними силами. Але дуже непросто відстежити тих співробітників, які постійно

витрачають запаси паперу і тонера, призначені для всього відділу, на друкування паперів для власних потреб.

Якщо організація надає обчислювальні послуги по роздрукуванню текстових і інших документів, то перед нею неминуче встане проблема тарифікації, безпосередньо пов'язана з автоматичним обліком ресурсів. Особливо організація питання моніторингу ускладнюється, якщо принтер не один і більшість з них знаходиться в мережі, локальній чи корпоративній.

Проте на сьогодення організація моніторингу роботи принтерів все ще залишається на етапі мінімальної автоматизації. Про це свідчать результати проведеного під час переддипломної практики експрес-аналізу програмного ринку країни. Тому розробка програмного забезпечення системи, яка відстежувала б, хто, коли і скільки надрукував, яку до того ж можна буде інтегрувати в систему контролю організації, є задачею дійсно актуальною. Адже це не тільки позбавило б адміністраторів від зайвого діалогу з власними співробітниками та клієнтами, але і надало б фірмі сучаснішого вигляду.

Таким чином, враховуючи вищеозначене, розробка автоматизованих комп’ютерних систем, які забезпечать моніторинг роботи принтерів в мережі на основі використання сучасних технологій, на сьогодення є питанням надзвичайно перспективним та нагальним. Адже такі системи можуть будуть корисними та незамінними в будь-яких галузях народного господарства країни та будь-якій сфері діяльності людини.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи моніторингу мережевих принтерів

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи моніторингу мережевих принтерів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем моніторингу мережевих принтерів.
– Дослідження системи моніторингу мережевих принтерів.
– Програмна реалізація системи моніторингу мережевих принтерів.

Об’єктом дослідження є процес моніторингу мережевих принтерів.

Предметом дослідження є методи моніторингу мережевих принтерів.

Методи дослідження базуються на методах теорії комп’ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Предметом розробки ВКРМ є програмне забезпечення моніторингу мережевих принтерів.

Як результат роботи очікується система моніторингу мережевих друкуючих пристроїв, яка може бути використана як незалежна система або може бути інтегрованою для роботи в іншій системі аналогічного класу та спрямування.

Основною задачею розробки ПЗ є створення програмної моделі системи, яка в процесі промислової експлуатації буде виконувати наступні функції:

– проводити моніторинг мережевих ДРП в фоновому режимі з заданою періодичністю 500 мс (інтервал моніторингу може бути змінений замовником);
– визначити необхідну інформацію про кожне надруковане завдання:
– ім'я користувача;
– ім'я комп'ютера;
-- ім'я документа;
– дату і час друку;
– число сторінок і число копій;
– об'єм документа;
– пріоритет виконання завдання;
– розмір паперу;
– папір кольоровий чи чорно-білий;
– чи був задіяний режим дуплексу (друк на обох сторонах листа);

– надавати можливість відповідальній особі/системному адміністратору проглянути вміст завдань друку як в черзі, так і для всіх вже надрукованих завдань;

– копіювання завдання з одного принтера на інший;

– визначення вартості всіх надрукованих завдань, тощо.

Система, що буде розроблена, повинна забезпечити виконання вищеозначених функцій в автоматичному фоновому режимі, разом з цим надаючи користувачу високий ступінь інформативності, адже до структури планується ввести зручний та зрозумілий для нього інтерфейс для одержання:

– службових повідомлень про успішне/неуспішне виконання операцій моніторингу мережевих ДРП;

– службових повідомлень про успішне/неуспішне проведення перевірок;

– протоколу реєстрації нестандартних ситуацій, які можуть виникнути в процесі роботи системи/обладнання;

– звітної інформації в будь-який відлік часу за будь-який термін роботи системи по безпосередньому призначенню.

Функції контролю/спостереження не будуть безпосередньо впливати на роботи системи в цілому і виконувати означені для них задачі в фоновому режимі.

Необхідно також передбачити встановлення початкових умов роботи інтерфейса, що дозволить користувачу налаштувати робочий простір по своєму бажанню:

– змінити розташування і розмір вікон;

– провести налаштування панелі інструментів;

– встановити бажані кольори тощо.

Тому до складу системи буде введено INI-файл для збереження налаштувань, виконаних користувачем на початку роботи з системою. В подальшому вони будуть установлюватись в автоматичному режим; по замовченню при кожному наступному завантаженні системи.

В процесі роботи системи по виконанню встановлених задач виникає необхідність в збереженні та обробці результатів моніторингу та службової інформації, яка буде утримуватись в двох базах даних (БД): в локальній БД (клієнтська частина) та в мережевій БД (серверна частина). Враховуючи специфіку задач, що буде виконувати система, найбільш доцільно використати реляційні БД. В такій БД об’єкти та взаємозв’язок між ними представляються у вигляді плоских прямокутних таблиць з рядів та стовпчиків.

Для розробки ПЗ системи нами обрано мову програмування DELPHI. DELPHI не має власного формата таблиць, але має засоби, які дозволять працювати з багатьма зовнішніми форматами, тому необхідно вибрати формат таблиць бази даних. Найбільш розповсюдженим та розвиненим є формат Paradox.

Таблиці Paradox утримують достатньо велике число полів, підтримують цілісність посилань, автоматично перевіряють дані, що вводяться, на сумісність по типу і підтримують парольний захист даних. Основні розширення таблиць БД Paradox, що будуть використані при розробці ПЗ, наводимо в таблиці 1.

Таблиця 1 – Файли таблиць БД Paradox

Розширення файла	Зміст файла
*.db	Дані таблиці.
*.mb	Великі двійкові дані (BL.OB, BinaryLarqeObject).
*.px	Ключ (головний індекс).
*.xq*i*.yq*	Індекси.
*.val	Параметри для перевірки типів даних, що вводяться, цілісності посилань.
*.net	Використовується для контролю парольного доступу.

Додаток, створений в процесі реалізації дипломного проекту за допомогою DELPHI, здійснює доступ до БД через спеціальний процесор баз даних ВДЕ. ВДЕ – це набір драйверів і динамічно приєднуваних бібліотек (файл *.dll), які забезпечують доступ до даних. Процесор ВДЕ дозволить найбільш ефективно організувати роботу з таблицями БД Paradox.

Для успішної роботи з БД необхідні програмні засоби, які б забезпечували доступ до потрібної інформації та виконання будь-яких дій з нею. Для рішення цієї задачі використаємо СУБД. Всі СУБД поділяються на дві групи: локальні та мережні.

В нашому випадку більш доцільно використати мережну СУБД, оскільки в процесі роботи система буде використовуватись режим мультидоступа користувачів, що будуть постійно взаємодіяти з однією БД за допомогою технології “клієнт-сервер”. В розробці СУБД немає необхідності, оскільки можна використати одну з стандартних СУБД: InterBase, Oracle, Microsoft SOL Server, тощо.

Враховуючи, що система буде мати складну ієрархічну структуру, при розробці ПЗ необхідно забезпечити організацію та виконання наступних системних програмних задач:

– реалізація роботи з мережею за допомогою протоколу TCP/IP;

– реалізація роботи з зовнішнім периферійним обладнанням: принтери, плотери, багатофункціональні друкуючі пристрої (БДРП), тощо;

– реалізація введення/виведення інформації;

– реалізація роботи з файловою системою БД Paradox;

– реалізація функцій часу;

– реалізація масштабування, виведення керуючих сигналів, перетворення кодів.

Багатофункціональність системи, що підлягає розробці, забезпечить локалізацію різноманітних задач, починаючи з налаштування і конфігурування, комунікаційних функцій і задач контролю, і закінчуючи системою розробки користувачем своїх елементів інтерфейсу і методик розрахунків в рамках системи, застосування у всіх цих задачах єдиного підходу, єдиної інформаційної бази і інструментів розробки.

В комп’ютерних системах моніторингу мережних друкуючих пристроїв, як це було визначено при розгляді існуючих систем-аналогів, апаратні засоби та програмне забезпечення існують в формі неподільного апартно-програмного комплексу, який виконує комплекс визначених функцій. Тому одною з самих складних задач, що підлягають вирішенню в процесі розробки програмного забезпечення системи, є задача оптимального розподілу функцій контролера між апаратними засобами та програмним забезпеченням.

Враховуючи зазначене вище, весь цикл розробки ПЗ та організації системи доцільно розподілити, використавши методику системного проектування та декомпозиції, на послідовність трьох фаз проектування:

а) аналіз задачі і вибір апаратних засобів;

б) розробка системного та прикладного програмного забезпечення;

в) комплектування апаратних засобів та ПЗ в прототипі системи та її налагодження.

Визначимо вимоги до архітектури майбутньої системи. Вибір виконуваних функцій і керування режимами відображення плануємо здійснювати через меню і кнопки керування. До функціоналу системи необхідно ввести наступні режими роботи:

– моніторингу – для відображення параметрів, які контролюються і враховуються системою по точках моніторингу (ПК користувачів, що працюють з ДРП); відображення буде відбуватись у вигляді таблиці;

– автоматичне формування звітів одержаних результатів моніторингу роботи ДРП по заданих шаблонах, редагування та виведення звітів на екран (або на друк);

– адміністратора – для визначення списку користувачів системи і списку задач, з якими користувачі можуть працювати, налаштування IP-адреси сервера, очищення БД, архівація БД (в разі необхідності);

– служба експорту-імпорту для організації обміну даними по моніторингу роботи мережних ДРП;

– інтерактивний режим – надання можливості системному адміністратору/відповідальній особі/користувачу одержати результати проведеного моніторингу та, зробивши відповідні висновки, виконати необхідні дії;

– автоматичний режим – організація і проведення процесу моніторингу мережевих ДРП.

Таким чином, робота системи, що підлягає розробці, буде будуватись на обробці даних (одержаних результатів моніторингу), які визначені та описані в цьому розділі.

В основу побудови архітектури майбутньої системи планується покласти модульний принцип, тобто є головний, керуючий модуль та підлеглі модулі, кожен з яких виконує якусь одну функцію.

Головний модуль – це вікно, з якого при натисненні відповідних кнопок можна виконувати різні операції. Кожна операція буде забезпечуватись окремим модулем, котрий можна буде запустити на виконання. Також, його можна буде змінити на допрацьований модуль (з тою ж назвою) простим шляхом перезапису файлу модуля його пізнішою версією.

Таким чином, розробник зможе без особливих труднощів:

– змінити функціонал системи;

– виправити можливі помилки;

– додати якісь нові якості до даного модуля (наприклад, нові операції);

– без особливих зусиль передати модуль користувачу на електронному носії інформації або для цього використати Internet.

Користувач просто скопіює новий модуль до директорії, в якій знаходиться програма – і все, пакет оновлено. Навіть не треба перезавантажувати систему. Можна одразу запускати її на виконання та продовжувати експлуатацію по безпосередньому призначенню.

До складу ПЗ, яке підлягає розробці, планується ввести графічний інтерфейс, який забезпечить роботу користувачів в інтерактивному режимі. При запуску системи на екран буде виведене вікно, в якому розташуємо кнопки з назвами операцій. При натисненні на ці кнопки виконаються задані операції та виведуться результати їх роботи на екран користувачу, а саме: автентифікація користувача; завантаження допоміжних модулів (робочі режими системи); обробка системних помилок; режим HELP.

Також система повинна бути сумісною зі всіма ПК, на яких встановлено ОС WINDOWS або навіть DOS, так як деякі модулі можуть працювати в мережі при відсутності WINDOWS. Хоча таких переваг, як віконний інтерфейс під чистим DOS користувач не отримає, однак він без проблем зможе виконати заплановані операції при роботі з мережею та зберегти потрібні дані.

Розробка структурної схеми

При розробці концепції побудови майбутньої системи та шляхів її реалізації, основний наголос робився на швидкості, зрозумілості її використання та безперечного виконання встановлених за системою функцій. Розробці підлягає складна (в сенсі реалізації ПЗ) багатофункціональна система, тому доцільно використати функції Windows API-Win32. Win32 – це набір функцій, які є частиною ОС, і реалізовані у вигляді DDL-бібліотек. Вони забезпечують пряме звертання програм до необхідних процедур, підпрограм чи функцій. При розробці архітектури системи доцільно використати наступні бібліотеки Win32 API ядра ОС Windows:

– User32: функції керування користувацьким інтерфейсом;

– Advapi32:функції доступу до системного реєстра.

Окрім вищеозначених бібліотек, які будуть основними елементами системи, при розробці ПЗ необхідно використати наступні компоненти і інтерфейси системних викликів ядра ОС Windows:

– бібліотеку драйверів пристроїв (на які необхідно створити образи);

– рівень NativeAPI (NTdll.dll); рівень NativeAPI ядра (ntoskrul.exe); рівень абстракції від обладнання (hal.dll).

Використання цих компонентів дозволить організувати взаємодію пристроїв з ПЗ системи для реалізації основної задачі – проведення моніторингу мережевих ДРП (рисунок 1).

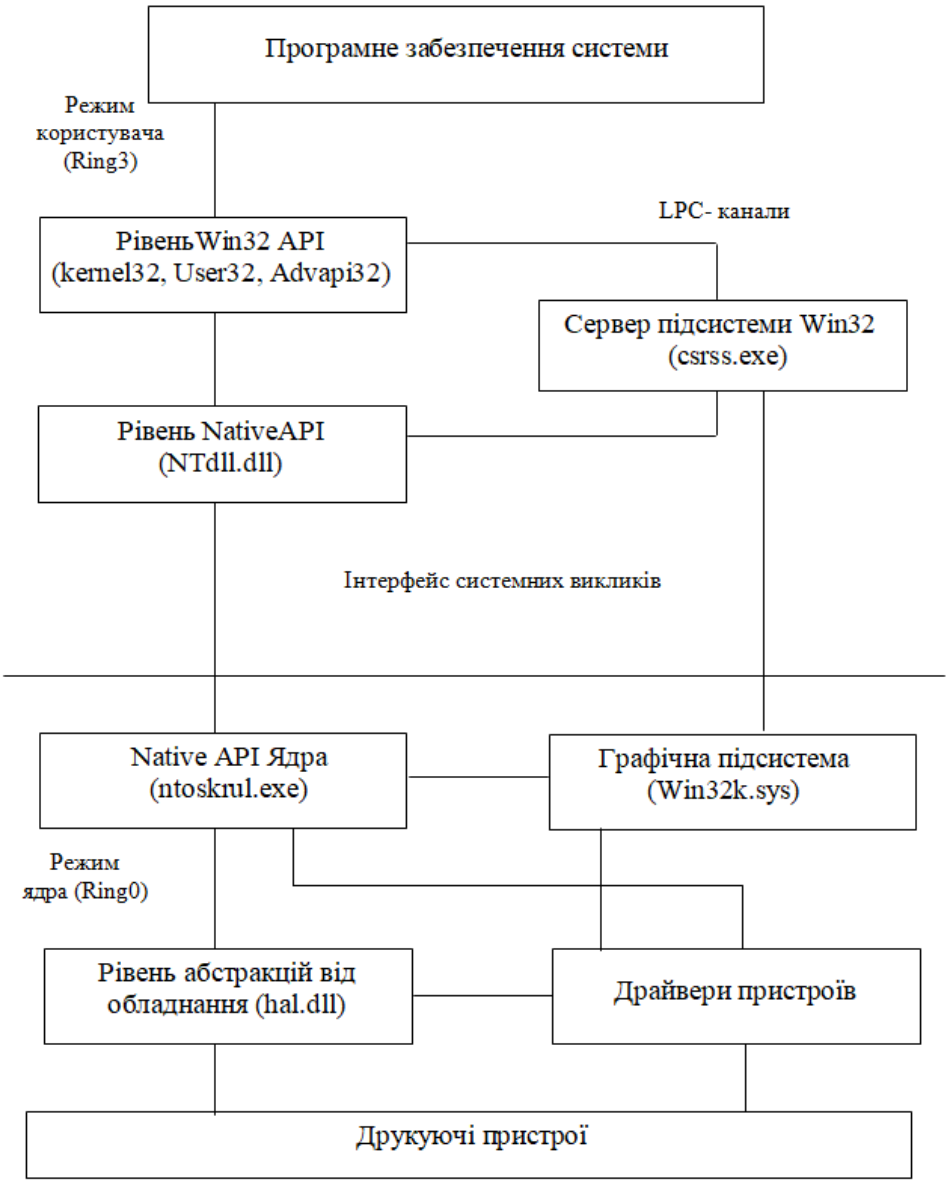


Рисунок 1 – Структурна схема системи

Розроблену структурну схему будемо розглядати в якості базової для побудови структури майбутньої системи, тому визначимо більш детально компоненти структурної схеми та означимо функції, які вони будуть виконувати в системі, яка підлягає розробці:

– HAL.dll – рівень абстракцій від обладнання: використання цієї бібліотеки дозволить забезпечити незалежність розробленої системи від апаратної платформи;

– NTdll.dll – ця бібліотека – своєрідний «місток» між тими бібліотеками, які працюють в ядрі ОС, і бібліотеками, що будуть працювати в системі;

– графічна підсистема (Win32.sys) та бібліотека Gdi32.dll забезпечать організацію та чітку роботу графічного інтерфейса користувача; вони надають додаткам та іншим бібліотекам графічні примітиви для рисування вікон та різноманітних віконних елементів керування;

– функція DeviceloControl, яка забезпечить керування драйверами пристроїв, змушуючи обраний пристрій виконати відповідну операцію, для визначення типу пристрою використаємо функцію GetDriveType.

При побудові структури системи використаємо сучасну технологію «Клієнт-Сервер», згідно якої введемо до її складу дві змістовні частини (підсистеми):

– частина 1: «Клієнт»;

– частина 2: «Сервер».

Частина 1 і частина 2 підлягають програмній реалізації в процесі виконання ВКРМ.

Клієнтська частина забезпечить в процесі експлуатації системи організацію та виконання власне процесу моніторингу роботи мережних ДРП і тому має бути встановленою на кожному ПК користувача, який в процесі роботи використовує ДРП. Тобто, таких частин в структурі системи може бути N-а кількість.

До складу клієнтської частини введемо наступні блоки: файл налаштувань; програмний агент та локальну БД Paradox.

Програмний агент – це програмно реалізований блок, який буде утримувати модулі, що забезпечать виконання процесу моніторингу, тобто забезпечить реалізацію задачі, яка поставлена перед автором ВКРМ.

Для збереження результатів моніторингу до складу клієнтської частини введемо локальну базу даних, яка за допомогою спеціально розробленого в процесі виконання ВКРМ додатку та драйверу BDE буде накопичувати результати моніторингу друку по кожному окремому ПК.

Файл налаштувань забезпечить в процесі роботи системи збереження необхідних для роботи налаштувань, які виконуються при першому завантаженні системи, а в подальшій роботі завантажуються в автоматичному режимі.

Клієнтська частина на основі використання сокетних технологій та протоколів TCP/IP через мережу буде взаємодіяти з серверною частиною.

Серверна частина системи буде встановлена на ПК системного адміністратора/відповідальної особи/керівника і забезпечить в процесі експлуатації системи збирання, обробку та збереження до загальної БД результатів моніторингу від кожної клієнтської частини (в локальній мережі їх може бути N-а кількість).

Для візуалізації одержаних в результаті проведення моніторингу даних до складу серверної частини доцільно також ввести модуль перегляду та друку звітів.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів моніторингу мережевих принтерів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем моніторингу мережевих принтерів. Досліджена система моніторингу мережевих принтерів. На основі отриманих результатів досліджень створена програмна реалізація системи моніторингу мережевих принтерів. Розроблені алгоритми дозволяють успішно вирішувати завдання моніторингу мережевих принтерів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Разработка математической gert-модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / А.А.Смирнов, Мохамад Гани Абу Таам // Информационные системы в управлении, образовании, промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 498 с.
2. Смирнов А.А. метод управления доступом в интеллектуальных узлах коммутации / Мохамад Гани Абу Таам, А.А.Смирнов // Информационные технологии и защита информации в информационно-коммуникационных системах: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – 486 с.
3. Смирнов А.А. Математическая gert-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.
4. Смирнов А.А. структурно-логическая GERT-модель технологии распространения компьютерных

вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Системи управління, навігації та зв'язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120-125.
5. Смирнов А.А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Гани Абу Таам, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 9(125). – Х.: ХУПС – 2014. – С. 105-110.
6. Смирнов А.А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 4 (41). – Харків: ХУПС. – 2014. – С. 48-52.
7. Смирнов А.А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Харків: ХУПС. – 2014. – С.90-95.
8. Смирнов А.А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-153.
9. Смирнов А.А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – Випуск 3(43) – Х.: ХУПС – 2015. – С. 100-107.
10. Смирнов А.А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 3(19). – Х.: ХУПС. – 2015. – С. 134-141.
11. Mohamad Abou Taam Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

УДК 004

Д. Марков, магістр гр. КІ-20МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНФІДЕНЦІЙНОЇ ПЕРЕДАЧІ ДАНИХ ДЛЯ СЕРВІСІВ МИТНОЇ СЛУЖБИ

У статті розроблено програмне забезпечення, яке призначено для системи конфіденційної передачі даних для сервісів митної служби. Метою розробки є дослідження та програмна реалізація системи конфіденційної передачі даних для сервісів митної служби. Об'єктом дослідження є процес конфіденційної передачі даних для сервісів митної служби. Предметом дослідження є методи конфіденційної передачі даних для сервісів митної служби. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи конфіденційної передачі даних для сервісів митної служби. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, конфіденційність, передача даних, сервіси митної служби

Постановка проблеми. Бурхливий розвиток науково-технічного прогресу призвів до проникнення інформаційних технологій майже в усі сфери сучасного життя. Зараз важко уявити собі життя без застосування комп'ютерів, Інтернету, мобільного зв'язку та інших досягнень у сфері ІТ до яких ми вже звикли. Одним з цих досягнень є застосування бездротового зв'язку. При цьому, це касається не тільки розмов по стільниковим або супутниковим телефонам, але й передачі різного виду даних, таких як текстової інформації, аудіо та відеоінформації.

Одним з соціальних інститутів сучасної держави є митна служба. Митна служба України – це єдина загальнодержавна система, яка складається з митних органів та спеціалізованих митних установ і організацій. Митними органами є спеціально уповноважений центральний орган виконавчої влади в галузі митної справи, регіональні митниці, митниці [1]. Для забезпечення виконання регіональними митницями та митницями завдань, визначених цим Кодексом та іншими законами України, можуть створюватися митні пости. Митний пост є структурним підрозділом регіональної митниці, митниці, який безпосередньо здійснює митний контроль та оформлення товарів і транспортних засобів, що переміщуються через митний кордон України [1-7]. При цьому через митні пости проходить велика кількість різного виду товарів, та виїжджає та заїжджає велика кількість людей, інформацію про яких потрібно обробляти в реальному режимі часу. Для цього сучасні митники оснащуються мобільними пристроями, які мають доступ до серверів митної служби. При цьому інформація яка передається з цих мобільних пристроїв як правило є для службового користування, тобто конфіденційною [5].

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи конфіденційної передачі даних для сервісів митної служби

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи конфіденційної передачі даних для сервісів митної служби.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем конфіденційної передачі даних для сервісів митної служби.
– Дослідження системи конфіденційної передачі даних для сервісів митної служби.
– Програмна реалізація системи конфіденційної передачі даних для сервісів митної служби.

Об'єктом дослідження є процес конфіденційної передачі даних для сервісів митної служби.

Предметом дослідження є методи конфіденційної передачі даних для сервісів митної служби.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Опис специфікації формату електронних повідомлень митної служби.

З метою вдосконалення механізму проведення митного оформлення товарів і транспортних засобів і для забезпечення уніфікації форматів даних електронних копій вантажних митних декларацій булла затверджена специфікація форматів електронних повідомлень програмно-інформаційного комплексу „Автоматизована система митного оформлення товарів та інших предметів" на рівні суб'єкт – митний орган і специфікація форматів електронних повідомлень програмно-інформаційного комплексу „Автоматизована система митного оформлення товарів та інших предметів" на рівні митний орган – Департамент інформаційних технологій та митної статистики (далі – специфікації форматів. Вони були розміщенні на WEB-сервері Держмитслужби України (розділ „Інформаційні ресурси") – специфікацій форматів; на WEB-сервері Держмитслужби України в мережі Internet (розділ „ЄАІС") – Специфікації форматів електронних повідомлень програмно-інформаційного комплексу „Автоматизована система митного оформлення товарів та інших предметів" на рівні суб'єкт – митний орган. При цьому була введена незалежність програмно-інформаційного комплексу „Автоматизована система митного оформлення товарів та інших предметів" (у реалізації Windows і WEB-версії) від форматів електронних повідомлень, розроблених комерційними підприємствами.

Технологія обміну електронною інформацією автоматизованої системи митного оформлення товарів і транспортних засобів передбачає наявність двох суб'єктів (сторін)

обміну – суб'єкта господарювання і митного органу, та об'єкта обміну – електронного повідомлення, яке містить електронні копії зовнішньоторговельних документів, зокрема вантажні митні декларації (у подальшому можливо ліцензії, дозволи, контракти тощо), діагностичні дані, дані контролю цілісності повідомлення тощо.

Обмін електронними повідомленнями на рівні суб'єкт – митний орган здійснюється шляхом формування суб'єктами господарювання електронного пакета документів, передання його до митного органу з використанням дискет або електронної пошти, оброблення митним органом пакета документів, формування електронного пакета повідомлення у відповідь і передання пакета відповіді суб'єкту господарювання. У цьому дипломному проекті пропонується передавати дані з мобільних пристроїв митника на сервер митної служби за допомогою Bluetooth або Wi-Fi. Узагальнену схему технології обміну електронною інформацією на рівні суб'єкт – митний орган наведено на рисунку 1.

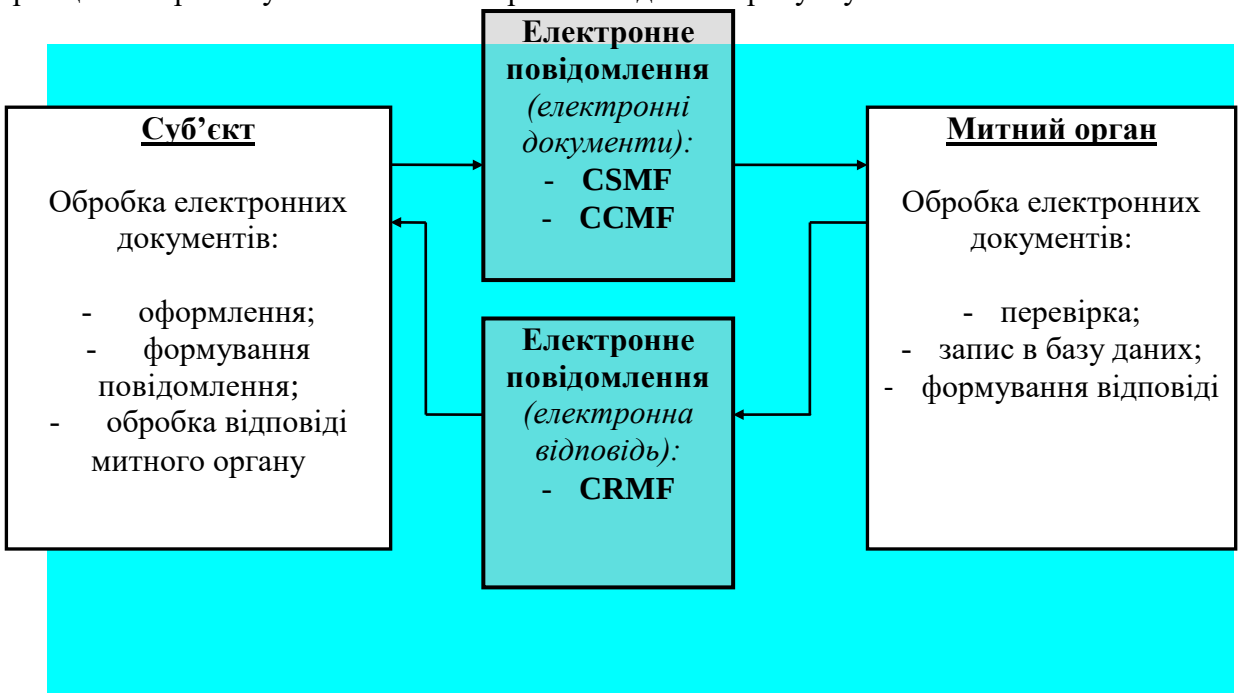


Рисунок 1 – Узагальнена схема технології обміну електронною інформацією на рівні суб'єкт – митний орган

Під форматами електронних повідомлень для обміну інформацією з автоматизованою системою митного оформлення товарів і транспортних засобів розуміється певна формалізована структура файла електронного повідомлення, що має вбудовані засоби контролю цілісності даних при передачі й унікально характеризує відправника й одержувача електронного повідомлення.

Версією 1.06 специфікації форматів електронних повідомлень передбачені три види повідомлень:

– CSMF – простий формат електронного повідомлення, що застосовується у відповідних автоматизованих додатках і має істотні обмеження за типами документів і їх кількістю;

– CCMF – складовий формат електронного повідомлення, який є базовим для основних комерційних додатків і який відстежується в автоматизованій системі митного оформлення товарів і транспортних засобів на основі списків сертифікованого програмного забезпечення й ліцензійних угод;

– CRMF – формат електронного повідомлення відповіді митниці на повідомлення CCMF.

Структура всіх трьох видів електронних повідомлень уніфікована й складається із:

– заголовка повідомлення (Head Message), у якому наводиться інформація про тип і версію формату повідомлення, про відправника й одержувача повідомлення, а також

містяться дані про кількість електронних копій документів у повідомленні, контрольні дані цілісності пакета тощо;

– основної частини повідомлення (Body Message), у якій містяться сегменти опису електронних копій документів, сегменти електронних копій та інші сегменти;

– закінчення повідомлення (Foot Message), у якому містяться контрольні дані про електронне повідомлення.

В основній частині повідомлення містяться сегменти – логічні елементи інформації. Сегменти можуть бути двох основних типів:

– сегменти опису (Info Segment), у яких міститься інформація про правила роботи й інтерпретації електронних документів, відповідей митних органів та інших даних (у простому форматі електронного повідомлення CSMF відсутній);

– сегменти даних (Data Segment), у яких містяться електронні копії документів, відповіді митних органів та інші дані.

В електронному повідомленні сегменти опису (за їх наявності) мають бути розміщені перед сегментами даних (у порядку розташування від початку повідомлення).

За своєю структурою сегменти даних поділяються на три частини:

– заголовок сегмента (Head Data Segment), у якому наводиться інформація про тип і версію даних, контрольні дані цілісності сегмента й інші дані;

– основну частину сегмента (Body Data Segment), у якій містяться форми електронних даних;

– закінчення сегмента (Foot Data Segment), у якому містяться контрольні дані про сегмент.

Форми електронних даних, які містяться в основній частині сегмента даних, містять опис і електронну інформацію певних структурних елементів документа (наприклад, загальний опис вантажної митної декларації або опис конкретного товару згідно з контрактом). За своєю структурою форми електронних даних складаються з трьох частин:

– заголовка форми (Head Form), у якому наводиться інформація про тип і версію форми, контрольні дані цілісності форми й інші дані;

– основної частини форми (Body Form), у якій містяться поля електронних даних;

– закінчення форми (Foot Form), у якому містяться контрольні дані про форму й ознаки закінчення форми.

Поля електронних даних є неподільною логічною одиницею інформації і містять безпосередні дані. Кожне поле електронних даних містить:

– код поля (Field Code) – ідентифікаційний 4-значний номер поля для інтерпретації даних;

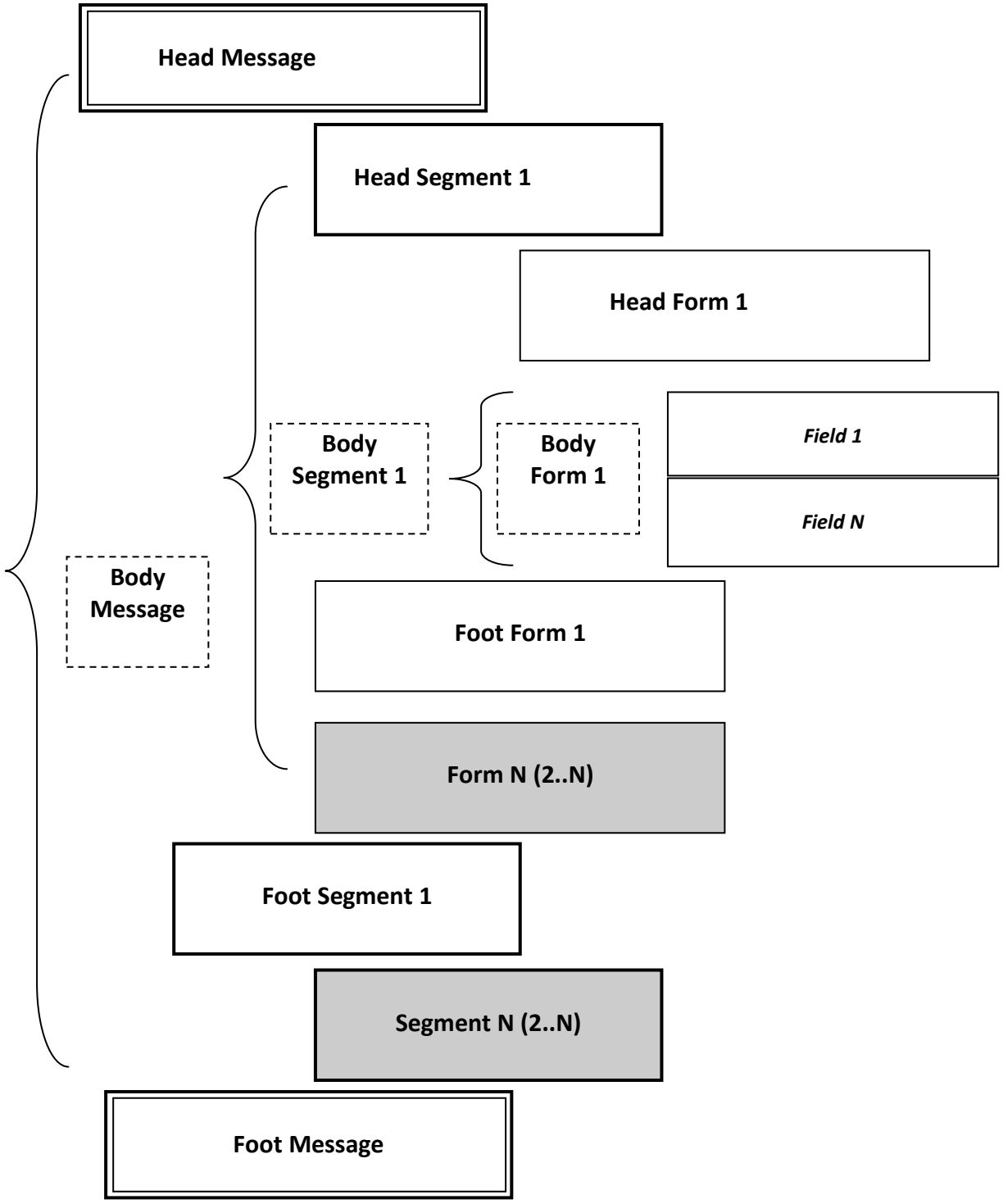


Рисунок 2 – Узагальнена структура форматів електронних повідомлень V 1.06

– значення поля (Field Data) – символьний рядок змінної довжини (від 1 до 1024 символів), у якому містяться безпосередні дані поля (деякі поля вимагають використання спеціальних шаблонів заповнення);

– закінчення поля (Field End) – символ закінчення поля електронних даних.

Поля електронних даних, що використовуються для представлення інформації, містять 4-значний цифровий код поля в форматі C4 (9999), безпосередньо дані в форматі C1...1024 і ознаку закінчення поля у форматі B1 (символ 02).

Усі дані в електронному повідомленні, крім символів закінчення структурних одиниць (сегментів, форм і полів), містяться в символьному вигляді (ASCII від 32 до 254).

Для опису полів інформації в додатках використовуються такі позначення:

С2 – символьне поле довжиною 2 символи;

С1...1024 – символьне поле змінної довжини (до 1024 символів);

У1 – поле довжиною 1 байт для подання двійкової інформації;

N2 – поле для занесення цифрової інформації (символи 0-9, "." і знак);

99 – шаблон заповнення поля, що вказує на обов'язковість заповнення цього поля цифровими символами (0 – 9);

ХХ – шаблон заповнення поля, що вказує на обов'язковість заповнення цього поля алфавітно-цифровими символами;

АА – шаблон заповнення поля, що вказує на обов'язковість заповнення цього поля алфавітними символами (А – Я);

ДД/ММ/РР – шаблон заповнення дати.

Усі файли електронних повідомлень обов'язково повинні мати розширення „.CMF." Щодо імені файла, то тут немає ніякого обмеження (крім обмежень операційної системи).

Контроль цілісності даних вирішується спільно автоматизованою системою митного оформлення товарів і транспортних засобів та автоматизованою системою декларанта "Митний брокер".

Основним напрямом контролю цілісності даних є контроль правильності передання електронного повідомлення. Такий контроль здійснюється шляхом звіряння контрольних сум, переданих в електронному повідомленні та розрахованих за переданими даними під час приймання й оброблення повідомлення. Ці контрольні суми рахуються по байтах, записаних або прочитаних у повідомленні, їх кількість визначається інформаційним елементом повідомлення – сегментом даних або сегментом опису, формою електронних даних або будь-якою іншою структурою, до якої входить контрольна сума.

Опис технології Bluetooth

Основні особливості

Приймачепередатчики Bluetooth працюють у діапазоні 2,4 Ггц зі швидкістю до 1 Мбіт/с із використанням технології FHSS. Вона припускає безперервну стрибкоподібну зміну частоти у всьому відведеному для передачі спектрі із частотою 1600 змін у секунду, що набагато швидше, ніж частота змін, передбачена для аналогічної технології в стандарті 802.11.

Пристрої Bluetooth з низьким енергоспоживанням забезпечують дальність передачі близько 9 м (30 футів). Високопотужні Bluetooth-пристрої здатні працювати на відстанях до 91 м (300 футів), однак такий режим роботи застосовується рідко.

Модулі Bluetooth мають відносно невеликі форми-фактори. Типові габарити 10,2x14x16 мм, тому вони можуть бути легко убудовані в різні користувальницькі пристрої.

Технологія Bluetooth здатна забезпечувати автоматичне з'єднання Bluetooth-пристроїв, що перебувають неподалік один від іншого, але користувач має можливість прийняти або відхилити можливість з'єднання з іншим користувачем. У випадку, якщо є сумніви в безпеці, з'єднання можна відхилити. Можливість шифрування також застережена в специфікації.

Використання Bluetooth для формування бездротових локальних мереж.

Технологія Bluetooth забезпечує робочі характеристики, подібні з такими бездротових локальних мереж. За рахунок використання високопотужної версії виробники надалі зможуть пропонувати точки доступу й маршрутизатори Bluetooth з радіусом дії таким же, який забезпечують мережі стандарту 802.11. Однак пропоновані в цей час виробу Bluetooth мають набагато меншу споживану потужність і орієнтовані на виконання функцій, характерних для бездротових персональних мереж. Технологія Bluetooth уступає виробам стандарту 802.11, у радіусі дії й продуктивності. Компоненти мереж 802.11 можуть забезпечувати швидкість передачі до 54 Мбіт/с, Bluetooth – у найкращому разі 1 Мбіт/с. Цього може виявитися цілком достатньо в більшості випадків заміни кабельних з'єднань, але

для перегляду Web-сторінок з використанням широкополосного з'єднання або створення митної мережі потрібні більш високі характеристики. Крім того, радіус дії пристроїв стандарту 802.11 в умовах митного пункту звичайно становить приблизно 90 м (300 футів), що набагато перевищує можливості Bluetooth. Для організації бездротової мережі на основі технології Bluetooth на досить великій площі довелося б розгортати занадто багато точок доступу. Тому досить малоймовірно, що продукти технології Bluetooth витиснуть із ринку вироби стандарту 802.11. Магазини електроніки торгують в основному виробами стандарту 802.11 (Wi-Fi), призначеними для організації бездротових персональних мереж, а не пристроями Bluetooth.

У постачальників мереж стандарту 802.11 є час для виходу на ринок і бездротові персональні мережі. Однак для цього необхідно здійснити деякі модифікації. Наприклад, зменшити габарити компонентів мереж стандарту 802.11, але для цього компанії повинні налагодити випуск більш мініатюрних чипсетів. Компоненти з меншими габаритами, як правило, споживають менше енергії, що робить їх придатними для пристроїв (типу стільникових телефонів), що харчуються від мініатюрних батарей. Оскільки група 802.15 розробляє стандарти для бездротових персональних мереж на основі технології Bluetooth, а група 802.11 зосереджена на бездротових локальних мережах, досить імовірно, що технології стандарту 802.11 і Bluetooth зможуть співіснувати й доповнювати одна іншу.

Мінімізація перешкод з боку Bluetooth

Кількість бездротових пристроїв росте, і тому доводиться усе більше уваги приділяти потенційно можливим взаємним перешкодам. Результати тестування фіксують істотні взаємні перешкоди між пристроями Bluetooth і іншими системами, що працюють у діапазоні 2,4 Ггц, такими як бездротові локальні мережі стандарту 802.11. Проблема виникає через те, що пристрої Bluetooth і компоненти мереж стандарту 802.11 ніколи "не розуміли" один одного й не відповідали тим самим правилам. Радіостанція Bluetooth може безсистемно почати передачу даних саме в те самий час, коли станція стандарту 802.11 передає фрейм. Виникає колізія, через яку станція стандарту 802.11 змушена передати цей фрейм повторно. Через відсутність якої-небудь координації й виникають взаємні радіочастотні перешкоди між пристроями стандарту 802.11 і специфікації Bluetooth.

Через потенційну можливість виникнення колізій мережі стандарту 802.11 і специфікації Bluetooth не реалізують всі свої можливості. Станція стандарту 802.11 автоматично знижує швидкість передачі даних і повторно передає фрейм, якщо трапляється колізія. Відповідно й протокол стандарту 802.11 при наявності поблизу пристроїв Bluetooth уводить затримки. Ступінь впливу радіочастотних перешкод залежить від ступеня використання й близькості пристроїв Bluetooth. Перешкоди виникають тоді, коли пристрої стандарту 802.11 і Bluetooth починають передавати дані одночасно. Митники можуть мати ноутбуки й PDA з убудованим інтерфейсом Bluetooth, але перешкод не буде, якщо їх Bluetooth-пристрої не використовують Bluetooth для передачі даних.

Додатки Bluetooth, що забезпечують печать з ноутбука або синхронізацію з настільним комп'ютером, використовують радіоканал протягом коротких періодів часу. У цьому випадку Bluetooth-пристрої не бувають активними настільки довго, щоб істотно знизити продуктивність мережі стандарту 802.

Якщо мережа Bluetooth досить велика й ступінь її використання коливається від середньої до високої, Bluetooth-система, можливо, буде викликати безліч колізій у мережі стандарту 802.11, розміщеної на тій же території. У такому випадку співіснування мереж стандарту 802.11 і Bluetooth виявиться утрудненим, і продуктивність, швидше за все, знизиться.

Крім інтенсивності використання Bluetooth-пристроїв ступінь впливу перешкод багато в чому залежить від близькості цих пристроїв до радіоплат інтерфейсу мережі й точкам доступу. Потужність, випромінювана Bluetooth-пристроями, звичайно нижче, ніж у мережах стандарту 802.11. Отже, станція стандарту 802.11 повинна перебувати досить близько (на

відстані близько 3 м) до передавального Bluetooth-пристрою, щоб виникли істотні взаємні перешкоди.

Типовим прикладом виникнення такої ситуації може служити ноутбук користувача, у якому Bluetooth використовується для підтримки з'єднань із PDA і принтером, а інтерфейс стандарту 802.11 – для доступу до Internet і митних серверів. Можливість виникнення перешкод у цьому випадку дуже велика, особливо якщо користувач працює поблизу границі зони дії мережі стандарту 802.11. Сигнал від Bluetooth-пристроїв, найімовірніше, заглушить ослаблений внаслідок великої відстані від точки доступу сигнал стандарту 802.11.

Існує кілька способів, що допомагають уникнути перешкод з боку Bluetooth-пристроїв.

– Регулюйте застосування радіочастотних пристроїв. Одним зі способів зниження рівня перешкод є правильний вибір типів радіочастотних пристроїв для будинку й офісу митного посту. Іншими словами, варто встановити власні регулятивні правила використання неліцензійних радіочастотних пристроїв. Екстремальною мірою була би повна заборона на використання Bluetooth-пристроїв, але це непрактично, а в деяких випадках і неможливо. Що стосується особистих додатків, то можна виробити політикові компанії, що обмежує використання Bluetooth тільки конкретними додатками, такими як синхронізація PDA і настільних комп'ютерів.

– Забезпечте адекватну зону дії мережі стандарту 802.11. Сильні, добре помітні сигнали у всіх зонах дії мережі стандарту 802.11 знижують ступінь впливу з боку сигналів Bluetooth. Якщо сигнал бездротової локальної мережі стає занадто слабким, перешкоди з боку сигналів Bluetooth стають більше проблематичними. Проведіть дослідження рівня сигналів у зоні розгортання мережі й визначите місця розміщення точок доступу.

– Перейдіть у діапазон 5 Ггц. Якщо жодна з вищезгаданих мір не вирішила проблему, розглянете можливість використання бездротової локальної мережі, що працює в діапазоні 5 Ггц, наприклад мережі стандарту 802.11 a. Ви можете повністю позбутися від перешкод у цьому діапазоні – принаймні, у доступному для огляду майбутньому.

Опис технології Wi-Fi

Альянс Wi-Fi (Wi-Fi Alliance), що почав свою роботу під ім'ям "Асоціація контролю сумісності з бездротовим Ethernet" або просто "асоціація WECA" (wireless ethernet compatibility alliance, WECA), є міжнародною некомерційною організацією, що займається маркетингом і проблемами взаємодії компонентів бездротових локальних мереж стандарту 802.11. Альянс Wi-Fi – це група, що розкручує бренд " Wi-Fi", під яким підпадають всі різновиди бездротових мереж, що відповідають стандарту 802.11 (802.11a, 802.11b і 802.11g), а також всі стандарти такого типу, які з'являться в майбутньому. Альянс Wi-Fi також просуває технологію *захищеного доступу до Wi-Fi* ***(Wi-Fi Protected Access, WPA),*** сполучна ланка між багаторазово розкритикованим механізмом WEP і стандартом захисту 802.111. Альянс Wi-Fi переслідує наступні цілі:

– забезпечувати по усьому світі сертифікацію, що спонукує виробників дотримуватися стандартів 802.11 при розробці компонентів бездротових локальних мереж;

– сприяти збуту сертифікованих Wi-Fi виробів для застосування їх у домашніх умовах, невеликих офісах і на підприємствах;

– тестувати і сертифікувати вироби Wi-Fi з метою забезпечення взаємодії мереж.

Сертифікація Wi-Fi – це процес, завдяки якому забезпечується можливість взаємодії компонентів бездротових локальних мереж, таких як точки доступу й радіоплати, виконані в різних форм-факторах. Для одержання сертифіката на свої вироби компанія повинна стати членом Альянсу Wi-Fi. Альянс керується затвердженими програмами тестування для сертифікації виробів на предмет забезпечення взаємодії з іншими сертифікованими Wi-Fi-компонентами. Після того як виріб успішно протестовано, його виробник одержує право використовувати логотип "Сертифіковане Wi-Fi" для кожного окремого виробу, а також на його впакуванні й інструкції із застосування. Сертифікація Wi-Fi дає клієнтам упевненість у тому, що вони придбали компоненти бездротової локальної мережі, що відповідають

вимогам забезпечення взаємодії з виробами багатьох інших виробників. Логотип "Wi-Fi" на виробі означає, що він відповідає вимогам тестування на сумісність і напевно зможе спільно працювати з Wi-Fi-сертифікованими виробами інших постачальників.

Захищений доступ до Wi-Fi

Механізм WEP не забезпечує достатнього рівня безпеки для більшості додатків, виконуваних у бездротових локальних мережах підприємств. Оскільки в ньому використовується статичний ключ, WEP легко зламати, використовуючи вже наявні програмні засоби. Це спонукує менеджерів інформаційних технологій використовувати більш динамічні форми WEP. Однак ці поліпшені механізми захисту є патентованими, що утрудняє забезпечення їхньої підтримки клієнтськими пристроями від інших постачальників. Тому Альянс Wi-Fi почав значні зусилля для ефективного стандартизованого захисту бездротових локальних мереж, визначивши механізм WPA як забезпечує взаємодія мереж. При використанні WPA мережне середовище, утворене радіоплатами інтерфейсу мережі різних типів стандарту 802.11, може користуватися перевагами розширених форм шифрування. WPA 1.0 є варіантом споконвічної, нератифікованої версії стандарту 802.11, що включає механізми тимчасового протоколу цілісності ключа (temporal key integrity protocol, TKIP) і 802. Їх. Комбінація цих двох механізмів дозволяє забезпечувати шифрування із ключем, що змінюється, і взаємну автентифікацію, що буває іноді зовсім необхідна для бездротових локальних мереж.

Для автентифікації WPA 1.0 використовує комбінацію відкритої автентифікації й автентифікації відповідно до механізму 802.11. Спочатку бездротовий клієнт автентифікується точками доступу, які дозволяють клієнтові посилати фрейми точці доступу. Потім WPA виконує автентифікацію на рівні користувача за допомогою механізму 802.11. Виконуючи цю процедуру, WPA 1.0 взаємодіє із сервером автентифікації підприємства. Якщо ніякий сервер автентифікації недоступний, як це буває в домашніх мережах і мережах невеликих офісів, то WPA 1.0 може працювати в так званому режимі попереднього спільно використовуваного ключа (pre-shared key mode).

Стандарт 802.11 обратно сполучимий з WPA1.0, однак 802.11 включає також опціонально використовуваний удосконалений стандарт шифрування (advanced encryption standard, AES). Для застосування AES необхідні співпроцесори, якими більшість точок доступу на сьогоднішній день не обладнані, тому AES більше підходить для мереж, що розгортаються знову. Новий стандарт WPA 2.0 використовує AES.

Розробка структурної схеми

При створенні структурної схеми формату передачі даних розроблювального дипломного програмного забезпечення враховувалася специфіка роботи на митниці. Як відомо митниця – це кордон між країнами й робота митника повинна бути бездоганною. Один із критичних важливих факторів під час роботи це швидкість складання й обробки митних документів (докладно розглянуто в вище). Чим швидше робота митника тим краще працює митна служба.

При повільної обробки документів на митних лініях або як їх називають порталах, створюється пробка яка згодом може досягати в довжину кілька кілометрів.

На рисунку 3 представлена розроблена структурна схема формату передачі дані програми.

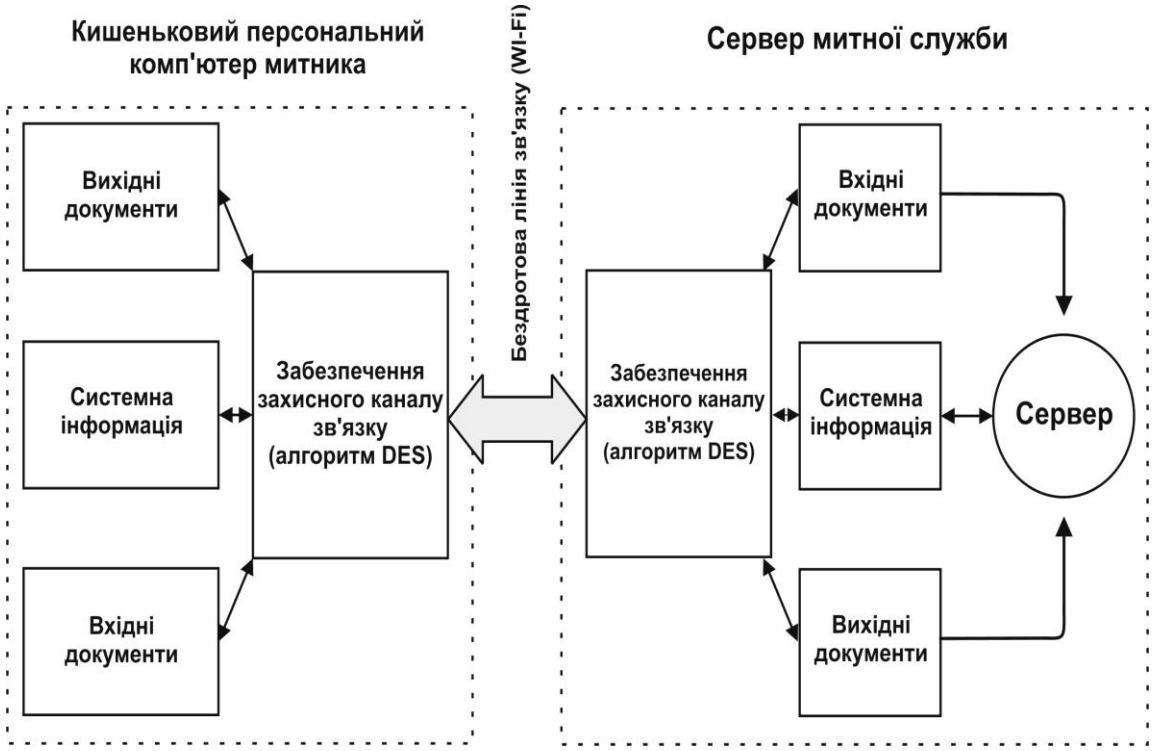


Рисунок 3 – Структурна схема системи

Схема розбита на два основних блоки – мобільний пристрій митника й сервер митної служби. Два цих блоки взаємодіють через радіо лінію зв'язку стандарту 802.11. Коли митникові надають дані, він через мобільному пристрої швидко передає їх на сервер митної служби по захищеному (алгоритм Blowfish розділ 4.2) радіоканалу зв'язку. Далі на сервері відбувається обробка шаблонових даних і видача вихідних документів з інструкціями про подальші дії залежно від типу автомобіля й вантажу. Також митникові передаються системна інформація про тривалість його роботи про кількість складених паперів, а також про термінові повідомлення даної зміни.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів конфіденційної передачі даних для сервісів митної служби. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем конфіденційної передачі даних для сервісів митної служби. Досліджена система конфіденційної передачі даних для сервісів митної служби. На основі отриманих результатів досліджень створена програмна реалізація системи конфіденційної передачі даних для сервісів митної служби. Розроблені під час виконання алгоритми дозволяють успішно вирішувати завдання конфіденційної передачі даних для сервісів митної служби. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и

промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

Т. Кузнєцова, магістр гр. КН-20МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ БІОМЕТРИЧНОГО ДОСТУПУ ДО ДАНИХ У ХМАРНОМУ СЕРВІСІ

У статті розроблено програмне забезпечення, яке призначено для системи біометричного доступу до даних у хмарному сервісі. Метою розробки є дослідження та програмна реалізація системи біометричного доступу до даних у хмарному сервісі. Об’єктом дослідження є процес біометричного доступу до даних у хмарному сервісі. Предметом дослідження є методи біометричного доступу до даних у хмарному сервісі. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи біометричного доступу до даних у хмарному сервісі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерні науки, біометричний доступ, хмарний сервіс

Постановка проблеми. Ідентифікацію й автентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація й автентифікація – це перша лінія оборони, "прохідна" інформаційного простору організації [1].

У відкритому мережному середовищі між сторонами ідентифікації/автентифікації не існує довіреного маршруту; це значить, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманої й використаними для перевірки дійсності.

Необхідно забезпечити захист від пасивного й активного прослуховування мережі, тобто від перехоплення, зміни й/або відтворення даних. Передача паролів у відкритому виді, мабуть, незадовільна; не рятує положення й шифрування паролів, тому що воно не захищає від відтворення. Потрібні більш складні протоколи автентифікації [1-6].

Сучасні засоби ідентифікації/автентифікаціи повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід у мережу – це, у першу чергу, вимогп зручності для користувачів.

Традиційно в Інтернет автентификація користувачів виробляється за допомогою Імені (Login) і Пароля (Password). Використання цього підходу, як і все у світі, має свої переваги й свої недоліки. Переваги очевидні – простота реалізації, відсутність необхідності здобувати додаткові пристрої, за винятком клавіатури, зрозуміло, звичка, нарешті.... Але є й недоліки, в основному пов'язані з «людським фактором», а саме те, що людині важко запам'ятовувати довгі й складні паролі й отут починаються проблеми – користувачі забувають паролі, передають свої паролі третім особам, або пишуть свої паролі на папірцях (і навіть прикріплюють їх на монітор), придумують собі прості паролі, або просто використовують той самий пароль «на всі випадки життя» [2-3]. Все це рано або пізно приводить до втрати пароля в найкращому разі або до його «крадіжки» і використанню без відома користувача.

Наявність проблеми підстьобнуло розробку альтернативних шляхів автентификації й ідентифікації. Була розроблена безліч рішень, що дозволяють так чи інакше замінити спосіб їхнього зберігання й введення або замінити саму схему Ім'я/Пароль. До першої групи рішень відносять різні пристрої, такі як смарт-карти й електронні таблетки й ключі, у яких зберігається Ім'я й Пароль або інформація, що їх заміняє, до останньої групи рішень відносять різні біопараметричні способи ідентифікації й автентификації по персональних особливостях користувача, таким як відбитки пальців, сітківка ока, форми особи й рук і інші. Смарт-карти, електронні таблетки й ключі (далі – електронні ключі) безумовно, усувають деякі з недоліків схеми Ім'я/Пароль: користувачеві не потрібно запам'ятовувати свій пароль, не потрібно його вводити, а також можна створювати й зберігати в електронних ключах паролі будь-якої складності й довжини. Однак, у цієї схеми є кілька очевидних недоліків – ключ із паролем як і раніше можуть украсти, його можна втратити або забути, можна передати добровільно (або не зовсім добровільно) третім особам, ну й нарешті необхідний додатковий прилад – зчитувач електронних ключів [1, 8].

Біопараметричні способи автентификації й ідентифікації усувають багато проблем, тому що як ключ використовується невід'ємна частина людського організму [4-6]. Такий ключ не можна втратити або забути, передати іншій особі, та й пароль як такий у принципі не використовується в цій схемі. Недоліків два – додаткові прилади для зчитування біопараметричних особливостей і необхідність у надійному й швидкому алгоритмі розпізнавання.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи біометричного доступу до даних у хмарному сервісі

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи біометричного доступу до даних у хмарному сервісі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем біометричного доступу до даних у хмарному сервісі.
– Дослідження системи біометричного доступу до даних у хмарному сервісі.
– Програмна реалізація системи біометричного доступу до даних у хмарному сервісі.

Об'єктом дослідження є процес біометричного доступу до даних у хмарному сервісі.

Предметом дослідження є методи біометричного доступу до даних у хмарному сервісі.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Автентифікація на основі біопараметричних параметрів

Розглянемо коротко використання біопараметричних параметрів у процесі автентифікаціи.

Автентифікація за формою руки

Спосіб заснований на аналізі зображення кисті. Цей спосіб досить широко розповсюджений, але не дуже надійний. Це зв'язано, у першу чергу, з великою варіабельністю форми кисті, як протягом життя людини, так і у відносно короткий термін. Деяким плюсом може служити малий розмір математичного "опису" кисті. В HandKey-системах довжина "опису" становить порядку десятків байт, що служить додатковим підтвердженням малої надійності методу, тому що інформації явно недостатньо для охвату всіх можливих "варіантів" форми кисті, якими природа наділили людей.

Автентифікація за формою особи

Спосіб заснований на аналізі великої кількості параметрів, таких як колір, форма, контраст, риси й т.д. Системи подібного роду в цей час мають недостатню надійність розпізнавання через велику чутливість до освітленості й ракурсу особи під час уведення параметрів ідентифікації.

Автентифікація по термограммі особи

Спосіб заснований на результатах досліджень, які показали, що термограмма, тобто схема розташування кровоносних посудин особи (вени й артерії), є унікальною для кожної людини. Для введення характеристики використовується спеціально розроблена інфрачервона камера. Система дозволяє провести ідентифікацію навіть у випадку, коли людина перебуває на іншому кінці неосвітленої кімнати. Температура тіла, охолодження шкіри особи в морозну погоду, природне старіння організму людини, використання спеціальних масок, проведення пластичних операцій не впливають на точність термограмми. Якість розпізнавання невисока, поширення метод одержав невелике.

Автентифікація по голосу

Надійна ідентифікація людини по голосу поки залишається нерозв'язною проблемою. Основна проблема полягає у великій розмаїтості проявів голосу однієї людини: голос може мінятися залежно від настрою, стану здоров'я, віку й т.д. Ця розмаїтість визначає серйозні труднощі при виділенні індивідуальних властивостей голосу людини. Крім того, облік шумового компонента є ще однією серйозною й не до кінця вирішеною проблемою в практичному застосуванні ідентифікації по голосу. Надійність розпізнавання не висока – помилка пропустити чужого змінюється в межах відсотків – часток відсотків.

Автентифікація по підпису людини

Ідентифікація людини по його підпису – середньо надійний метод біопараметричної ідентифікації особистості. Широкого поширення поки не одержав, хоча в банківських системах використовується часто.

Автентифікація по райдужній оболонці ока

Цей метод має високий ступінь надійності, однак, відповідні пристрої введення зображення райдужної оболонки ока мають поки досить високу вартість. Вдобавок – існують проблеми, пов'язані із процедурою сканування. Пристрій сканування, фактично, є високоякісною телекамерою, що визначає деякі незручності, пов'язані з камерою й властиво процедурою сканування.

Автентифікація по рисунку папіллярного візерунка пальця

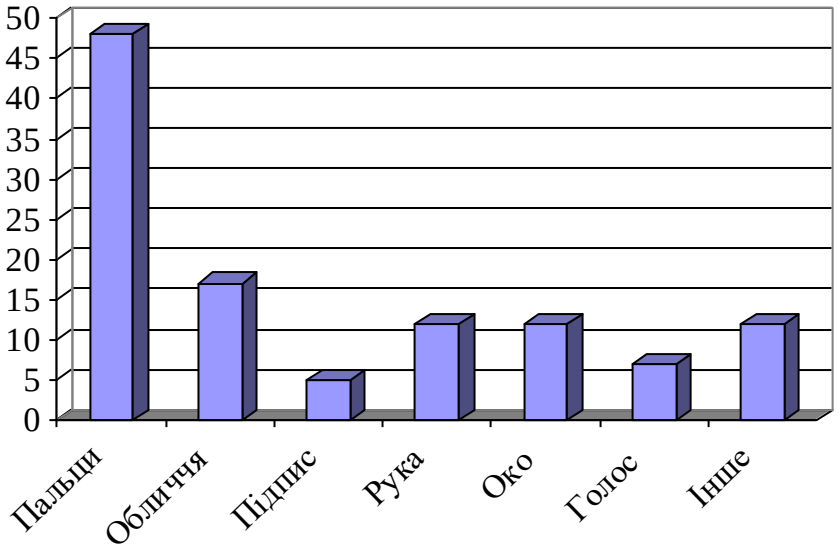
По надійності відповідних процедур ідентифікації метод зіставимо, а в деяких випадках забезпечує якість вище попереднього. Відповідні пристрої введення мають більше низьку вартість. Папіллярный візерунок пальця людини є унікальною біопараметричною характеристикою: в усьому світі немає двох різних пальців з тим самим візерунком.

Автентифікація по фрагментах генетичного коду

Жодна з перерахованих вище персональних характеристик людини не може зрівнятися по надійності розпізнавання з генетичним кодом людини. Однак практичні способи ідентифікації, що використовують унікальні особливості фрагментів генетичного коду, у цей час застосовуються рідко через їхню складність і високу вартість.

Перспективи використання

У цей час все більша увага приділяється розвитку й удосконалюванню технологій, що використовують як біопараметричний параметр відбитки пальців і рисунок райдужної оболонки ока, як найбільш перспективні в змісті мінімізації помилок розпізнавання, добре пророблені. Разом з тим, зовсім ясно, що голос і особа людини також будуть використовуватися для ідентифікації.



Ри

Рисунок 1 – Статистика застосування біопараметричних систем

Опис біопараметричної системи

Біопараметрична система – це автоматична система, здатна:

– одержати біопараметричний зразок (наприклад, відбиток пальця) від людини;

– витягти з нього біопараметричні дані (наприклад, особливі точки і їхні параметри);

– зрівняти ці дані з одним або декількома даними такого ж сорту, що зберігаються в базі даних;

– визначити, наскільки добре збігаються пред'явлені дані з якимись даними з бази;

– зробити висновок про те, чи вдалося ідентифікувати людину за пред'явленим даними, або підтвердити (перевірити), що цей саме той, за кого він себе видає.

Оцінка якості роботи біопараметричних систем

Параметри якості

Робота біопараметричної системи описується рядом технічних і цінових параметрів. Важливими технічними параметрами, які позначаються на цінах і можливості використання для того або іншого застосування є наступні.

FAR (False Acceptance Rate) – помилка (імовірність) прийняти "чужого" за "свого"/помилка пропустити "чужого". У системах, що присутні на ринку, ця помилка в основному змінюється в межах від 10^{-3} до 10^{-6}, хоча є рішення й з FAR= 10^{-9}.

FRR (False Rejection Rate) – помилка (імовірність) прийняти "свого" за "чужого"/відмовити в доступі "своєму". Звичайно в комерційних системах ця помилка вибирається рівної приблизно 0,01. У ряді випадків є спеціальні вимоги (при великому

потоці, щоб не створювати черг) поліпшення FRR до 0, 001-0,0001. У системах, що є присутні на ринку, FRR звичайно перебуває в діапазоні 0, 025-0,01.

Варто помітити, що у всіх алгоритмах FAR і FRR зв'язані: чим краще один параметр, тим гірше інший. Тому системи з малим FAR гарні ще й тим, що, погіршуючи цей параметр, але залишаючи його ще досить гарним, ми можемо поліпшити FRR.

Третій досить важливий параметр – розмір моделі відбитка пальця. Його величина визначає швидкість порівнянь і обсяг пам'яті, необхідної для зберіганні бази відбитків (обсяг інформації про відбиток пальця може бути на 3-4 порядки більше, ніж у моделі). У більшості систем зберігаються саме моделі й тільки в міліцейських системах зберігаються зображення відбитків пальців.

Наступний параметр – швидкість порівняння інформації, що зберігається в базі, із пред'явленим для контролю відбитком пальця. Це параметр, обумовлений алгоритмом, розміром моделі й використовуваних обчислювальних потужностей. Велике значення має при значних обсягах баз.

Варто враховувати також швидкість зчитування відбитка пальця. Вона може становити від 0,1 до 2 секунд і визначається в основному типом сканера, засобами боротьби з муляжами, а також конструкцією сканера.

Ще один важливий параметр – можливість розпізнати муляж (копію відбитка пальця). Деякі групи сканерів завдяки використовуваній технології відразу відкидають деякі види муляжів, наприклад, ємнісні сканери відбитків пальців або сканери із сенсорами тиску відразу відкидають фотомуляж, тоді як самі примітивні оптичні сканери його пропускають. Проте розроблено й використовується для різних типів сканерів досить багато систем, що розпізнають муляжі.

Також важливо, які інтерфейси використовуються при передачі зображення від сканера в обчислювальну систему (це визначає загальну швидкодію системи), які засоби захисту використовуються при передачі біопараметричної інформації до обчислювального пристрою, що приймає рішення про дозвіл доступу.

Можуть бути названі й інші параметри – розміри, вага сканерів, їхня тривалість життя, припустимі умови експлуатації й т.п.

Набір параметрів досить великий. Можливості тестування системи в споживача обмежені. Це означає, що для ухвалення рішення про використання біопараметричних систем доступу доцільне залучення професіоналів для консультацій. І це стає особливо актуальним через швидкий ріст ринку.

Оцінка реальної якості біопараметричних систем

Коли ми читаємо щось на тему біопараметрики в засобах масової інформації й навіть у проспектах біопараметричних фірм, те найчастіше зустрічаємося із двома крайніми точками зору. Одна з них – рівень розвитку біопараметрики дуже високий, вирішені всі проблеми, друга – усе перебуває ще в зародковому стані, працює погано, придумані муляжі, які обманюють всі пристрої. Істина, як завжди, перебуває посередині, але тенденції розвитку позитивні. Повідомлення про те, що деякі системи працюють не так добре, як хотілося б і забезпечують не дуже високий рівень надійності, або пропускають деякі види муляжів по конкретних фактах не позбавлені підстави. При ближчому розгляді найчастіше виявляється, що була обрана більш дешева система, що вміє менше, ніж більш дорога. У принципі кращі алгоритми вже забезпечують рівні помилок:

– "пропустити чужого" (FAR) – не більш ніж 1 на мільярд;
– "не пропустити свого" (FRR) – не менш чим 1 на 1000.

Проблеми біопараметричних систем

Проблема №1

Стійкість значень деяких біопараметричних характеристик часто перебільшується. У реальній роботі система (наприклад, класу "Handkey") досить часто "не довідається" зареєстрованого користувача.

Крім помилок FAR і FRR існує помилка третього роду, коли приймається рішення "чужий" через неможливість одержати спостереження обраної біопараметричної характеристики. Наприклад, дактилоскопічний сканер не може зняти зображення через які-небудь недоліки шкіри, дуже малої кількості особливих точок або відсутності папіллярного візерунка.

На простому персональному комп'ютері сучасні програмні засоби біопараметричних систем дозволяють робити порівняння більше 10 000 відбитків у секунду, є технічні рішення, які виявляють будь-які придумані на сьогодні муляжі біопараметричних параметрів. Однак, якщо ми хочемо мати все, то коштує це поки що не дуже дешево.

Проблема №2

Для оцінювання співвідношень FAR/FRR проводять велику кількість випробувань системи з використанням спеціальних баз даних біопараметричних характеристик, знятих у різний час. На жаль, це робиться не всіма виробниками біопараметричних систем. Через цього ефективність біопараметричних систем, що вже існують на ринку, часто реально менш висока, чим це анонсується.

Для тестування дактилоскопічних систем є стандартні бази відбитків пальців NIST-9 і NIST-14, є також бази даних відбитків, знятих за допомогою різних ємнісних і оптичних сенсорів.

Незважаючи на "хвороби росту", уже зараз можна сказати, що, якщо в людини існує досить гарний біопараметричний параметр, тобто системи, які можуть забезпечити FAR на рівні 10^{-9}, FRR – $10^{-2(-3)}$ і не пропустити жоден з наявних муляжів. Це не дуже дешево, але є. На жаль, для біопараметрики біля відсотка людей не мають деякі біопараметричні характеристики. У людей з більмом немає рисунка райдужної оболонки, у деяких людей відбитки пальці майже не мають характерних рис, що стримує поширення цих технологій.

Проблема №3

Існує ряд проблем, пов'язаних з невірним розумінням технічних параметрів пристроїв. Можна побачити твердження, що розмір сенсора 12х12мм цілком достатній для коректного зняття відбитка пальця, а деякі фірми рекламують сенсори розміром 9х9мм. Однак, більша частина напівпровідникових сенсорів насправді має недостатню площу сканування, що погіршує якість біопараметричної системи. Часто виготовлювачі сенсорів говорять про дозвіл, маючи на увазі насправді кількість чутливих елементів матриці.

Методи розпізнавання відбитків пальців

Метод виявлення ключових точок

Кожний відбиток пальця складається з певної кількості борозен і смужок. Смуги – це підняті частини шкірного покриву, борозни – впалі частини. Смуги становлять так звані ключові точки: **край смуг** (там, де смуги закінчуються) і **роздвоєння** – там, де вони розгалужуються.

Під час реєстрації ключові точки розташовуються в певному місці а їхнє розташування відносно один одного і їхній напрямок реєструються. На основі цих даних створюється **зразок** (шаблон) – інформація, що згодом буде використана для посвідчення особи користувача.

На етапі зіставлення, облічене зображення відбитка пальця піддається попередній обробці, у ході якої витягають ключові точки. Вони зіставляються із зареєстрованим зразком, намагаючись розташувати в певному місці як можна більша кількість схожих точок у межах заданих границь. Результатом зіставлення, як правило, є набір ключових точок. Потім використовується поріг, що визначає, наскільки більшим повинне бути це число, щоб було можливо зіставити відбиток пальця зі зразком.

Переваги:

- Використовується в додатках AFIS;
- Широко відомий, добре досліджений метод;
- Алгоритм підходить для множинного зіставлення.

Недоліки:

- В зв’язку з тим, що метод висуває більші вимоги до дозволу й розмірів чутливого датчика, він може бути використаний не у всіх технологіях, що зчитують відбитки пальців. При використанні сканерів, менш зроблених, чим апаратура AFIS-класу, дає низькі результати;
- Люди, що не мають зовсім або які мають невелику кількість ключових точок (особливий стан шкірного покриву) не можуть користуватися даною системою. Кількість ключових точок може бути обмежуючим фактором для безпеки алгоритму;
- Можливі збої в системі через помилкові ключові точки (ділянку, що містить помилку, що виникла через низьку якість реєстрації, відтворення зображення або нечіткого відбитка смуг).

Метод зіставлення візерунків

Важливою властивістю алгоритму зіставлення візерунків є те, що в увагу приймаються не тільки окремо взяті точки, але й більші характеристики відбитка пальця. Ці характеристики можуть також включати певний відсоток додаткових даних, включаючи товщину смуг, їхню кривизну або щільність. У зв'язку із цією кількістю даних, що збільшилася, алгоритм, заснований на зіставленні візерунків, менш залежить від величини сканера й абсолютно не залежить від кількості ключових точок у відбитку пальця. Заснований на зіставленні візерунків алгоритм, на відміну від методу виділення ключових точок, не зустрічає складностей при розпізнаванні пальця з відбитком гіршої якості.

Запатентований алгоритм зіставлення візерунків Precise Biometrics під час реєстрації відбитка визначає наявність вищезгаданих додаткових характеристик. Невеликі ділянки відбитка й відстань між ними витягають із загальної картини з метою максимально збільшити кількість унікальної інформації. Найбільш значимі ділянки навколо ключових точок і ділянки з невеликим радіусом вигину. Основна структура й унікальні комбінації смуг також є коштовними даними.

Процес підтвердження починається з попередньої обробки ліченого зображення відбитка. Зареєстровані візерунки, що зберігаються в зразку, зіставляються з перевіряється изображением, що, відбитка, щоб визначити, наскільки зразок збігається із зображенням. Поріг, що описує найменше припустиме відхилення згодом використовується при визначенні ступеня відповідності відбитка наявному зразку.

Переваги:

– Прекрасно працює з усіма відомими типами сканерів відбитків пальців;
– Будь-який відбиток, якому можна записати, може бути зареєстрований, навіть якщо він не має або має невелику кількість ключових точок;
– Прекрасно підходить для здійснення роботи з недостатньою кількістю обчислювальних ресурсів, наприклад, смарт-картою.

Недоліки:

– Не може використовувати базу даних AFIS (однак, може використовувати неопрацьовані зображення);
– Не оптимізований для ідентифікації (тобто для встановлення конкретної особистості, для схеми «один до багатьох»).

Для перевірки коректності реалізації даної задачі було виконано багато розрахунків та експериментальних матеріалів. Цьому питанню приділялась особлива увага тому, що помилка при розрахунку привела б до ряду негативних наслідків. Відлагодження та перевірка, що підтверджує вірність програмних рішень відбувалась за декількаами етапами:

– математична перевірка окремих модулів;
– математична перевірка всієї системи (з допомогою математичної логіки будується логічна схема всієї системи);
– практична перевірка підпрограм (перевіряється процедурна частина кожної підпрограми окремо);

– практична перевірка всієї системи у дії (перевіряється ситема в цілому за допомогою вводу різних даних у програму, потім на виході з програми перевіряємо отриману інформацію з очікуваною).

Для підтвердження правильності розрахунку програми були використані експериментальні дані різних форматів, були проведені консультації з даного питання зі спеціалістами.

Простота мови проектування та маніпулювання даними, зручність спілкування користувача з системою до мінімума вивчення цієї програми. Користувач програми – це людина, яка повинна володіти азами програмування. При написанні програми я намагалася, щоб програма відповідала наступним параметрам:

– Швидкодія. Програма працює постійно з великою кількістю кінцевих абонентів (селективний зв'язок).

– Захист. Забезпечити надійний захишенний канал зв`язку.

– Відсутність проблеми дорожнечі сучасних персональних комп'ютерів. Система, що написана може встановлюватись на будь-якому персональному комп'ютері – використовувати відносно швидкі алгоритми захисту зв'язку.

– Можливість зручно і швидко формувати приклади і теорію для користувача.

– Можливість звертання до системних ресурсів. Користувача системи цікавить її інформаційний та сенсовий зміст. Подробиці організації фізичного зберігання даних його не цікавлять.

Перш за все перед розробкою системи слід одержати уявлення на слідуючи моменти:

- на які частини можна розбити систему;
- одержати уявлення про кожну частину (фрагмент);
- яка інформація і з якою детальністю необхідна користувачу кожного фрагменту;
- які процеси передачі і обробки даних знаходяться в кожному фрагменті;
- технологія накопичування і обробки аудіо інформації системи;
- на якому обладнанні планується реалізувати систему;
- технологія функціонуваня системи;
- чи необхідна адаптація і настройка системи при змінах деяких умов.

Для розробки програми були попередньо розроблені структурна схема роботи системи, структурна схема формату передачі даних, функціональна схема роботи системи, діаграма процесів, а також блок-схеми алгоритму програми, розглянемо їх детально.

Створена автором система біометричного доступу до даних у хмарному сервісі складається із двох частин – клієнтської частини на стороні користувача й серверної частини що перебуває віддалено в Інтернеті. Створена система універсальна. Застосовуючи стандартизовані бібліотеки Bioparametrs Aplication Programming Interface і використовуючи стандартизований формат передачі повідомлень (розділ 3.8) користувач може використовувати будь-які біопараметричні сканери. При створенні й тестуванні системи автор використовував два біопареметричні сканери, а саме – сканер відбитків пальців MorphoSmart 1300 Sagem для розпізнання папілярного малюнка пальця й планшетний сканер SignatureGem 1x5 розпізнавання підпису людини.

Клієнтська частина виконана у вигляді Active X додатка з застосуванням стандартизованої бібліотеки Bioparametrs Aplication Programming Interface 1.1 і застосовна з Internet Explorer версії 4.0 і вище, а також у будь-яких інших програмах, що підтримують роботу з Active X компонентами.

Робота програмного забезпечення із застосуванням стандартизованих бібліотек Bioparametrs Aplication Programming Interface показана на рисунку 3.6.

Серверна частина виконана у вигляді модуля COM і повністю сумісна з IIS сервером із застосуванням стандартної бази даних від корпорації Майкрософт – Microsoft Access з інтерфейсом ODBC.

Для подальшого розуміння роботи розробленої системи введемо наступну термінологію.

Навчання – процедура зняття серії відбитків того самого пальця або інших біопараметричних характеристик (підпис людини, форма руки, і.т.буд.) з метою відбору деякої їхньої кількості з найбільше яскраво вираженими особливостями, чим ці особливості більше виділені тим краще **якість зразка** поняття прямо пов'язане із застосовуваними апаратними засобами зняття біопараметричних характеристик. У деяких випадках зразок непридатний для розпізнавання через різні причини (наприклад у випадки зняття відбитків пальців забруднення).

Паспорт – еталонний зразок (перевірений 100% зразок) для ідентифікації особи.

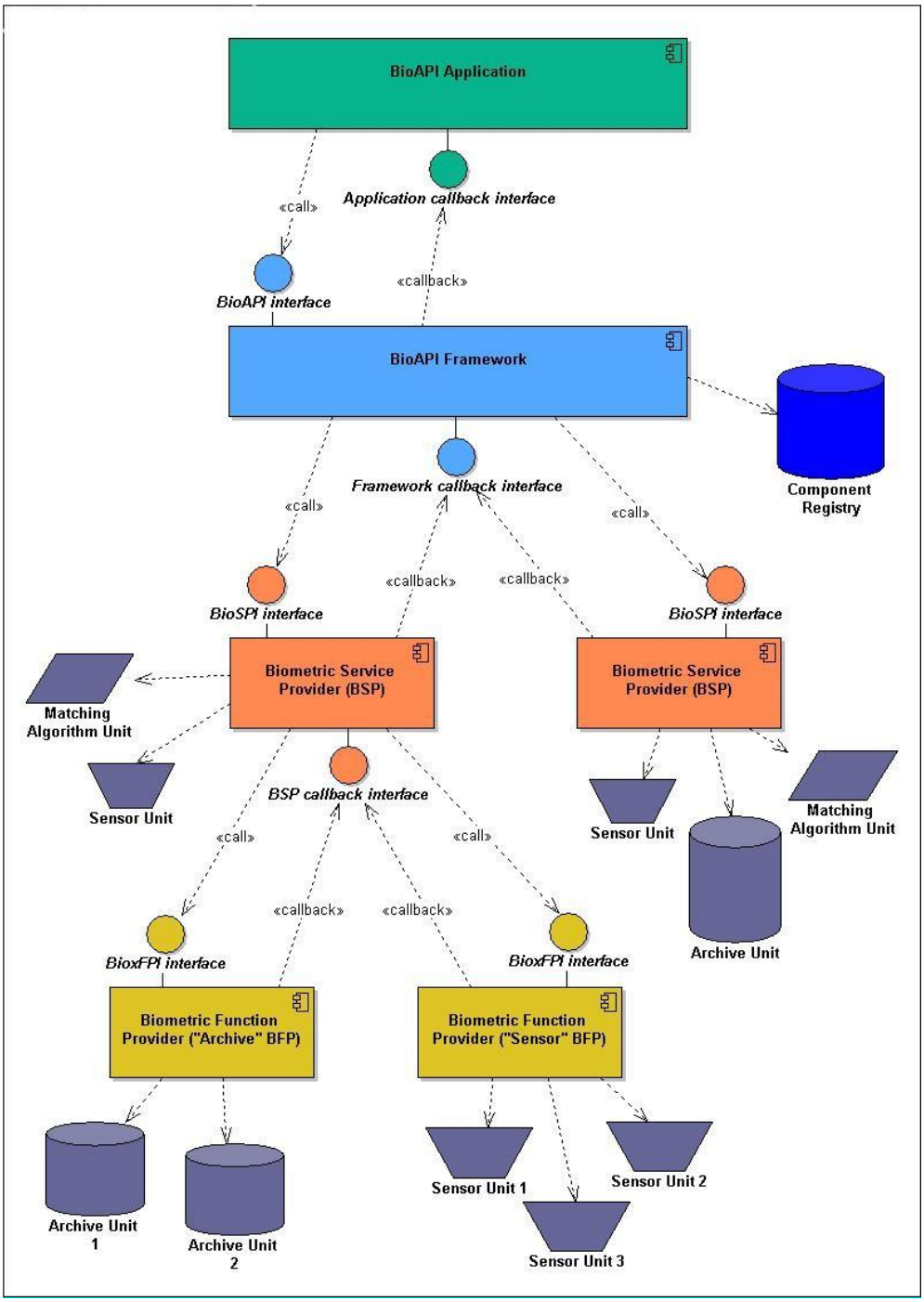


Рисунок 2 – Робота та взаємодія ПЗ з Bioparametrs Aplication Programming Interface

Модель – математичний образ (пакет даних) відбитка пальця, одержуваного з біопараметричного сканера, а також **біометричний ідентифікаційний запис** і **криптографічне додавання**. Модель необхідний запис для **розпізнавання** користувача й надання йому прав.

Біометричний ідентифікаційний запис (BIR, BSP) – група даних з **моделі** відповідальних за біопараметричні характеристики (використовуваний сканер, якість зразка, опис тип даних і т.д.).

Криптографічне додавання – група даних з **моделі** відповідальних за автентифікацію.

Розпізнавання – процедура порівняння Моделі й Паспорти, результатом якої є вивід про їхню ідентичність і видачі коду перевірки.

Розглянемо докладніше особливості реалізації й взаємодії клієнтської частини із серверної зображеної на рисунку 3.

Розглянемо схему знизу нагору, при одержанні з біопараметричного сканера даних на стороні клієнта розроблений Active X компонент використовуючи бібліотеку BIOAPI перевіряє якість отриманого зразка й формує біометричний ідентифікаційний запис (розділ 3.8) складається з 32 кілобайт інформації. Далі відбувається додавання криптографічного додавання (40 Кб) підтверджувального, що цей запис є записом користувача, формат запису стандартизований на території України. Після формування біометричного ідентифікаційного запису й криптографічного додавання відбувається остаточне формування моделі для перевірки користувача.

Зі сторінки доступу модель передається через Інтернет на серверну частину системи де обробляється скриптом доступу й надходить в DCOM модуль автентифікації де відбувається перевірка на відповідність. При позитивному проходженні перевірки й добуванні біометричного ідентифікаційного запису. DCOM модуль витягає з Microsoft Access паспорт користувача. Відбувається біопараметричне зіставлення даних і повернення клієнтові коду результату.

Розглянемо необхідність застосування технологій компонента Active X і COM модулів при розробці клієнтської й серверної частини системи.

Як відоме написання Active компонент і COM на основі моделі компонентних об'єктів дозволяє вбудовувати розроблені програми в різні джерела, такі як HTML сторінки використовуючи JavaScrpt, PHP скріпти, Pearl скріпти й т.ін., що приводить до універсальності. Виходячи з поставленого завдання застосування даної технології доцільно. Знаючи всього CLSID Active X компонента, ми одержуємо волю вибору в застосуванні в різних джерелах.

CLSID розробленого Active X об'єкта – "**CLSID:7D6416 BB-4417-4B 92-B564-A39A474DC84E**" (він унікальний).

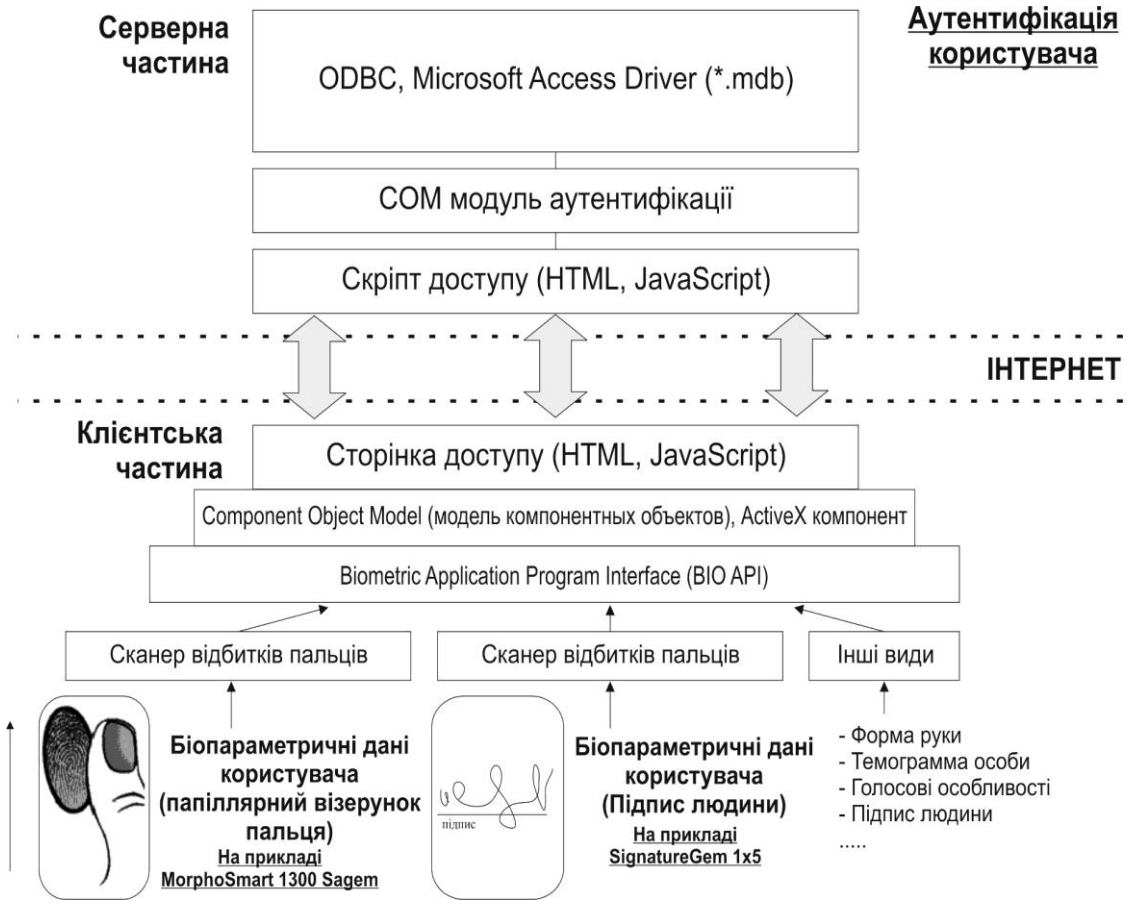


Рисунок 3– Структурна схема системи

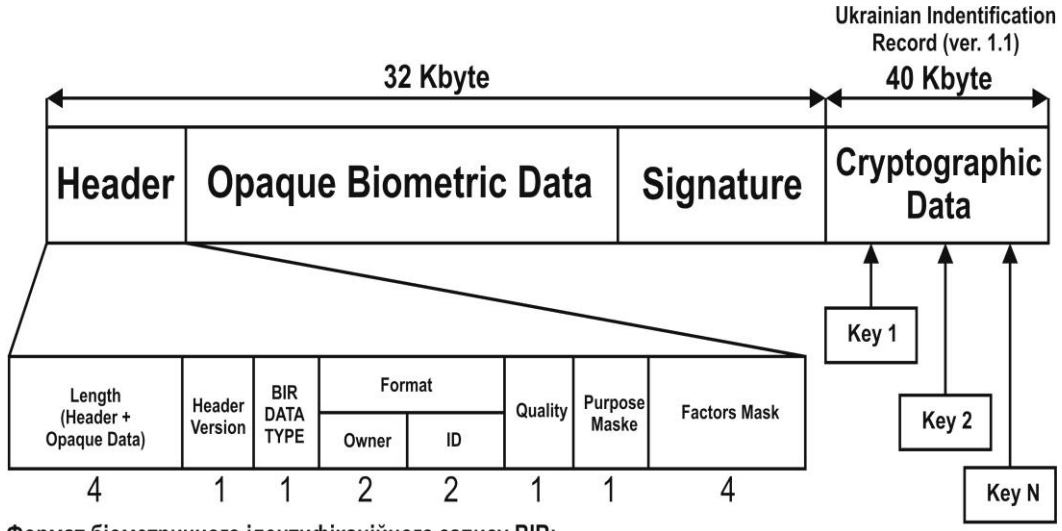
Для функціонування серверної частини системи, побудованої із застосуванням COM модуля, не буде потрібно здобувати ніяких додаткових апаратних засобів. Це дуже зручно для проектів з невеликою клієнтською базою. У випадку більших вимог до швидкості й обсягу розпізнавання в передбачені технології нарощування продуктивності із застосуванням програмних засобів від Майкрософт. Безсумнівний плюс такого підходу – можливість поступового нарощування продуктивності системи в міру росту клієнтської бази, чим забезпечується оптимізація й мінімізація витрат на експлуатацію системи.

Серверна частина через вибір COM модуля підтримує всі існуючі на даний момент технології масштабування й вирівнювання навантаження додатків від Майкрософт: Network Load Balancing, Component Load Balancing, Application Center, Object Pooling, JIT activation.

Розглянемо формат передачі даних, які складаються з біометричного ідентифікаційного запису й українського криптографічного додавання, зображених на рисунку 3

Основним терміном інтерфейсу BioAPI є біометричний ідентифікаційний запис – BIR (Biometric Identification Record), яку можна визначити як набір біометричних даних, з яким працюють додатки й провайдери послуг. У загальному BIR – це єдиний формат, пропонований для заміни й об'єднання самих різних форматів подання біометричних даних устаткуванням і програмним забезпеченням різних виробників.

Формат BIR, його структура й состав, затверджені Національним інститутом стандартів і технології США NIST, Росії, України й інших країн, а також затверджено Common Biometric Exchange File Format (CBEFF, узагальнений формат обміну біометричними даними). BIR складається із трьох секцій даних: заголовка, біометричних даних і електронного цифрового підпису. Далі розглянемо пояснення до полів BIR по специфікації BioAPI 1.1.



Формат біометричного ідентифікаційного запису BIR:

Length - довжина заголовка й біометричних даних;
Header Version - версія заголовка BIR;
BIR Data Type - тип даних BIR;
Format (Owner/ID) - опис формату біометричних даних;
Quality - якість (необхідно для деяких типів біометричних даних);
Purpose Mask - ціль: верифікація, ідентифікатор по імені користувача, ідентифікація, реєстрація для ідентифікації, аудит)
Factors Mask - використовуваний метод біометрії;
Opaque Biometric Data - біометричні дані;
Signature - поле електронно-цифрового підпису;
Record Data Type - тип біометричних даних;
Creation Date - дата створення BIR, час і день одержання біометричних даних;
Creator - ідентифікатор творця BIR.

Рисунок 4 – Структурна схема формату передачі даних

Сектор **Заголовок BIR** (Header) містить у собі наступні поля:

– **Length** – довжина, сума розміру заголовка й біометричних даних;

– **Header Version** – версія заголовка BIR;

– **BIR Data Type** – тип даних BIR. Насправді по стандарті CBEFF формування даного заголовка це поле носить інша назва, більш точно його визначальне: Опції захисту (Security options). У цьому полі вказується тип захисту біометричних даних (1 з 4 значень): тільки біометрія (немає захисту), криптографія, ЕЦП, криптографія й ЕЦП;

– **Format** (**Owner/ID**) – опис формату біометричних даних, представлених після заголовка BIR. Всі формати біометричних даних, підтримуючих BioAPI, реєструються в Міжнародній промисловій біометричній асоціації IBIA (International Biometric Industry Association).

Поле складається із двох підполей:

– Власник формату, тобто компанія, що зареєструвала даний формат подання біометричних даних, формат може бути декількох типів. У Додатку наведений список всіх зареєстрованих форматів подання біометричних даних.

– Ідентифікатор формату – номер використовуваного формату із зареєстрованих власником.

– **Quality** – якість, для деяких типів біометричних даних необхідно вказувати дане значення. Якість вказується в проміжку від 0 до 100. Якщо зазначено «-1» то якість не задана, якщо «-2», те в даному біометричному методі таке поняття як «якість» не використовується.

– **Purpose Mask** – ціль, з якої будуть використані біометричні дані. У даному полі вказується одне із шести значень:

1. верифікація (порівняння «один до одного», користувач називає своє ім'я й пред'являє ідентифікатор, по імені користувача шукається шаблон його ідентифікатора й вони рівняються);
2. ідентифікація (порівняння «один до багатьох», користувач пред'являє свій ідентифікатор, і в базі шаблонів шукається найбільш близький до нього);
3. реєстрація;
4. реєстрація тільки для верифікації;
5. реєстрація тільки для ідентифікації;
6. аудит.

– **Factors Mask** – використовуваний метод біометрії. У цей час зареєстровано 19 методів розпізнавання (можливе розширення даного списку при твердженні наступної версії формату):

– комбінація методів;
– форма особи;
– голос;
– відбиток пальця;
– сітківка ока;
– райдужна оболонка;
– геометрія кисті руки;
– динаміка підпису;
– динаміка клавіатурного набору;
– рух губ;
– термографія особи;
– термографія руки;
– хода;
– запах тіла;
– ДНК;
– форма вуха;
– геометрія пальця;
– геометрія долоні;
– малюнок вен на руці.

Сектор **Біометричні дані** (Opaque Biometric Data) – містить безпосередньо біометричні дані, використовувані для розпізнавання людини, відповідно до зареєстрованого формату, зазначеним у заголовку BIR у поле Format.

ЕЦП (Signature) – поле, у яке заноситься електронний цифровий підпис. Поле є опціональним. Якщо ЕЦП використовується, то підписуються разом і заголовок BIR, і біометричні дані.

Крім цього в заголовку BIR існує також декілька опціональних полів, актуальних не для всіх біометричних методів розпізнавання:

– **Record Data Type** – тип біометричних даних, що втримуються. Передані в складі BIR біометричні дані можуть бути трьох типів: неопрацьовані, преоброблені, оброблені;

– **Creation Date** – дата створення BIR, час і день одержання біометричних даних;

– **Creator** – ідентифікатор творця BIR.

В інтерфейсі BioAPI визначені два рівні:

– верхній, визначальний інтерфейс клієнтського й серверного додатків, що викликає функції автентифікації;

– нижній, визначальний інтерфейс взаємодії із провайдером біометричних послуг (Biometric Service Provider), що виконують виклики верхнього рівня.

Верхній рівень (у версії 1.0 має назву «H», high) визначає три основних функції, необхідних додатку для проведення біометричному автентифікації:

1. **Enroll** (реєстрація). Вимір з біометричного пристрою, що зчитує, обробляються в придатну для використання форму, з якої формується шаблон, що повертається додатку;

2. **Verify** (верифікація, порівняння «один до одного»). Одна або більша кількість вимірів знімається з біометричного пристрою, обробляється в придатну для використання форму й потім рівняється з відповідним шаблоном. Результати порівняння вертаються додатку;

3. **Identify** (ідентифікації, порівняння «один до багатьох»). Одна або більша кількість вимірів знімається з біометричного пристрою, обробляється в придатну для використання форму й рівняється з набором шаблонів. Як результат вертається список, що показує, наскільки близько виміру збігаються з найближчими кандидатами на ідентифікацію з набору шаблонів.

Нижній рівень, SPI (service provider interface) – визначає інтерфейс до провайдеру біометричних послуг (BSP – Biometric Service Provider), у якості якого можуть виступати практично будь-які підтримуючі цей інтерфейс біометричні системи, пристрої або програмні продукти . Функцією SPI є відображення «один до одного» викликів верхнього рівня у виклики до BSP.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів біометричного доступу до даних у хмарному сервісі. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем біометричного доступу до даних у хмарному сервісі. Досліджена система біометричного доступу до даних у хмарному сервісі. На основі отриманих результатів досліджень створена програмна реалізація системи біометричного доступу до даних у хмарному сервісі. Розроблені алгоритми дозволяють успішно вирішувати завдання біометричного доступу до даних у хмарному сервісі. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational

Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

І. Колодяжний, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЛЯ БЛОКУВАННЯ ВХІДНИХ ВУЗЛІВ TOR І СЕРВЕРІВ VPN-ПРОВАЙДЕРІВ

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Метою розробки є дослідження та програмна реалізація системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Об’єктом дослідження є процес кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Предметом дослідження є методи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерна інженерія, Tor, VPN

Постановка проблеми. Суттєвий прогрес і поширення інформаційних технологій, глобальний характер систем масової комунікації призвели до утворення глобального інформаційного простору, який змушує світову спільноту, кожну державу швидко орієнтуватися та адаптуватися у сучасному інформаційному середовищі. Світове співтовариство в цих умовах усвідомило, що міжнародна інформаційна безпека є проблемою, розв’язання якої суттєво впливає на існування людства. Тобто з розвитком і поширенням інформаційно-комунікаційних технологій у всі сфери життєдіяльності надзвичайної значимості набувають питання забезпечення інформаційної безпеки, визнаної в нашій країні однією з найважливіших складових національної безпеки, як багаторівневої проблеми державної інформаційної політики. Відзначимо, що статтею 17 Конституції України інформаційну безпеку визначено найважливішою функцією держави, справою всього Українського народу [1].

Необхідність протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо є одним із основних завдань забезпечення інформаційної безпеки і вкрай важливим для української держави на сучасному етапі. Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам.

Поширення комп’ютерних вірусів, шахрайство, крадіжки коштів із банківських рахунків або електронних гаманців, викрадення персональної та комерційної інформації,

порушення правил роботи комп'ютерних систем – це далеко не повний перелік кіберзлочинів, кількість яких з кожним днем збільшується. Причинами цього є: анонімність, що ускладнює виявлення злочину, злочинця; простота швидкого збагачення, доступність інтернет-інформації, яка тільки дозволяє вчиняти неправомірні діяння в мережі Інтернет [7]. Так, наприклад, за підсумками 2020 року головними загрозами для бізнесу стали крадіжки облікових даних і уразливості [8]. В руки кіберзлочинців потрапляє все більше ключів, які відкривають доступ до нашого приватного життя і роботи. Їм більше не потрібно витрачати час на винахід хитрих способів проникнення в компанію – злочинці можуть проникати в мережу і проводити атаки, просто використовуючи відомі методи, такі як вхід в систему з вкраденими обліковими даними [8]. Кіберзлочинці активно стимулюють соціально-політичну активність громадян, вказуючи їм конкретні напрями та завдання діяльності, підказуючи шляхи та засоби вирішення проблем, що стоять перед ними за допомогою методів переконання, які одержали потужний розвиток впродовж ХХ сторіччя. Важко знайти будь-який інший інструмент переконання чи навіювання, що порівнюється з пропагандою за ефективністю закріплення в свідомості певних поглядів та ідей.

За публічною інформацією СБУ, ворожа пропаганда активно реалізовується через соціальні мережі. Так, наприклад, на Кіровоградщині за засуджено антиукраїнського Інтернет-агітатора. Співробітники спецслужби встановили, що місцевий житель публікував у заборонених соціальних мережах матеріали із закликами до масових заворушень, збройного протистояння з правоохоронними органами, закликав приєднуватися до незаконних збройних формувань [2].

На Чернігівщині співробітники Служби безпеки України під процесуальним керівництвом прокуратури викрили адміністратора антиукраїнських спільнот у соціальних мережах. Правоохоронці встановили, що мешканець Прилуцького району створював у соцмережах акаунти, через які адміністрував антиукраїнські групи. Оперативники спецслужби задокументували, що зловмисник розповсюджував матеріали, які містили заклики до зміни меж території України, повалення конституційного ладу та державної влади, пропагував діяльність терористичних організацій «Л/ДНР», поширював інформацію, що дискредитує Збройні Сили України [3].

На Дніпропетровщині СБУ викрила підготовку РФ до втручання у вибори Президента України у 2018 році [4]. Співробітники СБУ під час виконання завдань із контррозвідувального захисту інтересів держави у сфері інформаційної безпеки протягом серпня викрили та заблокували діяльність мережі Інтернет-агітаторів, яких російські спецслужби залучили до заходів із підготовки до втручання у хід проведення виборів Президента України. Оперативники СБ України встановили, що російські спецслужби залучили до «співпраці» через комунікативні можливості Інтернету мешканців міст Дніпро, Кривий Ріг та Нікополь, які є адміністраторами груп у соціальних мережах. Спецслужби РФ поставили задання із підготовки «плацдарму» для проведення заздалегідь запланованих заходів із впливу на хід проведення майбутніх виборів Президента України через маніпулювання громадською думкою Інтернет-користувачів [4].

За матеріалами Служби безпеки України засуджено жителя Черкащини, який проводив антиукраїнську агітацію у соціальних мережах [5].

СБУ припиняє діяльність антиукраїнських адміністраторів у соцмережах. Наприклад, співробітники СБ України протягом липня 2018 року припинили у п'ятьох областях країни діяльність одинадцятьох адміністраторів у соцмережах, які розміщували в інтернеті антиукраїнські матеріали за вказівкою кураторів з російських спецслужб. Під час реалізації комплексу заходів із забезпечення інформаційної безпеки країни співробітники Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки та обласних управлінь СБ України виявили нові докази використання спецслужбами РФ соціальних мереж для шкоди державній безпеці нашої країни [6]. На Дніпропетровщині СБУ припинила діяльність мережі антиукраїнських Інтернет-провокаторів, які у заборонених

російських соціальних мережах провокували Інтернет-користувачів до масових заворушень у День Конституції України 2018 року [7].

Отже, виходячи з вище перерахованих інцидентів – вкрай важливо реалізувати систему протистояння анти-українській пропаганді, що розповсюджується за допомогою соціальних мереж.

Таким чином в Україні запроваджено протидію пропаганді в соцмережах (Указ Президента України від 15.05.2017 №133/2017 "Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"). Його суть полягає у забороні інтернет-провайдерам надавати послугу з доступу користувачів інтернету до сервісів, російського виробництва "Вконтакте", "Одноклассники" та ін. Проте, як показує практика, реалізований підхід до забезпечення інформаційної безпеки держави не є ефективним. Адже, наприклад, заблоковані веб-сайти як і раніше входять в ТОП-10 найвідвідуваніших сайтів в Україні, оскільки користувачі активно використовують VPN, Tor, Opera та інші способи "обійти" блокування [2].

Отже, запроваджений підхід до протидії розповсюдженню пропаганді в соцмережах не є ефективним та потребує удосконалення шляхом запровадження додаткового блокування Tor, VPN і сайтів з інформацією про обхід заблокованих ресурсів. Це дозволить підвищити ефективність протидії пропаганді сепаратизму і антиукраїнської ідеології у Інтернеті, в тому числі в соціальних мережах.

Отже, метою виконання магістерської дипломної роботи є підвищення ефективності протидії пропаганді сепаратизму і антиукраїнської ідеології у Інтернеті, в тому числі в соціальних мережах, за допомогою реалізації програмного забезпечення системи блокування вхідних вузлів Tor і серверів VPN-провайдерів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів.

Метою й завдання досліджень і публікацій. Метою роботи є дослідження та програмна реалізація системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів.

– Дослідження системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів.

– Програмна реалізація системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів.

Об'єктом дослідження є процес кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів.

Предметом дослідження є методи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис функціонування системи.

Система буде функціонувати таким чином, відправляється запит на відображення веб-ресурсу до сервера провайдера, запит, який містить доменне ім'я, приймає система та перевіряє чи наявне запитуванне доменне ім'я в базі даних. У випадку, якщо доменне ім'я наявне в базі даних – система, за допомогою реалізованого DNS-серверу, повертає DNS-відповідь, яка містить в собі адресу локального серверу.

База даних «чорний список», котрий містить заборонені IP/URL. Для роботи з базою даних передбачається графічний інтерфейс. Перше, що необхідно зробити – ввести пароль, якщо пароль введений правильно – відображається головне меню, інакше – повідомлення про неправильний пароль. В головному меню є можливість додавання доменного імені та IP, пошук доменного імені, видалення доменного імені, завантаження записів, виведення інформації про розробника.

Розробка структурної схеми

Структурна схема, яка зображена на рисунку 1, являє собою графічний опис структури системи. На структурній схемі зображені користувачі, локальний просторій, провайдер, сукупність серверів, що складають мережу Інтернет та веб-сторінка, яка зберігається на одному з серверів в мережі Інтернет.

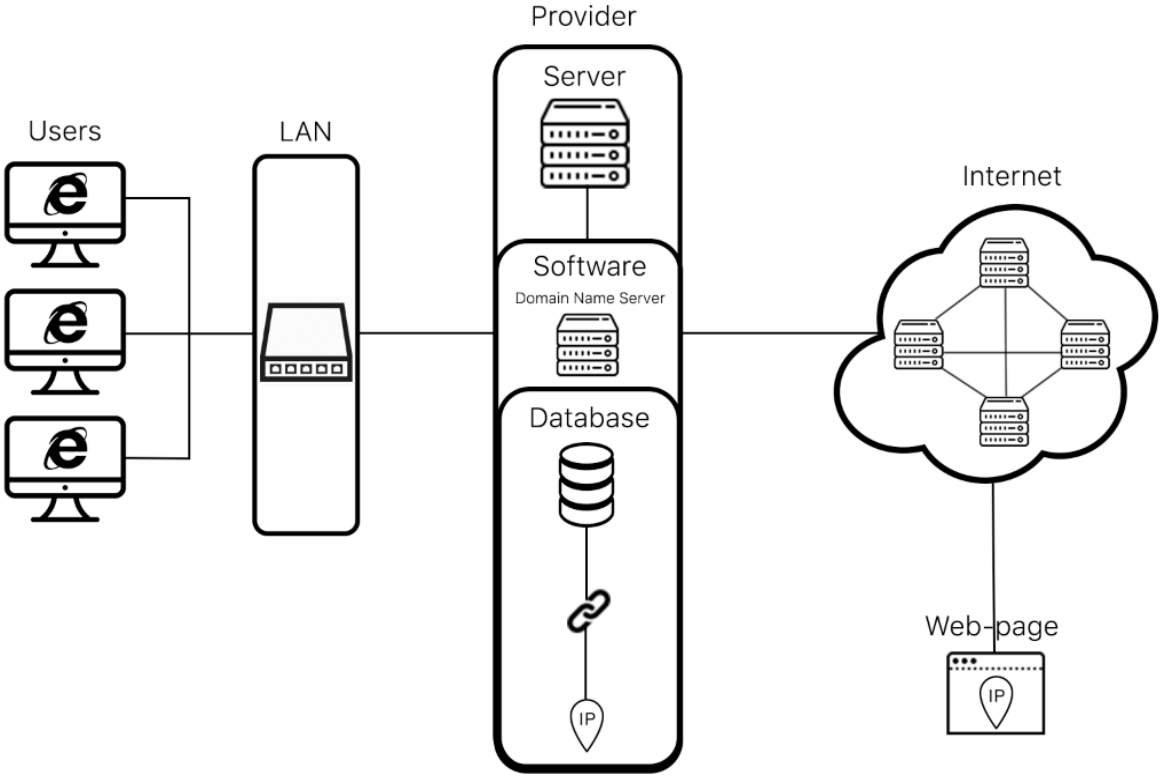


Рисунок 1 – Структурна схема системи

В свою чергу, провайдер містить в собі сервер, на якому встановлена власне сама система, що складається з DNS-серверу та бази даних, у якій зберігаються доменні ім’я та IP, доступ до яких повинен бути заблокований.

Висновки. У статті наведене теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Досліджена система кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Розроблені алгоритми дозволяють успішно вирішувати завдання кібербезпеки для блокування вхідних вузлів Tor і серверів VPN-провайдерів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

В. Капкан, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ СИЛОВОЇ ІНФРАСТРУКТУРИ ЦОД

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки силової інфраструктури ЦОД. Метою розробки є дослідження та програмна реалізація системи кібербезпеки силової інфраструктури ЦОД. Об’єктом дослідження є процес кібербезпеки силової інфраструктури ЦОД. Предметом дослідження є методи кібербезпеки силової інфраструктури ЦОД. Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи кібербезпеки силової інфраструктури ЦОД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, кібербезпека, силова інфраструктура, ЦОД

Постановка проблеми. Коли оператори центрів обробки даних розглядають питання кібербезпеки, вони звичайно думають про захист своєї IT-інфраструктури й розташовуваних у ЦОД даних. А коли вони думають про забезпечення безпеки своїх джерел електроживлення, вони думають про альтернативні джерела електрики, а також про обмеження фізичного доступу до своєї енергетичної інфраструктури.

Генератори, джерела безперебійного живлення й блоки розподілу живлення – все це допомагає забезпечувати й контролювати електроживлення центрів обробки даних. Але фахівці рідко приділяють досить увагу контролю кібербезпеки у своїх енергосистемах, хоча ці системи досить уразливі для кібератак. І, як це не парадоксально, деякі із систем, використовуваних для захисту інфраструктури, можуть самі по собі являти загрозу безпеки.

Більшістю енергетичних устаткувань у центрі обробки даних можна управляти дистанційно й точно також налаштовувати його через віддалені термінали. Завдяки цьому зловмисник у теорії може одержати контроль над цими пристроями й перервати подачу електроживлення в центр обробки даних або на конкретний пристрій у мережі ЦОД.

Деякі із цих систем керування можуть потрапити в категорію інтернету речей (IoT), а якщо точніше – у сегмент промислового інтернету речей (IIoT). Пристрої класу IIoT є частиною невидимої інфраструктури центра обробки даних, що перебуває в «сірій зоні» між сферами відповідальності фахівців з керування фізичною інфраструктурою й фахівців з кібербезпеки.

Відповідно до доповіді організації Darktrace базованої в Сан-Франциско (США), кількість атак на IoT-пристрої зросло на 100 відсотків торік. А відповідно до опитування, проведеному торік організацією SANS Institute, тільки 40 відсотків компаній впроваджують патчи й фікси для захисту пристроїв IIoT.

При цьому цілих 56 відсотків респондентів заявили, що складності при впровадженні таких виправлень є однією із самих серйозних проблем безпеки для їхніх компаній. Крім того, майже 40 відсотків опитаних заявили, що в них виникли проблеми з пошуком відповідних пристроїв, відстеженням і керуванням ними.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи кібербезпеки силової інфраструктури ЦОД

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи кібербезпеки силової інфраструктури ЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем кібербезпеки силової інфраструктури ЦОД.

– Дослідження системи кібербезпеки силової інфраструктури ЦОД.

– Програмна реалізація системи кібербезпеки силової інфраструктури ЦОД.

Об’єктом дослідження є процес кібербезпеки силової інфраструктури ЦОД.

Предметом дослідження є методи кібербезпеки силової інфраструктури ЦОД.

Методи дослідження базуються на методах теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Інтерес до різних IoT-пристроїв з боку зловмисників продовжує рости: за першу половину 2020 року ми одержали в три рази більше зразків шкідливого ПЗ, що атакує «розумні» пристрою, чим за весь 2021 рік. До слова, в 2021 їх було в 10 разів більше, ніж в 2018 році. Як бачите, тренд «чим далі, тим гірше» простежується дуже добре.

Ми вирішили вивчити, які вектори атак використовуються зловмисниками для зараження «розумних» пристроїв, які зловреди завантажуються в систему в результаті успішної атаки, а також чим все це може обернутися для власника пристрою й просто жертв нового ботнету.

Одним із самих популярних векторів атак і, відповідно, зараження пристроїв усе ще залишається перебір пароля Telnet. У другому кварталі 2020 року таких атак на ханипоти було в 3 рази більше, ніж всіх інших разом узятих.

Найчастіше зловмисники завантажували на IoT-пристрої один зі зловредів сімейства Mirai (20,9%).

Отже, у другому кварталі 2020 року лідером по кількості унікальних IP-адрес, з яких виходили атаки через перебір пароля Telnet стала Бразилія (23%). Друге місце, з невеликим відривом, зайняв Китай (17%). Росія ж у нашім списку зайняла 4-ое місце (7%). Усього за період з 1 січня по липень 2020 року на наших Telnet-ханипотах було зафіксовано більше 12 мільйонів атак з 86 560 унікальних IP-адрес, а шкідливе ПЗ завантажувались із 27 693 унікальних IP-адрес.

Оскільки частина власників «розумних» пристроїв змінює штатний пароль Telnet на більше складний, а багато хто гаджети й зовсім не підтримують цей протокол, зловмисники перебувають у постійному пошуку нових шляхів зараження. Цьому сприяє й висока конкуренція між вірусописьменниками, яка привела до зниження ефективності атак з перебором пароля: у випадку успішного злому пристрою його пароль міняється, а доступ до Telnet блокується.

Як приклад використання «альтернативної техніки» можна привести ботнет Reaper, у його активі за станом на кінець 2017 року налічувалося близько 2 мільйонів IoT-пристроїв. Замість перебору паролів до Telnet цей ботнет експлуатував відомі уразливості в ПЗ:

– Уразливості в прошиванні роутера D-Link 850L.
– Уразливості в IP-камерах GoAhead.
– Уразливості в CCTV камерах MVPower.
– Уразливість в Netgear ReadyNAS Surveillance.
– Уразливість в Vacron NVR.
– Уразливість у пристроях Netgear DGN.
– Уразливості в роутерах Linksys E1500/E2500.
– Уразливості в роутерах D-Link DIR-600 і DIR 300 – HW rev B
– Уразливості в пристроях AVTech.
– Переваги такого способу поширення в порівнянні з перебором пароля:
– Зараження відбувається значно швидше.

Закрити уразливість у ПЗ значно складніше, ніж перемінити пароль або відключити/заблокувати сервіс.

Незважаючи на те, що цей спосіб складніше в реалізації, він прийшовся до смаку багатьом вірусописьменикам і нові троянци, що використовують відомі уразливості в ПЗ «розумних» пристроїв, не змусили себе довго чекати.

Нові атаки – старі зловреди

Щоб подивитися, які уразливості намагаються експлуатувати зловреди, ми проаналізували дані про спроби підключень до різних портів на наших пастках.

Поки переважна більшість атак – це усе ще перебір паролів Telnet і SSH. На третім місці по популярності перебувають атаки на сервіс SMB, що надає віддалений доступ до файлів. Ми поки не бачили IoT-зловредів, що атакують цей сервіс. Однак деякі його версії містять серйозні відомі уразливості – EternalBlue (Windows) і EternalRed (Linux) -за допомогою яких, наприклад, поширювався сумно відомий троянець-шифрувальник WannaCry і шкідливий майнер криптовалюти Monero EternalMiner.

Як можна помітити, з більшим відривом лідирують пристрою компанії MikroTik, що працюють під керуванням RouterOS. Причина, як видно, в уразливості Chimay-Red. 1

Порт 7547

Досить популярні атаки на сервіс віддаленого адміністрування пристроїв (специфікація TR-069), що працює на порту 7547. По даним Shodan, у світі налічується більше 40 мільйонів пристроїв, у яких цей порт відкритий. І це незважаючи на те, що ще не

дуже давно уразливість стала причиною зараження мільйона роутерів Deutsche Telekom, а також «допомогла» поширенню зловредів сімейств Mirai і Hajime.

Ще один тип атак експлуатує уразливість Chimay-Red у роутерах MikroTik під керуванням RouterOS версії нижче 6.38.4. У березні 2020 року з її допомогою активно поширювався Hajime.

IP-камери

Зловмисники не обійшли стороною й IP-камери: у березні 2017 року в ПЗ пристроїв GoAhead було виявлено трохи серйозних уразливостей, а через місяць після публікації інформації про це з'явилися нові модифікації троянців Gafgyt і Persirai, що експлуатують ці уразливості. Уже через тиждень після початку активного поширення цих зловредів число заражених пристроїв виросло до 57 тисяч.

8 травня 2020 року був опублікований proof-of-concept до уразливості CVE-2020-10088 веб-сервера XionMai uc-httpd, що використовується в деяких «розумних» пристроях китайських виробників (наприклад, відеореєстратор KKMoon DVR). Уже наступного дня зареєстрована кількість спроб виявити пристрої, що використовують даний веб-сервер, виросла більш ніж в 3 рази. Винуватцем такого сплеску активності став троянець Satori, що раніше атакував роутери GPON.

Нові зловреди й погроза кінцевому користувачеві

DDoS-атаки

Головним завданням, що зловмисники вирішують за допомогою IoT-зловредів, була й залишається організація DDoS-атак. Заражені «розумні» пристрої стають частиною ботнету, що по команді починає атакувати зазначену адресу, позбавляючи хост можливості нормально обробляти запити реальних користувачів. Такими атаками, наприклад, продовжують займатися троянци сімейства Mirai і його клони, зокрема, зловред Hajime.

Це, мабуть, найбільш необразливий сценарій для кінцевого користувача. Максимум, що загрожує власникові зараженого пристрою (і це дуже малоймовірний сценарій)- блокування з боку інтернет-провайдеру. А «вилікувати» пристрій найчастіше можна за допомогою простого перезавантаження.

Видобуток криптовалюти

Інший тип корисного навантаження пов'язаний із криптовалютами. Наприклад, IoT-зловреди можуть установлювати майнер на заражений пристрій. Але через невелику обчислювальну потужність «розумних» пристроїв, доцільність такої атаки залишається під сумнівом, навіть незважаючи на їх потенційно велику кількість.

Більше хитрий і діючий спосіб збагатитися на парочку-іншу криптомонеток придумали автори троянця Satori. IoT-пристрій виступає в їхньому сценарії в ролі своєрідного «ключа», що відкриває доступ до високопродуктивного ПК:

На першому етапі зловмисники намагаються заразити якнайбільше роутерів, використовуючи відомі уразливості, а саме:

– CVE-2014-8361 – RCE в miniigd SOAP service в Realtek SDK;

– CVE 2017-17215 – RCE у прошиванні роутерів Huawei HG532;

– CVE-2020-10561, CVE-2020-10562 – обхід авторизації й можливість виконати довільні команди на роутерах Dasan GPON.

– CVE-2020-10088 – переповнення буфера в XiongMai uc-httpd 0.0, що використовується в прошиваннях деяких роутерів і інших «розумних» пристроїв деяких китайських виробників;

Використовуючи скомпрометовані роутери й уразливість CVE-2020-1000049 у механізмі віддаленого адміністрування ПЗ для майнинга криптовалюти Etherium – Claymore, замінити адреса гаманця на свій;

Крадіжка даних

Виявлений у травні 2020 року троянець VPNFilter переслідує інші мети. Головна серед них – перехоплення трафіку зараженого пристрою, добування з нього важливих даних

(логіни, паролі й т.п.) і відправлення їх на сервер зловмисників. От основні особливості VPNFilter:

Модульна архітектура. Автори зловреда можуть «дооснащать» його новими функціями «на лету». Так, на початку червня 2020 р. був виявлений новий модуль, що вмів инжектить javascript-код у перехоплені веб-сторінки;

Стійкість до перезавантажень пристрою. Троянець прописує себе в стандартний для Linux-систем планувальник crontab, а також може змінювати конфігураційні параметри в енергонезалежній пам'яті (NVRAM) пристрою;

Використання TOR для комунікації зі своїм сервером керування;

Можливість самознищення й виводу пристрою з ладу. Одержавши відповідну команду, троянець видаляє себе, а також перезаписує сміттєвими даними критичну частину прошивання після чого перезавантажує пристрій;

Спосіб поширення троянця дотепер залишається невідомим: його код не містить ніяких механізмів самопоширення. Однак ми схильні думати, що для зараження використовуються відомі уразливості в ПЗ пристроїв.

У найпершому звіті про VPNFilter говорилося про 500 тисячі заражених пристроїв. З тих пор їх стало більше, а список виробників уразливих гаджетів значно збільшився. На середину червня він включав наступні бренди:

- ASUS.
- D-Link.
- Huawei.
- Linksys.
- MikroTik.
- Netgear.
- QNAP.
- TP-Link.
- Ubiquiti.
- Upvel.
- ZTE.

Збільшує ситуацію ще й те, що пристрою цих виробників використовуються не тільки в корпоративних мережах, але часто й у якості домашніх роутерів звичайних користувачів.

«Розумних» пристроїв стає усе більше й, по деяких прогнозах, до 2020 року їхня кількість у кілька разів перевищить населення планети. Однак виробники усе ще приділяють недостатньо увагу їхньої безпеки: немає нагадувань про необхідність зміни стандартних паролів при першому настроюванні, немає повідомлень про вихід нових версій прошивань, а сам процес відновлення може бути складний для звичайного користувача. Все це робить IoT-пристрою підходящою метою для зловмисників. Їх простіше заразити ніж персональний комп'ютер і при цьому вони можуть займати далеко не останнє місце в домашній інфраструктурі: одні управляють усім інтернет-трафіком, інші можуть знімати відео, а треті управляють іншими пристроями (наприклад, кліматичною установкою).

Шкідливе ПЗ для «розумних» пристроїв розвивається не тільки кількісно, але і якісно: в арсеналі зловмисників з'являється усе більше експлойтів, використовуваних для самопоширення, а заражені пристрої використовуються для крадіжки персональних даних і майнинга криптовалют, а не тільки для організації DDoS-атак.

От кілька простих рад, які допоможуть мінімізувати ризик зараження «розумних» пристроїв:

– Не відкривайте доступ із зовнішньої мережі до пристрою без гострої потреби;

– Періодичне перезавантаження допоможе позбудеться від уже встановлених зловредів (але в більшості випадків ризик повторного зараження залишається);

– Регулярно перевіряйте наявність нових версій прошивання й обновляйте пристрій;

– Використовуйте складні паролі довжиною не менш 8 символів, що включають у себе букви різного регістра, цифри й спецсимволи;

– Міняйте заводські паролі після першого запуску пристрою, при первісному настроюванні (навіть якщо пристрій про це не просить);

– Закрийте/заблокуйте «зайві» порти, якщо є така можливість. Наприклад, якщо ви не підключаєтеся до роутеру по Telnet (порт tcp:23), варто відключити його, щоб перекрити зловмисникам можливу лазівку.

Розробка структурної схеми

Як було сказано вище більшістю енергетичних устаткувань у центрі обробки даних можна управляти дистанційно й точно також налаштовувати його через віддалені термінали. Ці енергетичні устаткування містять у собі мікроконтролери. Безпека системи, побудованої на базі мікроконтролера – це системний захист убудованого програмного забезпечення й даних, розглянутих як найважливіша ланка загальної функціональності системи. Збиток, що може нанести несанкціонований доступ до паролів і персональної інформації, досить очевидний, але в захисті бідує також і сама програма пристрою. Доступ до фрагментів коду, навіть у вигляді бінарних файлів, залежно від намірів зловмисника може привести до обходу ліцензійних і програмних обмежень, копіюванню ключових алгоритмів і навіть до клонування всього пристрою й створенню репліки. Ця репліка, завдяки відсутності витрат на розробку програмного забезпечення, може бути істотно дешевше оригіналу, що дозволить видалити з ринку первинного розроблювача.

Результатом виконання вимог безпеки завжди є ускладнення розроблювальної системи. Додаткові витрати на апаратні рішення й додатковий час, витрачений на розробку й тестування коду, відбиваються на вартості й складності підтримки кінцевого пристрою.

Особливо чутливими ці витрати стали тепер, у процесі масового впровадження IoT, коли, з одного боку, пристрою на мікроконтролерах повинні ставати усе більше масовими й усе більше дешевими, з іншого боку – робота в мережах IoT, де постійно відбуваються підключення до виділеного сервера або хмарного сервісу, висуває підвищені вимоги до інформаційної безпеки системи. До того ж майстерність атакуючої сторони росте, як і скоординованість дій окремих хакерів і реверс-інженерів. Порию доходи, отримані навіть від одиничних успішних атак, покривають видатки на численні невдалі спроби, а з урахуванням масовості ринку IoT, ці доходи мають тенденцію до росту.

Сімейство STM32G0 стало відповіддю фірми STMicroelectronics на найчастіше суперечливі вимоги до мікроконтролерів для ринку IoT. Вдало об'єднавши невисоку ціну, енергоефективність і розширений арсенал убудованих апаратних інструментів, відповідальних за безпеку, STM32G0 на базі ядра ARM Cortex-M0+ може стати основою системи, що не тільки задовольнить зростаючі запити до продуктивності й економії енергії, але й буде максимально захищеної без надмірних складностей у розробці й супроводі.

Щоб знати свого ворога, розглянемо можливі типи атак, потім поговоримо про загальні способи організації протидії, і наприкінці зосередимося на конкретних методах захисту, пропонованих сімейством STM32G0.

Атаки

При розгляді питань безпеки завжди необхідно пам'ятати про ключову аксіому миру інформаційної безпеки – навіть незважаючи на повноцінний комплекс початих захисних заходів, атака все-таки може увінчатися успіхом.

По-перше, які б міри не вживали для комплексного захисту системи, цілком імовірно, що нова, раніше невідома, пролом у безпеці буде виявлена й використана протягом терміну служби пристрою. Існує ціла екосистема, що поєднує програмістів, хакерів і фахівців з реверс-інжинірингу, де свіжознайдена «Уразливість нульового дня» (англ. «0day»), тобто неусунута помилка або шкідлива програма, проти якої ще не розроблений захисний механізм, служить не тільки предметом гордості, але й прибутковим товаром. Із цього треба простий вивід – у плині всього строку експлуатації приладу необхідно вживати певні зусилля для дослідження нових типів атак і для періодичного відновлення ПЗ.

По-друге, нижче ми розглянемо, наскільки високотехнологічними й дорогими можуть бути деякі техніки доступу до вмісту мікроконтролера. З погляду атакуючого, необхідно максимізувати співвідношення «очікувана вигода»/«витрати на атаку». Очікувана вигода пропорційна цінності добутої інформації, вартість атаки пропорційна ціні використовуваного устаткування й часу, витраченого на злом. З обліком цього можна сказати, що вжиті захисні заходи не роблять злом зовсім неможливим, але збільшують вартість атаки, роблячи злом справою усе менш вигідним. Зрозуміло, при збільшенні цінності інформації, закладеної в мікроконтролер, для зниження співвідношення «вигода»/«витрати» рекомендується розглянути можливість застосування більше складних (і, найчастіше, більше дорогих) методів захисту. І навпаки, якщо цінність умісту мікроконтролера невелике, можливо пропорційне зниження витрат на забезпечення безпеки.

При оцінці сумарної вартості злому необхідно також мати на увазі повторюваність атаки, тобто можливість повторного злому тим же самим набором інструментів, що знову приводить нас до виводу про необхідність періодично піддавати ревізії й модифікувати методи захисту від атак.

Типи атак

Розглянемо можливі види атак на мікроконтролер, починаючи з базових, і аж до професійно спланованих атак із застосуванням спеціалізованого інженерного устаткування. Існують наступні типи атак: атака програмного забезпечення (ПЗ), неінвазивна атака апаратного забезпечення й інвазивна атака апаратного забезпечення; також варто окремо розглянути специфіку атаки IoT-системи.

У таблиці 1 наведений короткий огляд розглянутих атакуючий технік.

Таблиця 1 – Типи атак

Тип атаки	Атака ПЗ	Апаратна неінвазивна	Апаратна інвазивна
Умови	Місцево або віддалено	Потрібен доступ до зібраного пристрою або до друкованої плати	Потрібен доступ до друкованої плати
Методики	Помилки в ПЗ Уразливості інтерфейсів Сканування інтерфейсів Фаззинг	Відлагоджувальний порт Комунікаційні порти Впроваджений код (code injection) Перешкоди по ланцюгах живлення (power glitches) Позаштатне тактирування (clock glitches) Аналіз побічних ефектів (side-channel attack)	Зондування кристала Лазерне різання Травлення Іонне травлення (FIB) Оптична й електронна мікроскопія Інжекція перешкод (fault injection)
Вартість	Від дуже низької до високої, залежно від рівня безпеки, наміченого при розробці убудованого ПЗ	Від середньої до високої. Потрібен обмежений набір щодо нескладного устаткування й персонал, що володіє середньою	Дуже висока. Необхідно дороге спеціалізоване устаткування й персонал, що володіє експертною

		кваліфікацією	кваліфікацією
Мети	Доступ до конфіденційної інформації (код і дані), перехоплення даних, відмова устаткування	Доступ до конфіденційної інформації й визначення алгоритмів роботи пристрою	Реверс-інжиніринг (одержання повного пакета документації для відтворення пристрою)

Атака програмного забезпечення

Використовуються уразливості властиво ПЗ, уразливості протоколів обміну й перехоплення каналів зв'язку. У переважній більшості випадків використовуються саме програмні атаки, тому що вони характеризуються низькою вартістю й високим нанесеним збитком. Набір устаткування для програмної атаки досить дешевий (найчастіше можна обійтися персональним комп'ютером з мінімальною кількістю розповсюджених інтерфейсних пристроїв), а співтовариство хакерів і реверс-інженерів, що практикують програмні зломи, дуже добре злагоджено.

Помилки в ПЗ дозволяють перевести пристрій у позаштатний режим роботи за допомогою таких програмних процедур, як переповнення буфера або ініціація витоків пам'яті. У цьому випадку атакуюча сторона може одержати, залежно від типу помилки, доступ до закритих даних або навіть повний контроль над системою.

Використання **уразливостей інтерфейсів** припускає доскональне знання деталей використання конкретних протоколів на базі конкретної апаратної платформи, що дає можливість робити атаки, засновані на тонкощах реалізації, таких, як робота з буфером, особливості використання програмної купи й стека, деталі функціонування стандартних бібліотек. **Сканування інтерфейсів** припускає запис переданих даних у вигляді, придатному для подальшого аналізу.

Одним зі спеціалізованих видів атаки ПЗ є **фаззинг** (fuzzing), коли на інтерфейси й канали уведення інформації приладу подаються свідомо неправильні, випадкові дані або дані в обсязі, що сильно перевищує штатні обсяги. Зловмисники зацікавлені як у виявленні закономірності зависань і помилкової роботи, здатних прояснити особливості внутрішньої логіки пристрою, так і в ініціації процесу витоку пам'яті, здатного в результаті дати доступ до коду, який захищається.

Неінвазивні методи атак апаратного забезпечення

При неінвазивной атаці захист обходиться за допомогою підключення до виводів мікроконтролера й інших використовуваних у приладі мікросхем.

Доступ до незаблокованого відлагоджувальному порту дозволяє атакуючий уважати дампи Flash-пам'яті, перетворити які в добре вихідний код, що досить читається, мовою високого рівня, наприклад, на Си – тільки справа часу. Крім того, запускаючи процес функціонування приладу, що зламується, під контролем **відлагоджувального порту**, зловмисник одержує доступ не тільки до властиво алгоритму, але й до тонкостей його взаємодії з конкретним оточенням.

Доступ до комунікаційних портів дозволяє застосувати спеціалізовані сканери інтерфейсів або записати процедури обміну інформацією для їхнього подальшого аналізу. Цей вид атаки в цілому схожий на сканування інтерфейсів з розділу програмних атак, але більше дійственен, тому що в атакуючої сторони з'являється доступ до внутрішніх комунікаційних ресурсів аналізованого пристрою – до I2C, SPI, 1-Wire, паралельним шинам зовнішньої пам'яті й іншим.

У випадку, якщо система не захищена від запуску стороннього коду, використовується так званий впроваджений код (code injection) – програма, що запускається на зламується оборудовании, що, і виконуючій функції сканування всіх доступних областей пам'яті для подальшого одержання бінарного прошивання пристрою, або активуюча процедури, здатні змусити пристрій змінити функціонування відповідно до мет атакуючої

сторони – записувати дані, отримані по комунікаційних інтерфейсах, зберігати паролі доступу, передавати інформацію стороннім користувачам.

Перешкоди по ланцюгах живлення (power glitches) і **позаштатне тактировані** (clock glitches) можуть перевести мікроконтролер у некоректний режим роботи, здатний дати атакуючій стороні додаткову інформацію про режими роботи пристрою. **Аналіз побічних ефектів** (side-channel attack) припускає сканування й аналіз додаткових параметрів, що характеризують роботу мікроконтролера, таких, як споживаний струм, температура корпуса, електромагнітна емісія. Ця інформація, сама по собі досить незначна, укупі з іншими добутими даними може дати ключ до розумію внутрішньої структури програми.

Інвазивні методи атак апаратного забезпечення

Інвазивна атака передбачає руйнуючий вплив, що забезпечує зловмисникові прямий фізичний доступ до кристала мікроконтролера.

До найпростішого способу інвазивної атаки варто віднести **зондування кристала**, коли за допомогою пошарового шліфування або **лазерного різання** розкривається корпус мікросхеми й на провідні зв'язки усередині кристала, які можуть служити контактними площадками, установлюються мікрозонди, що з'єднують досліджувану схему із зовнішнім устаткуванням, наприклад, з логічними аналізаторами або аналізаторами протоколів.

За допомогою шліфування, різання, травлення й оптичної або електронної мікроскопії можна встановити пошарову структуру кристала, що при відповідних навичках можна використовувати для одержання не тільки функціональної, але й принципової схеми чипа.

Інжекція перешкод використовується аналогічно перешкодам по ланцюгах живлення й позаштатному тактуванню при неінвазивних апаратних атаках, але тільки на новому, більше тонкому й продуктивному рівні.

Нарешті, **іонне травлення** за допомогою іонної гармати (апарата, принципово схожого на електронний мікроскоп, але потік, що використовує, важких іонів) дозволяє робити на мікрорівні дуже широкий спектр філігранних маніпуляцій, таких, як різання провідників, напилювання нових струмопровідних доріжок і навіть створення на існуючій підложці нових транзисторів. Іонна гармата – дуже тонкий і потужний інструмент, нерідко використовуваний навіть розроблювачами мікросхем для корекції пробних кристалів.

Як неінвазивні, так і інвазивні апаратні атаки вимагають фізичного доступу до зламується устройству, що. Найпоширеніший, очевидний і дешевий метод полягає у використанні незахищеного відлагоджувального порту, але, найчастіше атака апаратного забезпечення виливається в досить нетривіальний, складний і дорогий захід, виконуваний із залученням спеціалізованого устаткування, специфічних матеріалів і висококваліфікованих фахівців.

Методи атак IoT-систем

Ключова особливість IoT-пристрою полягає в тому, що крім мікроконтролера, сенсорів і виконавчих механізмів, воно в обов'язковому порядку містить у своєму составі канал зв'язку з інтернет-сервером, що залежно від завдань, поставлених перед системою, може зберігати й обробляти дані, забезпечувати взаємодія з користувачем і відповідати за інтеграцію й взаємодію всіх пристроїв, підключених до даної мережі. Крім того, інтернет-сервер відповідальний за контроль працездатності й відновлення програмного забезпечення підключених до нього IoT-пристроїв.

З погляду безпеки можна виділити наступні актуальні вектори атак на IoT-пристрій:

широка номенклатура (Ethernet, Wi-Fi, Bluetooth, LoRa і т.д.) і досить велика кількість уразливостей каналів зв'язку. Є виражена тенденція до збільшення кількості пристроїв, підключених через бездротові інтерфейси й різновиди PLC (Power line communication, використання ліній електропередачі для обміну даними), що не вимагають для підключення й атаки фізичного контакту із пристроєм;

тісний взаємозв'язок IoT-пристрою й сервера визначає можливість злому не пристрою, а саме сервера, з наступним доступом до каналу зв'язку й пристрою. Завдання ця, з одного боку, досить складні, тому що серверна частина розподілених IoT-систем часто базуються на

хмарних технологіях (Amazon Web Services, Google Cloud, Microsoft Azure), захист яких з боку провайдеру перебуває на дуже високому рівні. З іншого боку, треба мати на увазі можливість використання власних серверів, не завжди належним чином захищених, поширеність методів злому серверного устаткування й зкоординованість співтовариства хакерів;

IoT-пристрій, що працює, як правило, у мережі собі подібних, повинне коштувати недорого, інакше сумарна вартість рішення може виявитися непід'ємною. З огляду на ефект масштабу, розроблювач у процесі проектування повинен заощаджувати буквально кожний цент, у тому числі зважуючи раціональність застосованих мір, спрямованих на забезпечення безпеки, і іноді мимоволі приймаючи рішення, що тяжіють до економії, а не до безпеки. І отут досить до речі буде згадати про головних героїв нашої статті, мікроконтролерах серії STM32G0. Як буде показано нижче, STMicroelectronics при розробці цієї серії зробило упор саме на економії й безпеці, так що тепер їсти можливість сконструювати максимально захищене, але при цьому бюджетний пристрій;

Автори досліджень, пов'язаних з безпекою IoT (наприклад, «Privacy and the Internet of Things» Гілада Роснера), також відзначають появу таких системних ефектів, як зосередження на серверах величезних обсягів різнохарактерної інформації, несанкціоноване використання якої здатно привести до великого збитку, і змушений допуск до роботи персоналу, що найчастіше не володіє належною кваліфікацією й недостатньо стурбованого інформаційною безпекою.

Методи протидії

Після розбору видів можливих атак ми досить обґрунтовано можемо спрогнозувати й піддати аналізу методи захисту (рисунок 1).

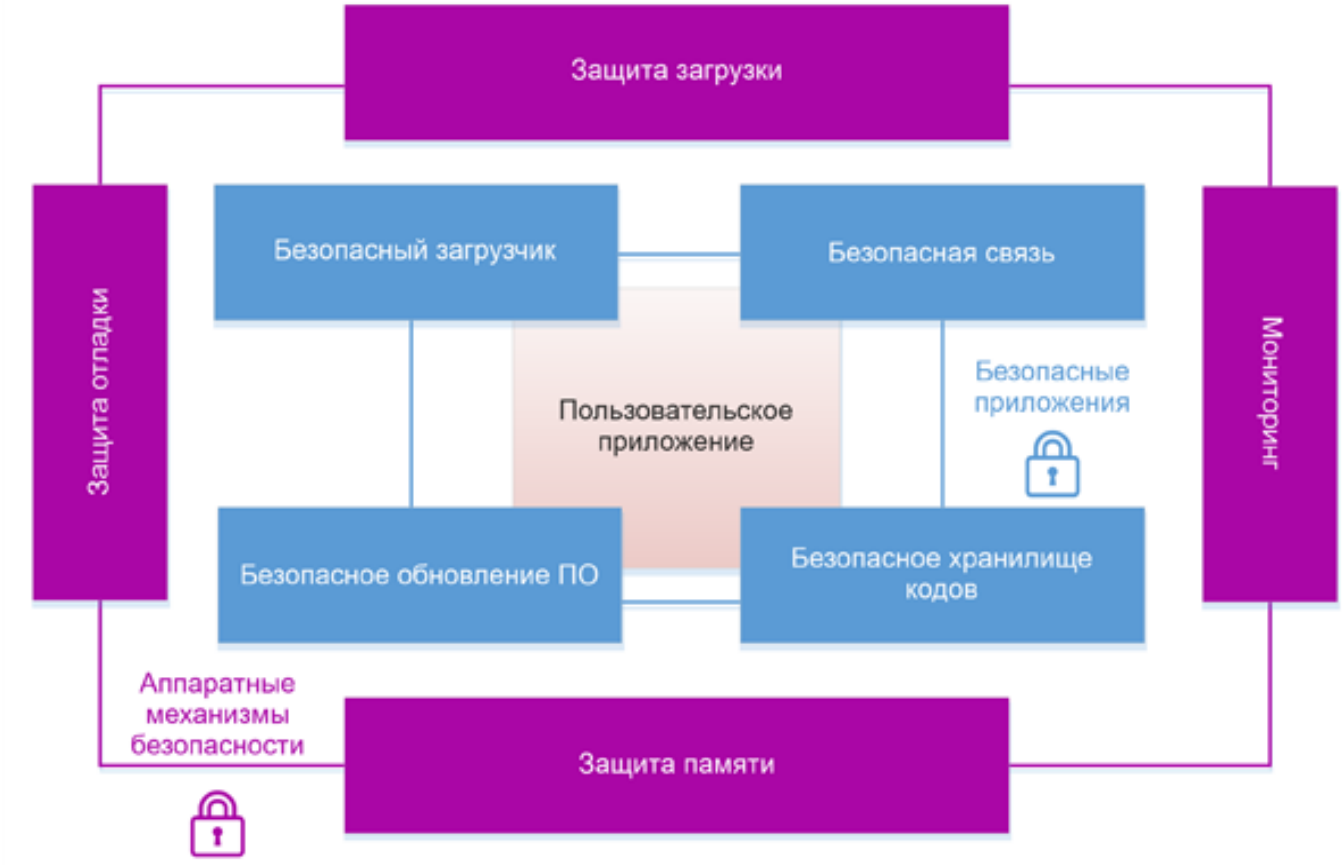


Рисунок 1 – Структурна схема системи

Захист Flash-пам'яті

Без сумніву, найважливіший і найдійовіший метод захисту – блокування доступу до пам'яті пристрою. Утримуюча пропрієтарний код і чутлива дані, Flash-пам'ять мікроконтролера в обов'язковому порядку повинна бути закрита як для зовнішніх інтерфейсів (таких як відлагоджувальні порти), так і від внутрішніх неавторизованих процесів.

У цілому, при плануванні атаки на мікроконтролер саме вміст Flash є метою номер один. Завантажник, основна програма й необхідні для роботи дані в Flash-пам'яті, разом зі схемою приладу, отриманої при аналізі апаратного забезпечення, сукупно здатні скласти повний пакет документації, необхідний для клонування пристрою.

При роботі з лінійкою STM32G0 для комплексного захисту пам'яті від зовнішньої атаки необхідно в першу чергу активувати RDP (тут і далі курсивом виділені конкретні захисні механізми, наявні в арсеналі STM32G0 і детально розібрані в наступній главі). Саме RDP відключає можливість зчитувати Flash-пам'ять через відлагоджувальний інтерфейс JTAG або SWD. Це перший рубіж оборони й свого роду вододіл, що змушує зловмисника переходити від простого копіювання інформації до осмислених атакуючих заходів.

При здійсненні **внутрішньої атаки** на Flash-пам'ять зловмисник намагається запустити сторонній код, інжектований в ОЗП або попередньо впроваджений у сторонню бібліотеку, для того, щоб одержати доступ до основних коду й даним. Метод непростий, але дуже продуктивний, захиститися від зовнішнього коду, що зчитує вміст внутрішньої пам'яті, досить важко, але, на щастя, у серії STM32G0 передбачений цілий арсенал від такого виду атак:**PCROP**, що забороняє доступ на читання, запис і навіть на стирання до певного блоку Flash-пам'яті; **Securable memory area**, що блокує доступ до завантажника після його однократного виконання; **MPU**, що дозволяє гнучко налаштовувати права доступу до Flash-пам'яті, ОЗП і регістрам.

Захист від запису невикористовуваної пам'яті допоможе запобігти інжекції коду або модифікацію основної програми. STMicroelectronics рекомендує не залишати невикористану пам'ять у вихідному стані (virgin value), а заповнювати її яким-небудь передбачуваним паттерном, наприклад, командою NOP, а краще кодом виклику переривання або свідомо некоректними значеннями (illegal op-codes), при спробі виконання яких буде також викликане переривання; у такому випадку мікроконтролер одержить інформацію про те, що в результаті збоїти або навмисного втручання почалося виконання коду з невикористовуваної області пам'яті й потрібно вжити відповідних заходів. Для захисту від запису, крім згаданого вище MPU, варто використовувати спеціалізований інструмент -WRP, за допомогою якого можна заблокувати на запис два незв'язаних блоки Flash-пам'яті різного розміру.

Документація від STMicroelectronics відзначає, що в список захисних заходів варто обов'язково включити активацію механізму ECC, що дозволяє автоматично детектувати і виправляти помилки пам'яті. ECC не є чистим засобом захисту від атак, будучи, відповідно до «AN4750, Handling of soft errors in STM32 applications», у першу чергу методом виявлення випадкових помилок (random failures control techniques), але при цьому входить в обов'язковий чек-лист активуємих захистів.

Захист ОЗП

Стік, масиви даних, буфери комунікаційних інтерфейсів і змінні – все це розташовано в ОЗП і є бажаною метою для хакера.

Досить поширене **виконання коду з ОЗП**, тому що саме ОЗП – найшвидша пам'ять, наявна в розпорядженні мікроконтролера, і найчастіше ділянка коду, при виконанні якого потрібна максимальна швидкість, переносять перед виконанням в ОЗП. Іншою причиною для виконання коду з ОЗП є наявність зовнішньої Flash-пам'яті, що містить зашифрований код, що переноситься в оперативну пам'ять, де згодом розшифровується й виконується. Зрозуміло, у такому випадку потрібно захистити ОЗП (або його частина) від зовнішнього доступу. У цьому нам допоможе MPU, що здатний гнучко настроїти права доступу до пам'яті

або навіть включити режим, у якому виконання коду з оперативної пам'яті повністю заборонене (execute never).

Після виконання деяких ділянок коду ОЗП може містити тимчасові значення секретних змінних. Наприклад, при відправленні або прийомі зашифрованого повідомлення пароль, що перебуває в захищеному секторі Flash-пам'яті, може бути зчитаний в ОЗП. Потрібно в обов'язковому порядку очищати ОЗП відразу після виконання операцій, здатних залишити у вільному доступі секретні дані. Всі тимчасові змінні повинні бути віддалені, буфери комунікаційних протоколів обнулені, стек і купа повинні бути зачищені. На додаток до цього рекомендується використовувати RDP для заборони завантаження з ОЗП й заборони завантаження із зовнішніх джерел (bootload).

Разом з ECC, детектуючим помилки Flash-пам'яті, працює контроль парності ОЗП, що автоматично виявляє помилки в ОЗП. Контроль парності рекомендується до обов'язкової активації, навіть незважаючи на те, що без нього обсяг оперативної пам'яті виростає на 12.5 % (1/8, додається по одному біті на кожний байт).

Ізоляція програмного забезпечення

Ізоляція коду відноситься до високорівневих технік захисту від злому, і припускає спільну скоординовану взаємодію апаратних можливостей, передбачених виготовлювачем мікроконтролера, розроблювачами операційних систем і програмістами, що пишуть прикладний код. Отут треба в черговий раз пом'янути добрим словом інженерів STMicroelectronics, що включили Memory protection unit до складу навіть самих недорогих лінійок STM32G0 Value Line, і тим самим заложивших потужний фундамент безпеки для всього сімейства.

Ізоляція ПЗ базується на можливості відокремлення окремих процесів, які не мають змоги впливати один на одного. Кожний процес має свою дозволену область роботи, власний стік даних, і не може вплинути на інші процеси. Ізоляцією процесів друг від друга управляє операційна система, і ця ізоляція переслідує двояку мету:

– захистити одні процеси від помилок, можливих в інших процесах. Обвалення одного із процесів через переповнення або витоки пам'яті може бути коректно оброблене й не приведе до втрати працездатності всього приладу;

– захистити одні процеси від навмисного шпигунського втручання з боку іншого процесу. Конфіденційні дані, такі, як криптографічний ключ або секретний алгоритм, будуть доступні в рамках тільки одного процесу, що виконується;

Для коректної ізоляції ПЗ разом з MPU рекомендується використовувати Securable memory area, за допомогою якої можна визначити деякі параметри процесів ще на рівні завантажника, що не модифікується.

Відлагоджувальні порти й інтерфейси завантаження

Обов'язкове відключення відлагоджувальних портів, реалізоване за допомогою RDP, уже було згадано в розділі, присвяченому захисті Flash-пам'яті, і є зовсім обов'язковою, першочерговою захисною мірою.

Крім цього, потрібно в обов'язковому порядку відключати невикористовувані можливості по завантаженню ззовні. Наприклад, навіть найпростіший мікроконтролер серії STM32G0, STM32G070, може завантажити зовнішній код з USART1, USART2, USART3, I2C1, I2C2, SPI1, SPI2 (глава «STM32G07xxx/08xxx device bootloader» в «AN2606. STM32 microcontroller system memory boot mode»). Це величезна діра в безпеці, і, якщо завантаження із зовнішнього джерела не передбачена конструкцією приладу, її потрібно обов'язково відключити за допомогою RDP.

Моніторинг стану системи

Програма мікроконтролера повинна постійно відслідковувати показання наявних на борті датчиків, для того, щоб при виході їхніх показань на межі припустимого, вживати заходів по зміні режиму роботи на більше безпечний. Деякі показники стану системи, призначені в першу чергу для захисту від випадкових збоїв, можуть, проте, застосовуватися для детектування атаки, що почалася на пристрій. Наприклад, спадання напруги живлення

нижче припустимої границі або відключення зовнішнього тактового сигналу можуть означати як ненавмисну апаратну проблему, так і хакерську атаку.

Механізм забезпечення безпеки тактування CSS забезпечує безпечне відключення зовнішніх тактових частот HSE і LSE у випадку їхньої відмови або ненормального поводження й перехід на роботу від убудованих генераторів.

Моніторинг напруги живлення за допомогою убудованого АЦП (для мікроконтролерів лінійки Value Line) і програмувальний детектор напруги PVD (для лінійок Access Line і Access Line & Encryption) можуть сигналізувати про вихід напруги живлення за межі норми й про необхідність переходу в безпечний режим.

Вимір температури кристала за допомогою убудованого сенсора дозволить визначити перегрів або занадто сильне охолодження приладу.

Виявлення фізичного доступу **(Tamper detection)** – функція, відповідальна винятково за безпеку. З її допомогою можна визначити розкриття корпуса приладу й ужити заходів для зміни режиму робота або знищення чутливої інформації.

Безпечне завантаження й відновлення ПЗ

Після скидання мікроконтролера завантаження різних компонентів програми відбувається поетапно: на самому початку мікроконтролер налаштовує опції забезпечення безпеки системи (MPU, IWDG і т.д.), потім завантажується користувальницький код, і наприкінці – сторонні бібліотеки. Забезпечення безпеки системи протягом цього покрокового процесу, коли більше довірений елемент перед завантаженням перевіряє безпека менш довіреного, називається «ланцюжком довіри» (chain of trust, рисунок 4) і забезпечується наступними процедурами:

– забезпеченням максимальної захищеності кореневого компонента (root). Якщо кореневий компонент буде скомпрометований, то буде скомпрометований весь ланцюжок безпеки, і всі інш завантажуватися компоненти, що, будуть під загрозою;

– перевіркою контрольних сум установлюваних компонентів (за допомогою MD5 або SHA256);

– максимальним використанням у процесі завантаження криптографічних схем;

Якщо при завантаженні всі операції можна фізично ізолювати усередині корпуса мікроконтролера, то при відновленні ПЗ канал доставки завжди вважається небезпечним. Навіть якщо ви обновляєте програму мікроконтролера через захищений Ethernet або передаючи прошивання за допомогою GSM-Модему, з метою безпеки краще розглядати відновлення, як, скажемо, бінарний файл, переданий користувачеві на пристрої USB Flash, і споконвічно припускати, що зацікавлена в зломі сторона обов'язково одержить доступ до цієї інформації.

Виходячи з таких передумов, видно, що відновлення ПЗ мікроконтролера завжди повинне бути криптографічно захищено, і, отже, мікроконтролер завжди повинен бути здатний автентифікувати, перевірити цілісність і встановити таке криптографічно захищене відновлення.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки силової інфраструктури ЦОД. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем кібербезпеки силової інфраструктури ЦОД. Досліджена система кібербезпеки силової інфраструктури ЦОД. На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки силової інфраструктури ЦОД. Розроблені алгоритми дозволяють успішно вирішувати завдання кібербезпеки силової інфраструктури ЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Даниленко Д.О. Дисперсійний аналіз мережного трафіку для забезпечення інформаційної безпеки телекомунікаційних систем / О.О. Кузнецов, О.А. Смірнов, Д.О. Даниленко // Інформаційна та економічна безпека: сучасний стан та тенденції розвитку : монографія за заг. ред. – Х.: ХІБС УБС НБУ – 2014 – С. 82-100.
2. Даниленко Д.О. Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі / Д.О. Даниленко, О.А. Смірнов, Є.В. Мелешко // Системи озброєння і військова техніка. – Випуск 1(29) – Х.: ХУПС – 2012. – С. 92-100
3. Даниленко Д.А. Метод обнаружения вредоносного программного обеспечения. Часть Корреляционный анализ сетевого трафика // А.А.Смирнов, Д.А. Даниленко, Е.В.Мелешко // Науково-технічний журнал «Інформаційно-керуючі системи на залізничному транспорті» – Випуск 4(95). – Х.: УкрДАЗТ – 2012. – С. 8-14.
4. Даниленко Д.А. Методы обнаружения вредоносного программного обеспечения в телекоммуникационных системах и сетях / Д.А. Даниленко // Збірник наукових праць "Системи обробки інформації". – Випуск 3(101) том 2. – Х.: ХУПС – 2012. – С. 152-155.
5. Даниленко Д.А. Системы обнаружения и предотвращения вторжений для защиты телекоммуникационных сетей от вредоносного программного обеспечения / Д.А. Даниленко, А.А. Смирнов, А.В. Коваленко // Системи управління, навігації та зв'язку. – Випуск 1 (21) том 2. – Київ: ДП «ЦНДІНУ». – 2012. – С. 183-186.
6. Даниленко Д.А. Системы обнаружения и предотвращения вторжений для защиты компьютерных сетей от вредоносного программного обеспечения / Д.А. Даниленко, А.А. Смирнов, И.Г. Кирилов // Збірник тез доповідей науково-практичної конференції «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку». м. Харків. 21-22 березня 2012 р. – Харків. АВВ МВС. – 2012. – С. 70-7
7. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Електронний ресурс]. – Режим доступу до ресурсу: http://www.rfcmd.ru/sphider/docs/InfoSec/GOST-R_ISO_IEC_13335-1- 2006.htm
8. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть Обзор и концепции [Електронний ресурс]. – Режим доступу до ресурсу: http://protect.gost.ru/document.aspx?control=7&id=179072
9. ДСТУ В 3265 – 95. Зв'язок військовий. Терміни та визначення. – К.: УкрНДІССІ, 1995. – 23 с.
10. ДСТУ ISO 9000:2007 Системи управління якістю. Основні положення та словник термінів [Електронний ресурс]. – Режим доступу до ресурсу: http://document.ua/docs/tdoc14237.php

УДК 004

А. Іванов, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ МІЖМАШИННИХ КОМУНІКАЦІЙ З ВИКОРИСТАННЯМ СТАНДАРТУ 10BASE-T1

У статті розроблено програмне забезпечення, яке призначено для системи міжмашинних комунікацій з використанням стандарту 10Base-T1. Метою розробки є дослідження та програмна реалізація системи міжмашинних комунікацій з використанням стандарту 10Base-T1. Об'єктом дослідження є процес міжмашинних комунікацій з використанням стандарту 10Base-T1. Предметом дослідження є методи міжмашинних комунікацій з використанням стандарту 10Base-T1. Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи міжмашинних комунікацій з використанням стандарту 10Base-T1. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, міжмашинні комунікації, 10Base-T1

Постановка проблеми. Поява однопарного Ethernet було в значній мірі пов'язане з інтересами автомобілебудування. Тепер ця технологія здобуває все більше значення для різних застосунків автоматизації, включаючи інтелектуальні будинки й промислове виробництво. 10 Base-T1, новий стандарт однопарного Ethernet, буде підтримувати одночасну передачу даних і напругу живлення.

Традиційний «мідний» Ethernet з неекранованими й екранованими кабелями із крученими парами – UTP, ScTP або Sc/FTP – становить основу локальних обчислювальних мереж. А завдяки технології Power over Ethernet (PoE) з його допомогою можна досить просто забезпечити живленням відеокамери, точки доступу бездротових мереж і інші подібні пристроїв.

Завдяки широкому використанню Ethernet з'явилася можливість створювати на основі єдиного протоколу конвергентні рішення для передачі даних, підключення комплексів безпеки, з'єднання систем автоматизації будинків і виробничих процесів. Удосконалювання технологічних рішень, мікропроцесорів і елементної бази привело до появи комплексів автоматизації нового типу, що, у свою чергу, зажадало модернізації використовуваної кабельної інфраструктури й стало стимулом для подальшого розвитку комунікаційної технології Ethernet.

Так, у сучасних автомобілях широко застосовуються системи мікропроцесорного управління компонентами, а також розважальні комплекси з високо-якісним відео й звуковим супроводом. У новітніх поїздах бортові електронні пристрої й різні варіанти аудіо- і відеорозваг поєднуються в системи, у яких використовуються кілометри кабелів.

Транспортні застосунки вплинули на появу нового різновиду Ethernet з однією крученою парою. Вона відкриває шлях до стандартизації інфраструктури передачі даних для промислових застосунків і відмові від використовуваних раніше протоколів промислових польових шин.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи міжмашинних комунікацій з використанням стандарту 10Base-T1

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи міжмашинних комунікацій з використанням стандарту 10Base-T1.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем міжмашинних комунікацій з використанням стандарту 10Base-T1.

– Дослідження системи міжмашинних комунікацій з використанням стандарту 10Base-T1.

– Програмна реалізація системи міжмашинних комунікацій з використанням стандарту 10Base-T1.

Об'єктом дослідження є процес міжмашинних комунікацій з використанням стандарту 10Base-T1.

Предметом дослідження є методи міжмашинних комунікацій з використанням стандарту 10Base-T1.

Методи дослідження базуються на методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Стандарт 10 Base-T1

В інституті IEEE комітетом 802.3 сформована робоча група 802.3cg Single Pair Ethernet для стандартизації комунікацій на основі однієї кручений пари з дальністю передачі понад 100 м, а при підготовці враховуються вимоги до мережі з боку рішень автоматизації на базі Інтернету речей.

Назва нового стандарту – 10 Base-T1. Розроблювальні специфікації розраховані на передачу даних на невеликі (short-reach) і значні (long-reach) відстані.

10 Base-T1S буде специфікувати тракт передачі даних до 15 м із чотирма з'єднувачами й діапазоном робочих частот від 0,3 до 200 МГц, а 10 Base-T1L – дальність до 1000 м, до 10 з'єднувачів у тракті, частоти від 0,1 до 20 Мгц.

Новий стандарт орієнтований на кабельні системи для комерційного застосування (у тому числі для використання в автомобілебудуванні), а також на комплекси промислової автоматизації, за допомогою яких численні датчики поєднуються з виконавчими пристроями, що передають незначні обсяги даних.

На прикінцеві пристрої, які підключені до однопарної кабельної інфраструктури, електроживлення, як правило, потрібно подавати дистанційно. Для цього розроблювачі мають намір забезпечити відповідність 10 Base-T1 вимогам специфікацій стандарту IEEE 802.3bu (Power over Data Lines, PoDL) – як для з'єднань точка-точка, так і для транкінгових схем подачі живлення (Powered Trunk).

Згодом стандарт IEEE 802.3cg 10 Mb/s Single Twisted-Pair може стати реальною альтернативою найбільш популярним польовим шинам, застосовуваним у різних системах автоматизації.

Стандартизація кабельної інфраструктури

Групи стандартизації кабельних систем Американського національного інституту стандартів (American National Standards Institute, ANSI) і Асоціації телекомунікаційної індустрії (Telecommunications Industry Association, TIA), а також Міжнародної організації по стандартизації (International Organization for Standardization, ISO) і Міжнародної електротехнічної комісії (International Electrotechnical Commission, IEC) приступилися до розробки специфікацій трактів передачі даних різної довжини для комерційних і індустріальних застосунків. Відповідні специфікації містять вимоги до кабелів, рознімань, комунікаційних шнурів і іншим компонентам каналів однопарних комунікацій.

Приміром, в TIA працюють над стандартом TIA-568.5, де визначаються однопарні з'єднання і їхні компоненти зі швидкодією 10 Мбіт/с для кабельних трактів довжиною до 100 м, 100 Мбіт/с – до 15 м, 1 Гбіт/с – до 15 і 40 м. Кабелі повинні підтримувати технологію Power over Data Lines, тобто забезпечувати подачу потужності до 50 Вт по одній кручений парі 24 AWG (American Wire Gauge, американський стандарт калібру проводів).

Розроблювальне доповнення до промислового стандарту TIA-1005 Industrial Cabling регламентує кабельну проводку для передачі даних на відстань до 1 км зі швидкістю 10 Мбіт/с. Щоб знизити втрати, у трактах такої довжини планується застосовувати кручену пару із провідниками калібру 18 AWG.

Подібні розробки здійснюються й в ISO. Так, стандарти ISO 11801-9906 Ed. 1 і 11801-6 Ed.1/Amd.1 будуть містити специфікації однопарної кабельної проводки для комерційних застосунків, у яких потрібне швидкодія 10, 100 і 1000 Мбіт/с. Стандарти ISO I11801-3 Ed.1/Amd.1 будуть присвячені кабельній інфраструктурі для промислових рішень.

Однопарні коннектори

До найважливіших компонентів кабельної інфраструктури ставляться з'єднувачі. За попередніми оцінками експертів, фронтальна площа з'єднувачів для однопарного Ethernet могла б становити від половини до третини відповідної площі рознімань RJ45. Вони розробляються розраховуючи на проведення калібру 18-26 AWG, повинні бути здатні підтримувати струм до 1 А и можуть випускатися в екранованих і неекранованих модифікаціях. Провідні виробники комутаційних продуктів уже підготували свої рішення.

Пропозиція компанії CommScope засновано на розніманнях LC і враховує вимоги стандарту IEC 63171-1. У цих розніманнях оптичні компоненти замінені металевими контактами. Як за вляє розроблювач, такі екрановані й неекрановані компактні коннектори прості в установці, що дуже важливо при монтажі в польових умовах і у важкодоступних місцях.

З'єднувачі інсталюються без застосування складних інструментів, а їхні контактні поверхні не уступають по надійності компонентам рознімань RJ45. Вони цілком здатні замінити використовувані сьогодні однопарні рішення, не пов'язані з технологією Ethernet,

уважають в CommScope. Коннектори, запропоновані CommScope, призначені для застосування в комерційних офісних додатках (Mechanical, Ingress, Climatic, Electromagnetic, MICE1).

На роботу в промислових умовах, включаючи найбільш складне навколишнє середовище (MICE2/MICE3), розраховані рознімання, запропоновані компанією Harting. Вони відповідають вимогам стандарту IEC 61076–3–125 і специфікаціям IP65/67 по запалювано– і вологозахищеності. Їхніми компонентами можуть служити в тому числі добре відомі в промислових додатках рознімання M8 і M12.

Екрановані модифікації коннекторів Harting забезпечують роботу на частотах до 600 Мгц. У запропонованих розніманнях передбачена підтримка технології Power over Data Lines і передача напруги живлення на відстань до 1 км.

Всеосяжний Ethernet

Отже, 10 Base-T1, нова технологія Ethernet, буде підтримувати однопарні комунікації й можливість одночасної передачі даних і напруги живлення (Power over Data Lines) по збалансованій кручений парі.

Поява однопарного Ethernet у значній мірі пов'язане з інтересами автомобілебудування. Однак у цей час ця технологія стає усе більше значимої для різних застосунків автоматизації, включаючи інтелектуальні будинки й промислове виробництво.

Очікувані комунікації 10 Base-T1 відкривають нові можливості для цифровізації систем автоматизації нижнього рівня. З їхньою появою взаємодія з датчиками й виконавчими пристроями в комплексах промислової автоматизації й інтелектуальних будинків може здійснюватися за допомогою цифрових, а не аналогових сигналів.

Спрощення кабельної інфраструктури, зменшення обсягів кабельної продукції й скорочення строків монтажу особливо важливі в рішеннях на основі технологій Інтернету речей, прикінцевих пристроїв у якому набагато більше, ніж у сучасних системах автоматизації.

Ethernet, таким чином, стає всеосяжною комунікаційною технологією, що охоплює все компоненти сучасних об'єктів нерухомості – від систем управління будинком (Building Management System, BMS) до розміщених у них центрів обробки даних. Крім того, вона уніфікує передачу даних для комплексів промислової автоматизації – від датчиків до IT-Інфраструктури, що підтримує ERP-Додатка. Завершення розробки стандартів 10 Base-T1 наближає появу й впровадження таких рішень.

Розробка структурної схеми

Темпи росту ринку автоматизації будинків перевищують темпи росту ринку будівництва будинків, оскільки, крім оснащення системами управління будинків-новобудов, при реконструкції й ремонті відбувається активне устаткування системами автоматизації більшої частини фонду будинків, що експлуатуються.

Рівень розвитку продуктів і систем автоматизації будинків є ключовим чинником, що забезпечує ефективне, безпечне, зручне й екологічно чисте функціонування будинків. Крім того, він впливає на всі елементи технічного оснащення будинку, особливо відносно систем опалення, вентиляції й кондиціювання повітря.

До продуктів автоматизації будинків ставляться спеціальні апаратні й програмні засоби й послуги з розробки й впровадження систем автоматизації й управління будинками.

Апаратні засоби включають датчики; виконавчі механізми й пристрої (керовані клапани, регулятори й т.д.); керуючі контролери, що здійснюють функції місцевого управління; комунікаційні контролери (маршрутизатори, шлюзи й т.п.), кабелі й кабельна арматури, призначені для побудови мереж необхідної топології, сумісності й продуктивності; а також комп'ютери для створення систем моніторингу й диспетчеризації систем управління будинку.

До програмних засобів ставиться:

– убудоване програмне забезпечення (ПЗ), що поставляється звичайно виготовлювачам устаткування й тому заставляється в ціну інтелектуальних апаратних засобів;

– ПЗ систем мережного зв'язку (для конфігурування, налаштування й тестування мереж);

– ПЗ для систем збору даних і диспетчерського управління (SCADA);

– спеціалізоване ПЗ для реалізації замовлених алгоритмів управління систем будинку.

Третю частину ринку становлять послуги з розробки й впровадження: проектування систем; розробка й прокладка кабельної системи будинку; послуги інжинірингу (реалізація алгоритмів управління системами, розробка зв'язку між підсистемами, розробка спеціалізованих апаратних засобів, написання замовленого ПЗ); монтаж устаткування; пусконалагоджувальні роботи, конфігурування, налаштування й тестування мережі й всієї системи управління.

Термін «інтелектуальний будинок» (intelligent building – англ.; intelligent – ‘розумний, тямущий’, у сполученні зі словом building – ‘гнучкий, що пристосовується’) у первісному змісті означає ‘будинок, готове до змін’ або ‘пристосовується здание, що,’, тобто будинок, здатне пристосовуватися до змін навколишнього середовища. Інакше кажучи, цей будинок, інженерні системи якого здатні забезпечити адаптацію до можливих змін у майбутньому.

Традиційні рішення інженерного устаткування будинки являють собою сукупність окремих, не взаємодіючих між собою систем. Будинок, у якому ці системи об'єднані в інтегрований комплекс і правильно організовані вже на етапі проектування (з обліком можливих майбутніх змін), має право називатися інтелектуальним.

У порівнянні з автономними системами комплексна система має наступні переваги:

– істотна економія на кабельних мережах і мережному устаткуванні;

– зниження енергоспоживання й підвищення надійності всієї системи;

– підвищення оперативності управління об'єктом;

– графічне подання інформації про стан систем і устаткування на різних рівнях (об'єктовому, зональному, адресному);

– зниження працезатрат експлуатаційних і диспетчерських служб;

– забезпечення необхідної взаємодії систем;

– зниження ймовірності виникнення страхових випадків;

– «відкритість» комплексу, що забезпечує можливість його нарощування й використання устаткування різних виробників.

Поняття «інтелектуальний будинок» ще не має точного тлумачення, але більшість людей, які ним користуються, сприймають його як автоматизовану технічну систему, що:

– «почуває», що відбувається усередині будинку й зовні;

– «реагує» таким чином, щоб найбільш ефективним способом забезпечити безпечне й комфортабельне перебування в ньому, звівши до мінімуму споживання енергії й енергоресурсів;

– «взаємодіє» з людьми за допомогою застосування простих і легко доступних засобів спілкування.

Інтелектуальний будинок є продуктом сучасного розвитку існуючих систем автоматики в будинках у напрямку:

– комплексної оптимізації використання ресурсів;

– підвищення гнучкості конфігурування й зниження загальної вартості володіння;

– інтеграції із широким спектром технологічного й телекомунікаційного устаткування;

– спрощення взаємодії з користувачем.

Характерні риси інтелектуальних будинків

До основних особливостей інтелектуальних будинків можна віднести:

– здатність оптимально реагувати на зміни в процесах, що відбуваються в будинку;

– сполучення децентралізованих (розподілених) принципів побудови систем із централізацією функції моніторингу;

– структурований підхід до побудови інженерних систем будинку;

– можливість внесення змін з мінімальними витратами;

– надання певного набору послуг мешканцям будинку.

Інтелектуальний будинок створюється для людини, тому основним критерієм ефективності проекту інтелектуального будинку є якість його взаємодії з мешканцями.

«Інтелект» житлового середовища сучасного будинку забезпечується взаємозалежною роботою автоматизованих будинкових і квартирних систем. Всі системи з'єднані високотехнологічними керуючими й інформаційною мережами, які прокладені у всіх житлових і суспільних приміщеннях будинку.

Основні системи інтелектуальних будинків

При інтеграції в структуру інтелектуальні будинки стають учасниками єдиної системи, тому особливе значення надається можливості гнучкої взаємодії з іншими підсистемами:

1. Комплекс систем життєзабезпечення. До складу входять:

– система управління вентиляцією й кондиціюванням повітря;

– система управління тепло- і водопостачанням;

– система управління електропостачанням;

– система управління освітленням;

– система управління поновлюваними джерелами енергії.

2. Комплекс систем безпеки. Забезпечують моніторинг стану інтелектуального будинку, запобігання й ліквідацію аварійних і небезпечних ситуацій, частково є надбудовою над технологічними підсистемами й можуть використовувати ті самі датчики, інтерфейси й виконавчі механізми, якщо це не заважає їхній роботі. До складу входять:

– контроль і управління електричними споживачами;

– контроль і управління внутрішнім кліматом;

– контроль протікань води;

– система пожежної безпеки;

– система охоронної сигналізація;

– контроль стану зовнішнього середовища;

– контроль і управління доступом до ресурсів будинку;

– контроль за дітьми;

– контроль і обслуговування свійських тварина.

3. Комплекс систем інформатизації. Є базисом, на якому будуються все компоненти інформаційно-обчислювальних мереж інтелектуального будинку. Правильна організація системи визначає надійність функціонування системи інтелектуального будинку як інтегрованого комплексу:

– мережа (ЛОМ);

– система телефонної мережі;

– система прийому ефірного й супутникового телебачення;

– телекомунікаційна підсистема;

– система радіофікації;

– засоби оперативного радіозв'язку персоналу й інші системи.

Рисунок 1 – Структурна схема системи

Управління інтелектуальним будинком виконується по сценаріях. Сценарії розділяються на дві основні групи:

– технологічні, які визначають роботу інженерних систем з метою створення безпечних (з погляду техніки, санітарних норм, екології) умов проживання;

– користувальницькі, які визначають комфортні умови проживання, максимально адаптовані до індивідуальних характеристик.

Визначення вимог до інтелектуальних будинків

Визначення вимог до інтелектуальних будинків простіше встановити виходячи із сукупності процесів життєдіяльності будинку, розглядаючи функціонування інтелектуальних будинків нерозривно від взаємодії з людиною. Абстрагуючись, інтелектуальні будинки можна представити як набір сервісів і способів їхньої реалізації. Ступінь автоматизації залежить від бажання людини перекласти на системи інтелектуальних будинків ту частину процесів, що повинна виконуватися автоматично, напівавтоматично або якимось зручним способом. Тому не може існувати єдиного рецепта по автоматизації будинку.

Проблення вихідних вимог до інтелектуальних будинків повинна відбуватися в тісній взаємодії з тими, хто буде брати участь в експлуатації будинку, забезпечувати реалізацію сервісів і слуг, і тими, хто буде ними користуватися, або їхніми представниками. Нерідко в практиці будівництва сучасних будинків на комерційній основі немає можливості

здійснити пророблення вимог з тими, хто буде експлуатувати будинок і користуватися його сервісами. У такому випадку організація пророблення вимог лягає на ті, хто їх представляє – комерційного забудовника або ріелтора. Їхнім завданням стає визначення співвідношення вартості пропонованого комерційного об'єкта до состава систем і сервісів, видам і рівню послуг проектованого об'єкта.

Успіх комерційного проекту визначається правильно обраним співвідношенням споживчих якостей і вартості. У цьому випадку під якістю розуміється вся сукупність параметрів об'єкта. І серед них немаловажним стає інтелектуальність будинку. Визначення системи якісних показників інтелектуального будинку, пропонованих споживачеві, стає однієї з основних завдань при дослідженні ринку перед початком реалізації комерційного будівництва.

У розробці системи показників якості інтелектуального будинку зацікавлені всі учасники ринку. Організацію даної роботи можна виконати силами фахівців у цій області разом з комерційними забудовниками й ріелторами. Рішення даної проблеми дозволить припинити спекуляції на тему ступеня інтелектуальності будинків і допоможе формуванню цивілізованого ринку в будівництві.

Принципи побудови інтелектуального будинку

До основних технічних принципів побудови інтелектуального будинку ставляться:

– Стандартизація архітектури комплексу систем (відкритість систем). Під відкритістю розуміється наявність єдиного протоколу взаємодії устаткування різних виробників. В основі побудови інтелектуального будинку саме й лежать принципи «відкритої архітектури». При оснащенні будинку системами й устаткуванням від різних виробників важливо, щоб технічні пристрої не конфліктували між собою, а були б сумісні й представляли єдине ціле. Для того щоб системи розуміли один одного, вони повинні використовувати ті самі правила – стандарти – при обміні даними. В області телекомунікацій такі правила називають протоколами.

У цей час широке поширення в області систем управління будинками одержали стандарти 10 Base-T1,BACnet, LonWorks, EIB і ін.

Стандарт 10 Base-T1 був описаний вище. Саме він використовується в даному проекті.

Розглянемо інші стандарти, які можуть застосовуватися в області систем управління будинками.

Стандарт BACnet (Building Automation Control Network – мережний протокол для автоматизації будинків) був розроблений Американським суспільством інженерів по опаленню, охолодженню й кондиціюванню повітря (ASHRAE).

Стандарт EIB (European Installation Bus – європейська інсталяційна шина) призначений для управління енергоспоживанням, освітленням, жалюзі, мікрокліматом і для контролю доступу; визначає вимоги до:

– каналів зв'язку (провідні, інфрачервоної, телефонні, радіо, мережі 220 В 50 Гц, оптоволокно, локальні комп'ютерні мережі Ethernet);

– формату інформації, що курсує;

– принципам взаємодії з користувачем (спеціалізовані інформаційні панелі й програмне забезпечення для персонального комп'ютера).

Технологія EIB дозволяє організувати передачу повідомлень від пристроїв фіксації подій до виконавчих механізмів по наступних інтерфейсах:

– провідні канали зв'язку;

– зв'язок по силовим електричним проводам;

– телефонні й радіоканали;

– інфрачервоне випромінювання;

– інтерфейси комп'ютерних мереж.

У європейських країнах все більше поширення в якості основного мережного стандарту одержує LonWorks, розроблений у компанії Echelon Corporation. Спочатку цей

стандарт був розроблений для HVAC (систем опалення, вентиляції й кондиціювання повітря), однак у цей час він уже використовується при побудові комплексних систем (включаючи системи безпеки, обліку енергоносіїв, освітлення й ін.). З метою пропаганди й поширення стандарту LonWorks у травні 1994 року була створена асоціація LonMark, що поєднує виробників і інсталяторів Lon-Продуктів. Мережа управління LonWorks підтримує різні середовища для передачі інформації: кабель «кручена пари», коаксіальний кабель, волоконно-оптичний кабель, радіоканал і ін. Стандарт LonWorks дозволяє будувати системи управління будинками по вільній топології, що щонайкраще відповідає структурі комплексних систем інтелектуального будинку:

– типізація устаткування й процесів;
– єдине фізичне середовище передачі інформації;
– централізація (функцій моніторингу й управління) і інтеграція систем;
– децентралізація (розподілені системи управління);
– сегментація (модульний принцип побудови систем);
– адаптація (готовність до змін);
– наращуємість і надмірність (наявність резерву).

Реалізація проекту інтелектуального будинку істотно відрізняється від традиційної схеми побудови будинку.

При проектуванні інтелектуального будинку визначальним принципом є формування єдиного підходу при побудові всіх систем різних комплексів.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів міжмашинних комунікацій з використанням стандарту 10Base-T1. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем міжмашинних комунікацій з використанням стандарту 10Base-T1. Досліджена система міжмашинних комунікацій з використанням стандарту 10Base-T1. На основі отриманих результатів досліджень створена програмна реалізація системи міжмашинних комунікацій з використанням стандарту 10Base-T1. Розроблені алгоритми дозволяють успішно вирішувати завдання міжмашинних комунікацій з використанням стандарту 10Base-T1. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Аде Ф.Г. Искусственный интеллект / Ф.Г. Аде., В.Н. Бондарев. – Севастополь: Изд-во СевНТУ, 2002. – 615 с.
2. Алексєєва Т. В. Технічна діагностика гідравлічних приводів / В.Д. Бабанська, Т.М. Башта та ін. – М.: Машинобудування, 1989. – 263 с.
3. Андрощук О.С. Методологічні аспекти побудови інтелектуальних систем підтримки прийняття рішень в особливих ситуаціях / О.С. Андрощук, В.В. Огурцов, О.І. Демідова // Восточно-Европейский журнал передовых технологий. – Х.: Технологический цент, 2009. – 5/2 (41). – С. 18-21.
4. Ашеров А. Т. Эргономика информационных технологий: учеб. издание / А.Т. Ашеров, С.А. Капленко, В.В. Чубук. – Х.: ХГЭУ, 2000. – 224 с.
5. Байлов В. В. Эксплуатация и сервис радиоэлектронных систем: учеб. Пособие / В.В. Байлов, В.С. Плаксиенко. – Таганрог: Изд-во ТРТУ, 2002. – 90 с.
6. Барзилович Е.Ю. Модели технического обслуживания сложных систем: учеб. пособие / Барзилович Е.Ю. – М.: Высш. школа, 1982. – 231 с.
7. Бартіш М.Я. Дослідження операцій. Лінійні моделі: підручник / М.Я. Бартіш, І.М. Дудзяни. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2007. – Ч.1., 168с.
8. Бейхельт Ф. Надежность и техническое обслуживание. Математический подход / Ф. Бейхельт, П. Франкен. Пер. с нем. – М.: Радио и связь, 1988. – 392 с.
9. Беневоленский С.Б. Алгоритм идентификации процессов деградации физических свойств технических объектов / С.Б Беневоленский, А.А. Лисов // Измерительная техника. – М: Стандартинформ, 2005. – № 2. – С. 16-18.
10. Бет Э.В. Метод семантических таблиц / Э.В. Бет; перев. под ред. А.В. Идельсона и Г.Е. Минца // Математическая теория логического вывода. – М.: Наука, 1967. – С. 191-199.

11. Бланк И. А. Инвестиционный менеджмент / И.А. Бланк. – К.: Ника – Центр, 2006. – 448 с.

УДК 004

І. Заікін, магістр гр. КН-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КОМПЛЕКСНОГО ВІДЕОНАГЛЯДУ БАНКІВСЬКОЇ УСТАНОВИ

У статті розроблено програмне забезпечення, яке призначено для системи комплексного відеонагляду банківської установи. Метою розробки є дослідження та програмна реалізація системи комплексного відеонагляду банківської установи. Об’єктом дослідження є процес комплексного відеонагляду банківської установи. Предметом дослідження є методи комплексного відеонагляду банківської установи. Методи дослідження базуються на методах технічного захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи комплексного відеонагляду банківської установи. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерні науки, захисту доступу, обробка графічних даних

Постановка проблеми. Фінансову систему неможливо представити без банківських установ. Коло задач, які вирішують банки постійно збільшується: починаючи від обігу фінансових потоків, закінчуючи різними видами кредитування. В усі часи проблемам забезпечення безпеки банківських установ надавали велике значення. При цьому при побудові сучасної комплексної системи безпеки банку приходиться враховувати велику кількість чинників, починаючи від законодавчих питань охорони банку, інформаційної безпеки конфіденційних даних, які передаються по каналам зв’язку банківських мереж, і закінчуючи фізичним захистом банківських установ [1-5]. В даному випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти увагу сконцентруємо на останньому чиннику. Розглянемо такий аспект фізичних засобів, як технічне забезпечення системи охорони. Система комплексного відеонагляду банківської установи повинна вирішувати наступні задачі:

– побудову комплексної системи безпеки банку;
– одержання повної картини ситуації на об'єкті;
– забезпечення безпеки банкоматів;
– реєстрацію й контроль доступу співробітників і відвідувачів;
– контроль транспортних засобів на території банку.

Усі ці задачі можуть вирішуватися за рахунок широкого застосування сучасних досягнень мікроконтролерної техніки, охоронного телебачення, захищеної передачі даних які отримані з вищеперерахованих пристроїв [1-7].

Таким чином сучасна технічна система комплексного відеонагляду банківської установи представляє собою програмно-аппаратний комплекс, в якому застосовані усі останні напрацювання в області пристроїв забезпечення захисту банківської установи та інформаційно-програмного забезпечення даних які отримуються з цих пристроїв, їх передачі, зберігання та обробки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи комплексного відеонагляду банківської установи

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи комплексного відеонагляду банківської установи.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завданнь:

Огляд існуючих систем комплексного відеонагляду банківської установи.

Дослідження системи комплексного відеонагляду банківської установи.

Програмна реалізація системи комплексного відеонагляду банківської установи.

Об’єктом дослідження є процес комплексного відеонагляду банківської установи.

Предметом дослідження є методи комплексного відеонагляду банківської установи.

Методи дослідження базуються на методах технічного захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Головною метою системи безпеки є забезпечення стійкого функціонування банку й запобігання погроз його безпеки, захист законних інтересів кредитної організації від протиправних зазіхань, охорона життя й здоров'я персоналу, недопущення розкраданя фінансових і матеріально-технічних засобів, знищення майна й цінностей, розголошення, втрати, витоку, перекручування й знищення службової інформації, порушення роботи технічних засобів, забезпечення виробничої діяльності, включаючи й засобу інформатизації.

Завданнями системи безпеки є:

прогнозування й своєчасне виявлення й усунення погроз безпеки персоналу й ресурсам банку;

причин і умов, що сприяють нанесенню фінансового, матеріального й морального збитку, порушенню його нормального функціонування й розвитку;

віднесення інформації до категорії обмеженого доступу (державній, службовій, банківській і комерційній таємницям, іншої конфіденційної інформації, що підлягає захисту від неправомірного використання), а інших ресурсів - до різних рівнів уразливості (небезпеки) і підметів збереженню;

створення механізму й умов оперативного реагування на погрози безпеки й прояв негативних тенденцій у функціонуванні банку;

ефективне припинення погроз персоналу й зазіхань на ресурси на основі правових, організаційних і інженерно-технічних мір і засобів забезпечення безпеки;

створення умов для максимально можливого відшкодування й локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб, ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічних цілей банку.

Технічне забезпечення безпеки базується:

- на системі стандартизації й уніфікації;
- на системі ліцензування діяльності;
- на системах сертифікації засобів захисту;
- на системі сертифікації ТЗ і ПЗ об'єктів інформатизації;
- на системі атестації захищених об'єктів інформатизацією.

Основними складовими забезпечення безпеки ресурсів системи комплексного відеонагляду банківської установи є:

- система фізичного захисту (безпеки) матеріальних об'єктів і фінансових ресурсів;
- система безпеки інформаційних ресурсів.

Система фізичного захисту (безпеки) матеріальних об'єктів і фінансових ресурсів передбачає:

- систему інженерно-технічних і організаційних мір охорони;
- систему регулювання доступу;
- систему мір (режиму) схоронності й контроль імовірних каналів витоку інформації;
- систему мер повернення матеріальних цінностей (або компенсації).

Система охоронних мір передбачає:

- багаторубіжність побудови охорони (території, будинку, приміщення) по наростаючій до найціннішої конкретності, що оберігається;
- комплексне застосування сучасних технічних засобів охорони, виявлення, спостереження, збору й обробки інформації, що забезпечують достовірне відображення й об'єктивне документування подій;
- надійний інженерно-технічний захист імовірних шляхів несанкціонованого вторгнення в охоронювані межі;
- стійку (дубльовану) систему зв'язку й керування всіх взаємодіючих в охороні структур;
- високу підготовку й готовність основних і резервних сил охорони до оперативної протидії порушника;
- самоохорону персоналу.

Опис реалізації системи комплексного відеонагляду банківської установи

Для невеликого відділення банку досить не більше чотирьох - п'яти камер. Використовуючи монітор з вбудованим комутатором і вдало розташувавши камери, забезпечимо цілодобове спостереження за охоронюваною територією. Камери можуть розташовуватися усередині приміщення на поворотних пристроях. При цьому в денний час вони можуть використовуватися для контролю в банківському залі, а ввечері й уночі для контролю охоронюваної території. Кількість одночасно відображуваних камер повинне бути обмежено. При збільшенні кількості моніторів операторові важко стежити за всіма змінами. У багатокамерних системах використовуються додаткові пристрої. До додаткових пристроїв відносяться детектори руху, які аналізують зміни зображення, наприклад, переміщення будь-якого предмета в поле зору камери й сигналізують операторові про це.

Для дистанційного керування камерами використовуються поворотні пристрої. Вони дозволяють збільшити огляд камери за допомогою її повороту у двох площинах. Керування поворотними пристроями здійснюється джойстиком.

Для одночасного одержання декількох зображень (до 16) на екрані одного монітора використовуються квадратори («дільники екрана»). Квадратори перетворять сигнали від декількох відеокамер у зображення, що відображається на одному моніторі. При цьому зображення від будь-якої камери можна оперативно розгорнути на весь екран.

Для послідовного виводу на екран зображення від декількох камер у системах спостереження використовуються мультиплексори (комутатори). У режимі перегляду вони послідовно підключають камери до монітора.

Для оперативної роботи оператор має можливість вивести на екран будь-яке зображення або виключити будь-яку камеру. Періодичність перемикання й час спостереження зображення задається для всіх камер одночасово. На великих об'єктах число камер може становити кілька десятків. Для підвищення ефективності роботи оператора використовують матричні комутатори. Вони дозволяють створити гнучку й нарощувану систему безпеки, у яку можуть входити не тільки компоненти телевізійних систем, але й системи сигналізації й контролю доступу.

Запис відеозображення може здійснюватися на спеціалізовані відеомагнітофони в традиційних системах або в цифровій формі за допомогою комп'ютера. Сучасні тенденції науково-технічного прогресу привели до того, що в основному використовуються цифрові носії, тобто дані по захищеному Ір-каналу передаються в базу даних, де зберігаються, і звідки дістаються якщо буде потреба. Всі пристрої поєднуються в систему, що забезпечує можливість оперативного спостереження. Керування системами спостереження залежно від їхньої складності й обстановки на об'єкті може бути автоматичним або ручним.

Комп'ютерні системи спостереження володіють рядом особливостей, які в різних ситуаціях можуть грати як позитивну, так і негативну роль. Перерозподіл функцій між програмними й апаратними засобами приводить до того, що комп'ютерні системи не завжди можуть забезпечити швидке перемикання режимів. Крім того, підвищуються вимоги до оператора - уміння працювати з комп'ютером і графічним інтерфейсом.

Опис елементів системи безпеки банку

Телевізійна камера.

Якість зображення визначається, насамперед, телевізійною камерою. Вона являє собою закінчений пристрій, що будучи підключеним до відеовходу монітора або телевізора дозволяє спостерігати зображення на екрані на значній відстані від об'єкта зйомки. У цей час випускаються відеокамери для систем телевізійного спостереження (включаючи модифікації), що відрізняються:

- характером зображення (чорно-біле або кольорове);
- чіткістю зображення;
- світлочутливістю (мінімальною робочою освітленістю об'єкта зйомки);
- можливістю цифрової обробки відеосигналу;
- припустимими кліматичними умовами роботи;
- напругою живлення.

З метою забезпечення якісної роботи в умовах змінної яскравості зображення й різних рівнів фонових засвіток сучасні телекамери, для систем телевізійного спостереження, оснащуються підсистемами компенсації цих впливів. З метою збільшення сектора огляду, телевізійні камери встановлюють на поворотні пристрої з горизонтальним або з горизонтальним і вертикальним скануванням. При повороті камери варто враховувати можливі реакції систем компенсації зовнішніх впливів (засвітка, вплив імпульсних джерел штучного висвітлення й т.д.). При установці на вулиці, телекамери містяться в спеціальні захисні корпуси.

Відеомонітор

Другим важливим елементом систем відеоспостереження є відеомонітор. Він повинен забезпечувати високу довгострокову стабільність і не вимагати регулярного калібрування. Надійність також залежить від того, на скільки оптимальні схемні рішення, міцна й зручна механічна конструкція. Технологія виробництва віщальних відеомоніторів за останні роки перетерпіла істотні зміни. У складі апаратури обробки відеоінформації звичайно використовуються два основних типи пристроїв: світчери й компресори. На додаток до основних пристроїв обробки широко застосовуються різні допоміжні пристрої:

- кабельні підсилювачі - для компенсації втрат у кабелі при передачі відеосигналу на відстань до 2 км;
- розгалужувачи, що дозволяють до одному тілі камері підключати кілька моніторів, відеомагнітофонів і т.п.;
- генератори допоміжної текстової інформації (дати, часу й т.п.).

Функціональні системи відеокамер

Основу будь-якої системи телевізійного спостереження становлять телекамери. У конструкції відеокамери можна виділити наступні основні функціональні системи:

- перетворювач світло-сигнал;
- синхронізації;
- автоматичного регулювання посилення;
- електронний затвор;
- автоматичної установки балансу чорного;
- гамма-корекції;
- зйомки при низьких рівнях освітленості;
- об'єктив з автоматичною діафрагмою.

Функція зйомки при низьких рівнях освітленості (LOLUX) чудова тим, що дозволяє знімати майже без висвітлення. При цьому можна одержати прекрасне зображення з гарним колірним балансом без збільшення рівня шуму.

Перетворювачі «світло-сигнал»

Найважливішим елементом конструкції відеокамери є перетворювач «світло-сигнал», що забезпечує кодування зображення, що знімається, у формі електричних сигналів. Перетворювачі світло-сигнал являють собою або передавальної електронно-променеві ТБ

трубки (ЕПТ), або твердотільні матриці - так звані «прилади із зарядовим зв'язком» (ПЗЗ). У сучасних відеокамерах, як правило, застосовуються матриці ПЗЗ, що забезпечують більшу надійність роботи при досить високих параметрах. Число рядків матриці приймає значення від 380 до 900.

Для камер на ПЗЗ, на відміну від трубкових аналогів, характерно також відсутність післязображень (інерційності мішені), продовжень, що тягнуться за об'єктами, які рухаються, у зображенні, не говорячи вже про пропалювання фотопровідного шару мішені. Причому зазначені параметри не залежать від строку експлуатації матриць ПЗЗ. У відеокамерах застосовуються 2/3", 1/2", 1/3", 1/4" і 1/6" прилади із зарядовим зв'язком (ПЗЗ). Число пікселів (піксель - один елемент ПЗЗ) у ПЗЗ може бути від 300 до 1000. Кількість елементів матриці забезпечує горизонтальний дозвіл зображення залежно від моделі 300-600 телевізійних ліній (твл). Успіх мініатюрних відеокамер обумовлений високою надійністю і якістю перетворювачів на приладах із зарядовим зв'язком (ПЗЗ)

Пристрій синхронізації

Пристрій синхронізації забезпечує часове узгодження роботи всіх систем і блоків камери. Синхронізація відеокамер може здійснюватися від внутрішнього або зовнішнього генератора. Зовнішня синхронізація використовується в багатокамерних системах для одержання немиготливого перемикання. При спільному використанні камер із внутрішньою синхронізацією, вони комутируються пристроями, що містять пам'ять на кадр.

Об'єктиви відеокамер

Об'єктиви до камер відрізняються величиною фокусної відстані, світлосилою, характером створюваного оптичного зображення. При зйомці з однієї й тої ж точки об'єктивами з різними фокусними відстанями масштаб зображення змінюється прямо пропорційно величині фокусної відстані. Короткофокусний об'єктив навіть при невеликому диафрагмирувані має велику глибину різкості. Довгофокусний об'єктив навіть при зйомці вилучених об'єктів має обмежену глибину різкості. Об'єктив камери вибирається відповідно до призначення камери. Для максимального огляду вибирають широкоугольні об'єктиви з фокусною відстанню порядку 3,5 мм. При цьому кут зору камери буде близько 90°. Довгофокусні об'єктиви з фокусною відстанню 12 мм і кутом зору 30° використовують при спостереженні периметра об'єкта. Для використання в умовах штучного висвітлення необхідна можливість відключення електронного затвора й автоматичного регулювання посилення камери.

Об'єктив зі змінною фокусною відстанню

Для забезпечення ефекту збільшення зображення використовуються об'єктиви із трансфокатором, спеціальні телекамери з електронним трансфокатором, або цифрову апаратуру збільшення/зменшення зображення (відеопроцесори). Об'єктиви відеокамер, що мають змінну фокусну відстань, називаються « вари-об'єктиви». Вони дозволяють здійснити плавну зміну масштабу зображення (робити «наїзд»). Масштаб змінюється вручну або за допомогою електропривода. При цьому зберігається фокусування зображення. Застосування трансфокаторів дозволяє «наблизити» зображення від 5 до 20 разів, що дозволяє розглянути навіть сильно віддалені об'єкти.

Об'єктив з автоматичною діафрагмою

Об'єктив з автоматичною діафрагмою встановлює розмір отвору діафрагми, що забезпечує оптимальну інтенсивність світлового потоку, що проходить через об'єктив і попадає на мішень перетворювача «світло-сигнал». Використання об'єктивів з автоматичною діафрагмою дозволяє одержувати якісне зображення як при яскравому сонці, так і при місячному світлі.

Додаткові можливості й сервісні пристрої відеокамер

Автоматичне регулювання посилення

Режим автоматичного регулювання посилення дозволяє робити безперервну зйомку при всіх рівнях освітленості без необхідності перемикати посилення або застосовувати відповідні фільтри й має також таку чудову властивість, як пріоритетність апертури. Вона

полягає в тому, що після того, як вручну встановлена діафрагма, для одержання бажаної глибини різкості, система АРП автоматично встановлює необхідний рівень відеосигналу.

Електронний затвор

Структура матриці типу HAD дозволила застосувати електронний затвор з функцією змінного часу експозиції. Це дає можливість знімати передавальної ТВ камерою швидкоплинні динамічні процеси й об'єкти за час другої частини кожного поля, а це і є період відкривання електронного затвора.

Автоматична установка балансу білого

Ця функція корисна, коли оператор не має часу для установки камери в режим зйомки. Автоматична установка балансу білого полягає в підборі посилення в каналах червоного і синього кольору (у кольорових відеокамерах) стосовно посилення зеленого.

Гамма-корекція

Гамма-корекція - розтягування відеосигналу в області чорного. У деяких моделях відеокамер є схема, що дозволяє збільшити число градацій у передачі півтонів чорного й сірого кольору. Дія її фактично обратна дії схеми стиску контрастності, що підвищує й поглиблює контрастність півтонів у зображенні.

Монітори для систем телевізійного спостереження

Відеомонітор повинен забезпечувати строгу відповідність зображення подаваному відеосигналу. Параметри, що визначають якість зображення:

- чіткість;
- фокусування;
- відтворення кольору;
- відомість;
- геометричні перекручування.

Додаткові пристрої систем телевізійного спостереження

Спеціалізовані цифрові відеомагнітофони

Для запису зображення в системах телевізійного контролю служать спеціалізовані відеомагнітофони. Вони ведуть безперервний цифровий запис зображень у базу даних. Функціональні можливості відеомагнітофонів:

- запис і відтворення чорно-білого або кольорового зображення;
- програмування режимів запису;
- вивід на екран часу й дати;
- здійснення запису по таймері або по зовнішньому сигналі;
- програмування таймера з установкою щоденного початку й закінчення запису, а також установка режиму запису на тиждень;
- спеціальні режими відтворення (покадрове відтворення, пауза, швидкісний пошук вперед та назад);
- стоп-кадр;
- видача сигналів синхронізації на зовнішні пристрої;
- програмування режимів роботи при спрацьовуванні сигналізації;
- реєстрація часу аварійного відключення живлення; - зберігання інформації в енергонезалежній пам'яті.

У багатокамерних системах відеоспостереження відеомагнітофони використовуються разом з відеокомпресорами й мультиплексорами.

Відеокомпресори

Відеокомпресор (квадратор) - пристрій, що дозволяє на екрані монітора одночасно спостерігати в режимі реального часу зображення від декількох відеокамер і записувати його на відеомагнітофон. Наявність входу тривоги (ALARM-вхід) дозволяє підключити до відеокомпресора систему сигналізації, щоб при її спрацьовуванні автоматично підключити необхідну камеру для спостереження за об'єктом тривоги.

Мультиплексори

Мультиплексор дозволяє послідовно виводити на монітор і записувати на один відеомагнітофон інформацію від декількох телевізійних камер. При цьому запис здійснюється без втрати якості зображення. До мультиплексорів можна підключити систему сигналізації до ALARM-Входу. У деяких моделях це дасть можливість автоматично включити ту камеру, де відбулося порушення. Більшість мультиплексорів мають режим «динамічного розподілу часу запису» для кожної камери, а моделі MV-209 і MV-216 - вбудований детектор руху.

Детектори руху

При кількості камер більше чотирьох увага оператора розсіюється й ефективність спостереження знижується. При охороні банку потрібна установка великої кількості камер. Вирішити цю проблему можна установкою детекторів руху. Детектори руху обробляють відеозображення від телекамер і при необхідності можуть включати відеомагнітофон для запису зображення або подавати сигнал тривоги. Детектор реагує на зміну зображення об'єкта (контраст або рух) і подає сигнал тривоги.

Матричні комутатори

При великій кількості камер ефективність роботи оператора може бути підвищена шляхом застосування матричних комутаторів. Матричний комутатор дозволяє створити гнучку й нарощувану систему безпеки, у яку можуть входити не тільки системи телевізійного спостереження, але й системи охорони й контролю доступу. При наявності детектора руху, комутатор самостійно відслідковує ситуацію й, у випадку тривоги, виводить зображення від камер на монітори. Передустановки дозволяють задавати комутатору «маршрут» огляду об'єкта. При цьому на монітор будуть виводитися зображення обраних камер, збільшувати трансфокатор й т.д. Він називається режимом «вартового».

Відеопринтери

Для реєстрації відеозображення, поряд зі спецвідеомагнитофонами, у системах охорони використовуються й відеопринтери. Відеопринтери дозволяють роздрукувати:

- фотографії клієнтів;
- фотографії небажаних відвідувачів;
- кадри надзвичайних ситуацій;
- кадри з будь-якої відеокасети.

Передача зображення через IP-канал

Система дозволяє передавати оцифроване зображення через Ip-мережу. Можливо не тільки запитувати зображення, але й видавати сигнали керування на виконавчі пристрої, такі як поворотні пристрої, ворота, сирени й т.д. Здійснюється цифрова обробка й стиск відеоінформації. Цифровий метод передачі відеоінформації дозволяє використовувати одну лінію для передачі відео, графічних, інформаційних, тривожних, керуючих і програмних сигналів. Інформація передається блоками у відповідності зі спеціальним протоколом обміну, що дозволяє уникнути втрату інформації. При передачі серії кадрів, видається інформація тільки про зміни в зображенні. Середня швидкість 4800 бод.

Складовою частиною системи є програмне забезпечення, розроблене як для передавального, так і для прийомного пристрою. Воно містить зручне меню, у якому можна вибирати роботу з однією картинкою або з послідовністю кадрів, програмування режиму роботи камери й доступ до керуючого й архівному меню. У керуючому меню встановлюються Ip-адреса й паролі доступу. У тривожній ситуації можна витягти картинки, що зберігаються в архіві, і відтворити їх у будь-якій послідовності на екрані або на принтері.

Вибір системи телевізійного спостереження

Будь-яка система телевізійного спостереження включає три функціональні частини:

- телевізійні камери;
- апаратуру обробки відеоінформації;
- монітори.

По способу прийому й обробки відеоінформації розрізняють:

- традиційні системи тспостереження на базі спеціалізованої апаратури;
- комп'ютерні системи телевізійного спостереження.

Завдання системи телевізійного спостереження - наочно представити відеоінформацію про оперативну обстановку контрольованого об'єкта. Для рішення цього завдання, відповідно до характеристик контрольованих об'єктів, вибираються параметри системи. До основних факторів, що визначають вибір состава системи телевізійного спостереження відносяться:

- кількість контрольованих об'єктів;
- швидкість реакції системи;
- вартість;
- простота керування й можливість роботи у веденому режимі;
- надійність;
- гнучкість.

Параметри елементів системи телевізійного спостереження вибираються відповідно до характеристик об'єктів:

- розміри об'єктів;
- середня відстань до об'єктів;
- швидкість переміщення об'єктів;
- умови висвітлення об'єктів.

Завдання системи телевізійного спостереження - наочно представити відеоінформацію про оперативну обстановку контрольованого об'єкта. У комп'ютерних системах на одному моніторі відображається не більше 16 камер. При більшому числі камер розміри окремих зображень сильно зменшуються, а відеоканали перемикаються в режимі перелистування блоками до 16 камер.

Наочність поданя оперативної обстановки вище в системах з великою кількістю моніторів, тому що при цьому можливо відображення всіх камер одночасно із зображенням потрібного розміру. Швидкість обробки відеоінформації близька до обробки в масштабі реального часу й при оптимальному составі засобів обробки відеоінформації не залежить від кількості камер. У комп'ютерних системах швидкість обробки відеоінформації зменшується в міру росту кількості камер. Швидкість реакції апаратури на дії оператора вище в традиційних системах. Методи цифрової обробки дозволяють поліпшувати відеозображення, фільтрувати шуми, виділяти й досліджувати окремі деталі.

Комп'ютерні системи телевізійного спостереження

Комп'ютерні системи спостереження призначені для комплексного керування системою телеспостереження. Вони можуть забезпечувати охорону й контроль доступу в приміщення як невеликих, так і великих офісів банківської мережі й т.д.

Комп'ютерні системи забезпечують:

- Перегляд кольорового й чорно-білого відеозображення від одного до шістнадцяти джерел відеосигналів одночасно або на вибір оператора.
- Автоматичне або напівавтоматичне покадрове збереження зображення в цифровому виді із заданою дискретністю.
- Накладення дати, часу, службових сигналів і іншої інформації на відеозображення.
- Стиск і передачу по каналах обчислювальної мережі (глобальній, локальній), а також по каналах телефонного зв'язку через модем.
- Покадровий перегляд збереженої відеоінформації з можливістю завдання вибірки й сортуванню по даті, часу, найменуванню об'єкта та ін.
- Обробку зображення цифровими методами в реальному масштабі часу:

- трансфокация;
- регулювання яскравості, колірної насиченості, контрастності;
- монтаж відеозображень;
- компенсація тла, засвіток, фільтрація шумів та ін.

- Дистанційне керування системою по телефонній лінії.
- Підключення службових сигналів (сигнал тривоги, виклику, і ін.) і можливість автоматичного керування системою по заданому алгоритмі (зменшення інтервалів часу запису кадрів при надходженні сигналів тривоги).
- Програмне й дистанційне керування системами охорони й багаторівневого доступу.

Основною перевагою комп'ютерних систем є їхня гнучкість. Для керування засобами телеспостереження, сигналізації й системою контролю доступу використовують програмні засоби. Графічний редактор дозволяє побудувати план будинку з автоматичним виводом зображення «тривожної зони». Програма керування пристроями телеспостереження дозволяє управляти комутаторами, відеомагнітофонами, мультиплексорами, трансфокаторами камер, моніторами й т.д.

В процесі практичної реалізації теоретичних принципів розробки системи, була розроблена структурна схема обробки відеосигналу, яка зображена на рисунку 1. Завдяки структурній схемі можна чітко побачити основні структурні блоки системи та взаємозв'язки між ними.

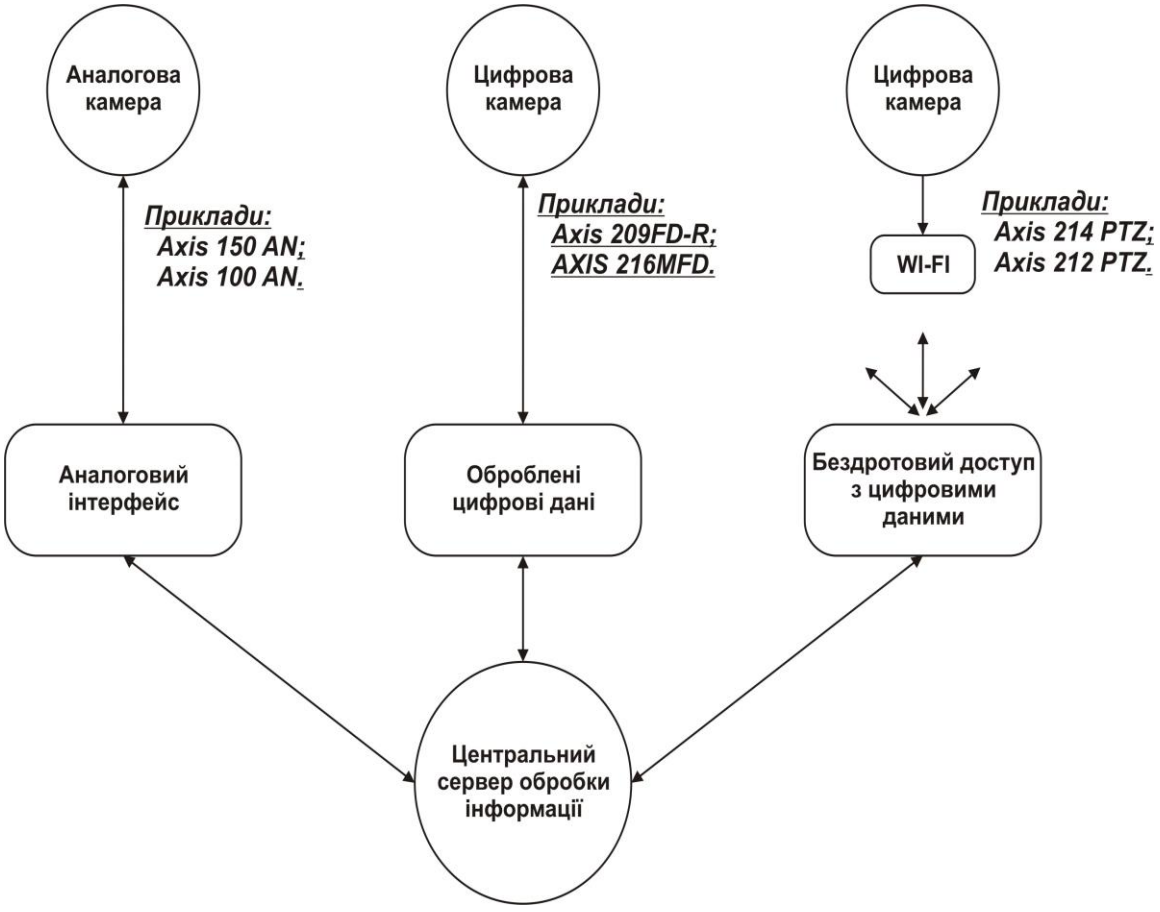


Рисунок 1 – Структурна схема обробки відеосигналу

При розробці структурної схеми основний упор робився на існуючи розробки ПЗ і їх модулі допомоги.

Аналіз рисунка 1 дозволяє чітко прослідити як працює програма. Розглянемо схему зверху вниз, в напрямку від пристрою до кінцевої програми.

Відеосигнал йде з блоку спостереження (цифрова відеокамера, аналогова відеокамера) після отримання відеоінформації з якого відбувається передача потоку у центральний сервер обробки інформації. Передача залежить від способу підключення пристрою

відеоспостереження, що і відображено у середньому блоці структурної схеми обробки відеосигналу.

Для проведення спостереження за об'єктами застосовувалося встаткування фірми Axis Communications. Устаткування фірми дозволяє об'єднати всі пристрої цифрової й аналогової системи відеоспостереження в мережу з єдиним центром керування (приклади встаткування зазначені на рисунку 1.).

Системи відеоспостереження найбільш ефективні для банківської сфери, де є розгалужені приміщення, склади, офіси й інші об'єкти, де без вилученого відеоспостереження просто не обійтися.

За рахунок децентралізації всієї системи відеоспостереження служба охорони, може уникнути марного використання мережних ресурсів і незручностей, що виникають через обмежену пропускну здатність мережі.

Головним інтелектуальним вузлом цифрової системи відеоспостереження на об'єкті є мережний цифровий відеореєстратор AXIS 100 AN, 150 AN. До нього можна підключити 4 аналогові або 5 цифрових відеокамер (рисунок 3.2), установлених на віддалених об'єктах. Інформація з відеокамер стискується JPEG компресором відеореєстратора й записується на його жорсткі диски.

Рисунок 2 - Задня стінка відеокамери з доступними інтерфейсами взаємодії застосовувана при реалізації дипломного проекту

Запис може здійснюватися в декількох режимах: безупинно, запис подій/тривожних ситуацій, ручна або за графіком. Відеореєстратор має всі необхідні компоненти для запису й перегляду відеопо мережі: центральний процесор, Ethernet інтерфейс, контролери пам'яті, інтерфейси пристроїв, JPEG компресор, місце для установки до чотирьох жорстких дисків IDE.

Обраний метод побудови системи в дипломному проектуванні в побудові цифрової системи відеоспостереження, різко знижує обсяг переданої по мережі інформації й полегшує роботу операторів, що в остаточному підсумку дає великий економічний ефект. Висока надійність AXIS 100 AN, 150 AN і підтримка різних протоколів обміну інформації дозволяють використовувати його як у локальні (LAN), так і в глобальні (WAN) мережах, а застосування апаратури фірми Adder (розглянуто нижче) дозволяє забезпечити високий ступінь безпеки, що необхідно в банківській справі. Цифрову систему відеоспостереження досить легко інтегрувати йз уже наявними системами охоронної сигналізація й контролю доступу на об'єкт.

Для організації надійних каналів передачі відеопотоку, а також організації робочого місця оператора (відеотермінала). При розробці дипломного проекту була обрана апаратне забезпечення фірми Adder.

Устаткування Adder дозволяє збільшити число використовуваних моніторів і пристроїв уведення (мишок/клавіатур), необхідних для керування системою відеоспостереження.

Абревіатура використовувана на структурній схемі побудови й роботи системи VKVM розшифровується як як: «клавіатура» («Keyboard»), «монітор» («Video monitor»), «миша» («Mouse»).

Розглянемо докладно як реалізована робота VKVM у випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти – до центрального ПК за допомогою інтерфейсного кабелю Adder VKVM-2M, підключається AdderView AVP4 – KVM перемикач. Він являє собою цифровий пристрій, комутуючий відеосигнал монітора й сигнали клавіатури й миші від центрального комп'ютера на кілька комплектів Клавіатура/Монітор/Миша (Keyboard/Video/Mouse.) KVM перемикач AdderView AVP4, складається із двох основних пристроїв:

- відео-перемикач, що міняє напрямок аналогових відеоімпульсів між моніторами й комп'ютером спільного використання;
- мікропроцесорна система, що передає й приймає сигнали із клавіатури й миші й дає можливість управляти комп'ютером з кожного з робочих місць по черзі перемикаючись між ними).

При цьому число комплектів Клавіатура/Монітор/Миша визначається тільки можливостями й кількістю KVM-перемикачів. Немає необхідності мати спеціальне програмне забезпечення, і відсутні традиційні громіздкі процедури підключення все реалізується на апаратному рівні, що забезпечило можливість у випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти реалізувати практичну й зручну систему терміналів і зосередити зусилля на більше глибокому пророблені реалізації обробки відеопотоку інформації.

KVM перемикач AdderView AVP4 здатний віддаленно підключити до центрального комп'ютера до 4 комплектів Клавіатура/Монітор/Миша або інше встаткування. Для того, щоб розгалузити систему до AdderView AVP4 за допомогою інтерфейсних кабелів Adder VKVM - 0,5M використовувалося підключення 3 KVM перемикачі AdderView AVP2, кожний з яких дозволяє віддаленно підключити до 2 робочих місць, що підходить у поставленому завданні дипломного проектування.

До них, у свою чергу, підключаються подовжувачі AdderLink ALXT, які допомагають одержати високу якість зображення й звуку на відстані до 300 м. Екстендери Adder, забезпечують передачу відеосигналу з високим розрішенням, і можливість гнучкого розподілу пристроїв, керування, контролю й взаємодії із пристроями відображення.

При використанні екстендерів Adder AdderLink немає необхідності використовувати оптоволоконі кабелі й розташовувати центральний процесор поруч із кожним екраном. Екстендер ALXT, що є приймачем цифрових сигналів зв'язується з ALXR (передавач цифрових сигналів), за допомогою мережного кабелю CAT5 (кабель типу "кручена пари" категорії 5).

До екстендерів ALXR за допомогою кабелів Adder VKVM - 0,5M підключаються 6 комплектів Клавіатура/Монітор/Миша.

Вибір такого типу обладнання в дипломному проектуванні дозволило застосовувати тільки один кабель для кожного підключення до кожного робочого місця, що дуже зручно при прокладані комунікаційних ліній.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів комплексного відеонагляду банківської установи. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем комплексного відеонагляду банківської установи. Досліджена система комплексного відеонагляду банківської установи. На основі отриманих результатів досліджень створена програмна реалізація системи комплексного відеонагляду банківської установи. Розроблені алгоритми дозволяють успішно вирішувати завдання комплексного відеонагляду банківської

установи. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
2. Дрєєв О.М. Моделювання впливу інтенсивності трафіку на оперативність доставляння інформації / О.М. Дрєєв // Науково-виробничій журнал "Зв'язок". – Київ: ДУТ, 2014. – № 2 (108) С. 24-29.
3. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
4. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19
5. Дреев А.Н. SPIHT кодирование с отложенной передачей значимых битов / А.Н. Дреев // Тези доповідей. Новітні технології – для захисту повітряного простору. Дев'ята наукова конференція 17 квітня 2013 р. – Х.: ХУПС. – 2013. – С. 206
6. Дреев А.Н. Повышение оперативности доставки данных повышенной востребованности в телекоммуникационных системах и сетях / А.Н. Дреев, А.А. Смирнов, Е.В. Мелешко // Проблеми і перспективи розвитку ІТ-індустрії 25-26 квітня 2013 р. Системи обробки інформації. – Випуск 3 (110). Том 2. – Харків: ХУПС. – 2013. С. – 199.
7. Дрєєв О.М. Середньостатистичний та найімовірніший час доставки багатопакетного повідомлення в телекомунікаційній системі або мережі / О.М. Дрєєв, О.А. Смірнов // V Всеукраїнська науково-практична конференція "Інформатика та системні науки" ІСН – 2014, 13-15 березня 2014 року, м. Полтава – С. 92
8. Дрєєв О.М. Визначення оптимального розміру блоку при бітовому арифметичному кодуванні / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 11-12 квітня 2014 р. – Кіровоград – С. 44
9. Дреев А.Н. Экстраполяция квазипериодических процессов с аддитивными помехами / А.Н. Дреев, А.А. Смирнов // П'ята Міжнародна науково-практична конференція "Інформаційні технології та моделювання в економіці" 15-16 травня 2014 р. – Черкаси – С. 59
10. Дреев А.Н. Статистическая модель передачи многопакетного сообщения в телекоммуникационной системе или сети / А.Н. Дреев, А.А. Смирнов // «Компьютерное моделирование в наукоемких технологиях (КМНТ-2014)» Харьков, 28-31 мая 2014 года – С. 137-140

УДК 004

А. Загорій, магістр гр. КІ-20М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЛЯ ЗАХИСТУ ПРОГРАМНИХ МАСИВІВ НА ОСНОВІ ВИКОРИСТАННЯ БІБЛІОТЕКИ CRYPTO API

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Метою розробки є дослідження та програмна реалізація системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Об'єктом дослідження є процес кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Предметом дослідження є методи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Методи дослідження базуються на методах захисту

інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, захисту доступу, Crypto API

Постановка проблеми. Інформація про уразливість може бути використана зловмисниками при написанні вірусів. Наприклад, один з найперших відомих мережевих черв'яків (вірус Morica) в 1988 році використовував такі уразливості як переповнення буфера в Unix-демоні finger для поширення між машинами. Тоді кількість заражених машин склало близько 6 тисяч, а економічний збиток за даними рахункової палати США склав від 10 до 100 млн доларів.

З 2016 комп'ютерні віруси завдали світовій економіці збитків в 450 млрд. доларів. У 2017 збиток від вірусу WannaCry оцінили в 1 млрд. доларів. Випадки зараження були зафіксовані щонайменше в 150 країнах. Вірус застосовував експлойт EternalBlue, що використовує уразливість в протоколі SMB, пов'язану з переповненням буфера. У 2017 році відбулась масштабна хакерська атака з боку Росії проти України та ще 59 країн. Причиною стала компрометація системи оновлення програми M.E.Doc встановленням бекдору та вірусу NotPetya. Збитки підприємств по всьому світу склали 8 млрд. доларів.

Сучасний комп'ютерний світ представляє собою різнобічну і досить складну сукупність обчислювальних засобів, систем обробки інформації, комунікаційних технологій, програмного забезпечення (ПЗ) та високоефективних засобів його проектування. Вся ця багатогранна та взаємопов'язана метасистема вирішує величезне коло проблем в різноманітних сферах людської діяльності: від простого рішення шкільних задач на домашньому персональному комп'ютері (ПК) до управління складними технологічними процесами та космічними технологіями. Тому природним шляхом розвитком інформаційних технологій на даний час є принциповий перехід від відкритого використання інформаційних масивів та КС до захищеного їх використання.

Як показав проведений в період переддипломної практики аналіз провідних комп'ютерних фірм світової спільності, вбудовані в сучасні ОС механізми захисту не забезпечують гарантованого захисту інформації від несанкціонованого доступу. На жаль, це також є типовою тенденцією, отже – під сумнівом обгрунтованність концепції вбудованої системи захисту в сучасних ОС, а значить виникає необхідність в використанні додаткового захисту інформації.

Враховуючи вищеозначене та той фактор, що світова спільнота вступила в цифрове століття, коли на зміну паперовим носіям інформації прийшли електронні, а особисті контакти все частіше замінюються листуванням по e-mail з засвідченням необхідних документів цифровим електронним підписом, криптографічні алгоритми стають звичним та вкрай необхідним інструментом. Проте ніякий, навіть найкраще реалізований механізм захисту, не зможе забезпечити якісного захисту комп'ютерної інформації в цілому. Захист інформації потребує комплексування різнорідних механізмів в єдину систему. Таким чином, при розробці ВКРМ основним об'єктом нашої уваги будуть вимоги до заданих якостей захищеності, які будуть забезпечуватись сукупністю реалізованих захисних механізмів: блочного шифрування, електронний цифровий підпис зашифрованих файлів, електронний цифровий підпис файлів.

На ринку програмних продуктів (ПП) пропонується досить великий діапазон систем аналогічного спрямування та класу. Але більшість з них на даний час вже зламані та й коштують такі системи досить дорого, що, враховуючи економічний стан нашої країни, робить ці досить привабливі системи недосяжними для багатьох користувачів. Таким чином, розробка комплексних систем захисту на даний час є питанням дійсно актуальним та перспективним.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API.

– Дослідження системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API.

– Програмна реалізація системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API.

Об'єктом дослідження є процес кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API.

Предметом дослідження є методи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу Забезпечення надійного захисту інформації не є разовим заходом, а сукупністю різноманітних заходів. Але традиційна архітектура навіть комплексної системи захисту не є оптимальним рішенням поставленої задачі, адже зловмисники – це професіонали вищого ґатунку, які постійно вдосконалюють свою майстерність та професійний рівень. Це підтверджує той факт, що на даний час всі існуючі системи захисту фактично вже зламані.

Тому при розробці системи захисту було вирішено використати нетрадиційний підхід до побудови її архітектури, в основі якої закладений науковий напрямок "Теорія забезпечення безпеки програм та їх комплексів".

Використання цього напрямку забезпечує: інтеграцію основних наукових положень прикладної теорії алгоритмів, теорії управління якістю ПЗ, теорії надійності і дозволяє на практиці реалізувати єдині системні позиції попередження випадкового/навмисного розкриття, злому, знищення зберігаємої/обробляємої/захищаємої/траспортуємої інформації/ПП в локальній та глобальній мережах.

Вирішення проблеми забезпечення цілісності і достовірності інформації при її передачі в захищених/незахищених мережах, витікає з необхідності захисту від зловмисних дій, адже несанкціоноване зчитування інформації, яке здійснюється в мережі, направлене:

– на одержання секретної інформації;

– на ідентифікацію інформації, яку запитує користувач;

– на зчитування паролів та їх ототожнення з конкретним користувачем;

– на спотворення або видалення власної інформації сервера та порушення роботи мережі;

– на контроль активності абонентів мережі для одержання побічної інформації про взаємодію користувачів та характер інформації, якою обмінюються абоненти мережі.

Окрім цього, зловмисником:

– можуть бути змінені атрибути (характеристики) електронних документів;

– зловмисник може видати себе за дійсного власника електронного документа або, навпаки, відмовитись від авторства на власний документ/файл;

– зловмисник може дизасемблювати та скопіювати програму з ціллю її подальшого розповсюдження.

Найбільш ефективними методами захисту від вищеозначених зловмисних дій та погроз є криптографічні методи захисту.

Це обумовлено тим, що відомі та поширені способи контролю цілісності програм розроблені на базі використання контрольної суми повздовжнього контролю і контролю на чітність, і, як правило, представляють собою досить прості (але надійні) способи захисту від внесення змін в код програм.

Оскільки область значень контрольної суми досить обмежена, а значення функції контролю на чітність взагалі представлені одним-двома бітами, то для досвідченого порушника не важко найти наступну колізію:

$$f(k_1) = f(k_2), \quad (1)$$

де k_1 – код програми без спотворення;

k_2 - код програми, спотворений зловмисником;

f - функція контролю.

В цьому випадку, значення функції для різних аргументів співпадають, а це означає, що тестування не виявить внесених дефектних змін до файлу.

Тому для встановлення достовірності необхідно використати більш складні методи, такі, як автентифікація з використанням криптографічних методів, які віднайдуть також і сліди, що залишив зловмисник.

Найбільш ідеальним варіантом є забезпечення такого ступеню захисту, коли зловмисник не зможе використати в комерційних цілях одержаний файл з однієї причини – він не зможе його одержати.

Термін “криптологія” походить від двох грецьких слів: “крипто” (тайний) та “логос” (вчення). Криптологія, як наука, складається з двох тісно теоретичних і практично пов’язаних дисциплін: криптографії та криптоаналіза.

Криптографія – це наука про способи та методи перетворення (шифрування) інформації з ціллю її захисту від незаконних користувачів. Криптоаналіз займається методами і способами злому шифрів.

Шифр (криптосистема) – метод перетворення інформації з ціллю її захисту від незаконних користувачів. Злом шифру – процес одержання інформації з шифрованого повідомлення без знання використаного шифра.

Шифрування – процес використання шифру до інформації, що підлягає захисту. Дешифрування – процес, зворотний шифруванню.

Вихідний текст, що має сенсове/логічне значення, яке необхідно зашифрувати, називають відкритим текстом. Зашифрований текст, що має вигляд випадкового набору символів/цифр, називається шифротекстом або криптограмою.

Під ключем в криптографії слід розуміти змінний елемент шифру, який використано для шифрування конкретного відкритого тексту.

Зазвичай, атака зловмисника (криптоаналітика) зводиться до спроби розкриття шифру (спроба здійснення атаки) на основі шифротекста. Якщо ж зловмисник має до того ж деякі уривки відкритого тексту і відповідні їм елементи шифротексту, тоді слід чекати спроби здійснення атаки на основі відкритого тексту.

Атака на основі вибраного відкритого тексту заключається в тому, що противник, використавши свій відкритий текст, одержує правильний шифротекст і робить спробу зламати шифр.

Теоретично існує абсолютно стійкій шифр, але єдиним таким шифром є будь-яка форма стрічки одноразового використання, в якій відкритий текст об’єднується з випадковим ключем такої ж довжини.

Цей результат був доказаний К.Шеноном за допомогою розробленого їм теоретико-іформаційного метода дослідження шифрів, але широкого застосування на практиці фактично не одержав із-за великої ступені складності та високої ціни.

В силу даних причин, абсолютно стійкі шифри використовуються тільки в спеціальних мережах для передавання особливо важливої державної інформації. Тому цей метод недоцільно застосовувати в нашій розробці.

Щоб криптозахист не можна було "обійти" з іншої сторони, доцільно використати вбудовані криптографічні можливості ОС Windows. До недоліків слід віднести повноцінне функціонування Crypto API тільки на базі ОС Windows. Тому при виборі операційної системи, на яку буде орієнтована наша розробка, ми зупинимось саме на цій операційній системі.

Функції Crypto API забезпечать прикладним програмам системи доступ до криптографічних можливостей Windows, але вони є лише "передавальною ланкою" в складному ланцюгу обробки інформації.

Основну роботу будуть виконувати сховані від очей програміста функції, які входять в спеціалізовані модулі – провайдери (постачальники) криптографічних послуг, або криптопровайдери, як це показано на рисунку 3.1.

Програмна частина криптопровайдера представляє собою dll-файл, підписаний Microsoft; періодично Windows перевіряє ЕЦП, що виключає можливість заміни (підміни) криптопровайдера. Криптопровайдери відмінні один від одного наступними ознаками: складом функцій (одні – виконують шифрування, інші – створюють та провіряють ЕЦП, тощо); вимогами до ОС алгоритмами, що здійснюють базові дії (створення ключів, хешування, тощо).

По складу функцій і забезпечуючих їх виконання алгоритмів, криптопровайдери підрозділяються на типи.

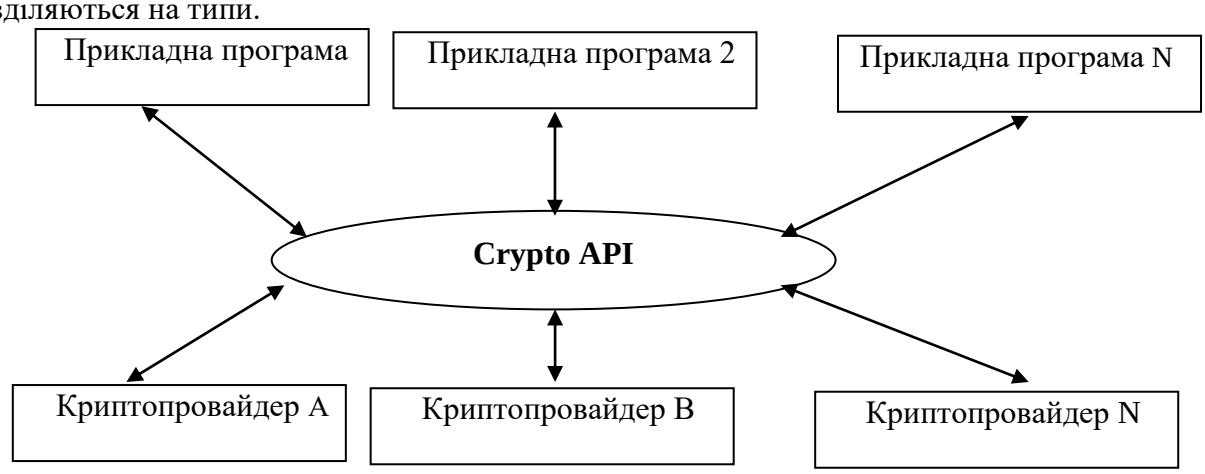


Рисунок 1 – Структурна схема взаємозв'язку ПП з криптопровайдерами

Наприклад, CSP типу RROV RSA FULL (підтримує як шифрування, так і ЕЦП) використовує для обміну ключами і створення ЕЦП алгоритм RSA, для шифрування – алгоритмами RC2 та RC4, для хешування МД5 та SHA.

Використання криптографічних можливостей Windows, по сутті, є роботою програми з графічним пристроєм на низькому рівні, адже криптопровайдер подібний графічному драйверу: він може забезпечувати взаємодію ПЗ з обладнанням (пристрій читання смарт-карт, апаратні датчики випадкових чисел, тощо).

Для виведення інформації на графічний пристрій, додаток не повинен безпосередньо звертатися до драйвера – замість цього в системі необхідно одержати контекст пристрою за допомогою якого і будуть здійсненні всі операції. Це дозволить використовувати при написанні програми графічний пристрій, нічого не знаючи про його програмну реалізацію. Точно такий же принцип використаний і для криптографічних функцій: додаток звертається до криптопровайдера не напрямки, а через CryptoAPI, але спочатку провівши запит в ОС контексту криптопровайдера.

Таким чином, ОС Windows надає дуже зручний інструмент для організації криптозахисту у вигляді бібліотеки CryptoAPI з набором функцій та процедур з

криптопровайдерами, але необхідно розробити алгоритми реалізації основних функцій системи криптозахисту:

– підключення;

– шифрування/розшифрування за допомогою симетричних/асиметричних ключів;

– створення контейнерів ключів;

– створення ключових пар, тощо.

Ці алгоритми об'єднаємо в модуль CryptoAPI.

Після того, як будуть викликані відповідні криптопровайдери (через функції Crypto API), перейдемо до шифрування файлів. Шифрування будемо виконувати з урахуванням вищеозначених вимог, обмежень і таким чином, щоб лише користувач/розробник, знаючий відповідний пароль, міг одержати доступ до них. Більш детально розробка БСА та їх програмування будуть описані в розділі 4 пояснювальної записки.

Для розробки ПЗ підсистеми нами обрано мову програмування DELPHI, обґрунтування цього вибору надається в розділі 2 пояснювальної записки.

Таким чином, нами визначені та обґрунтовані:

– вимоги та обмеження, врахування яких повинна забезпечити система;

– методи, які будуть використані при розробці архітектури системи та її програмного забезпечення;

– функції, виконання яких повинна забезпечити система.

Маємо всі необхідні дані для визначення структури майбутньої системи та розробки її структурної схеми та функціональної схеми.

Розробка структурної схеми

Основною задачею, що повинна бути виконана згідно технічного завдання та постановки задачі на реалізацію ВКРМ, є розробка програмного забезпечення системи кібербезпеки для захисту інформаційних та програмних масивів на основі використання бібліотеки Crypto API

Розроблене ПЗ повинне забезпечити в процесі експлуатації виконання наступних функцій:

– шифрування/розшифрування об'єкту захисту за допомогою симетричних та асиметричних алгоритмів (використаємо їх комбінацію) та блочних шифрів;

– створення: контейнерів ключів, ключових пар, ключа обміну ключами (КОК), електричного цифрового підпису (ЕЦП);

– створення: цифрових конвертів, сеансових ключів за допомогою блочних шифрів;

– з'єднання з криптопровайдером ОС Windows;

– визначення хеш-функції.

На основі визначених вимог та обмежень до майбутньої системи визначимо більш детально компоненти її структури.

Система умовно поділена на дві змістовні частині:

– частина 1 «ПЗ захисту. Клієнтська частина»: бібліотека CryptoAPI, функції шифрування: шифрування блочним шрифтом, шифрування блочним шифром і підпис ЕЦП, підпис файлів ЕЦП; передача на сервер; прийом від сервера; дешифрування одержаних файлів;

– частина 2 "ПЗ захисту. Серверна частина": передача клієнту списку файлів знаходиться на зберіганні; передача клієнтській частині файлів по запиту; збереження файлів.

В якості технології передачі даних використаємо технологію Socket та протоколи TCP/IP.

Елементи частини 1 та частини 2 певним чином пов'язані, а вихідний елемент є постійним і фіксованим. Разом з тим, вони, як елементи системи, тісно взаємозв'язані, використовуючи в процесі роботи вихідні дані однієї частини, як вхідні дані іншої.

Використання в системі декількох механізмів захисту одночасно до одного і того ж файлу, дозволить розробити дієспроможну та досить потужну систему, призначення якої – забезпечення захисту інформації в мережі від НСД та НСВ.

Написання такого програмного продукту вимагає від програміста-розробника знання принципів побудови комп'ютерних систем захисту програмних продуктів та дотримання вимог, які пред'являються до систем аналогічного класу та спрямування, (описаних в розділі 2 пояснювальної записки).

Під час розробки ПЗ згідно теми ВКРМ, автор має звернути увагу на можливість вирішення програмою найбільшого кола задач, врахувавши при цьому позитивні якості систем-аналогів, розглянутих в розділі 2 пояснювальної записки, та здійснити спробу уникнення виявлених недоліків.

В процесі експлуатації система захисту, на основі використання бібліотеки Crypto AP, має вирішувати наступні основні питання:

- шифрування об'єкту захисту (модуль криптозахисту);
- підписання файлу з елементами захисту ЕЦП (модуль криптографії)
- дешифрування одержаного файлу;
- автентифікація респондента по ЕЦП,

які підлягають програмній реалізації в процесі виконання ВКРМ.

Таким чином, нами визначені складові компонента майбутньої системи, способи зв'язку між ними та чітко визначені функції, які вони будуть виконувати. Тому можемо розробити структурну схему системи, яка наведена на рисунку 3.2.

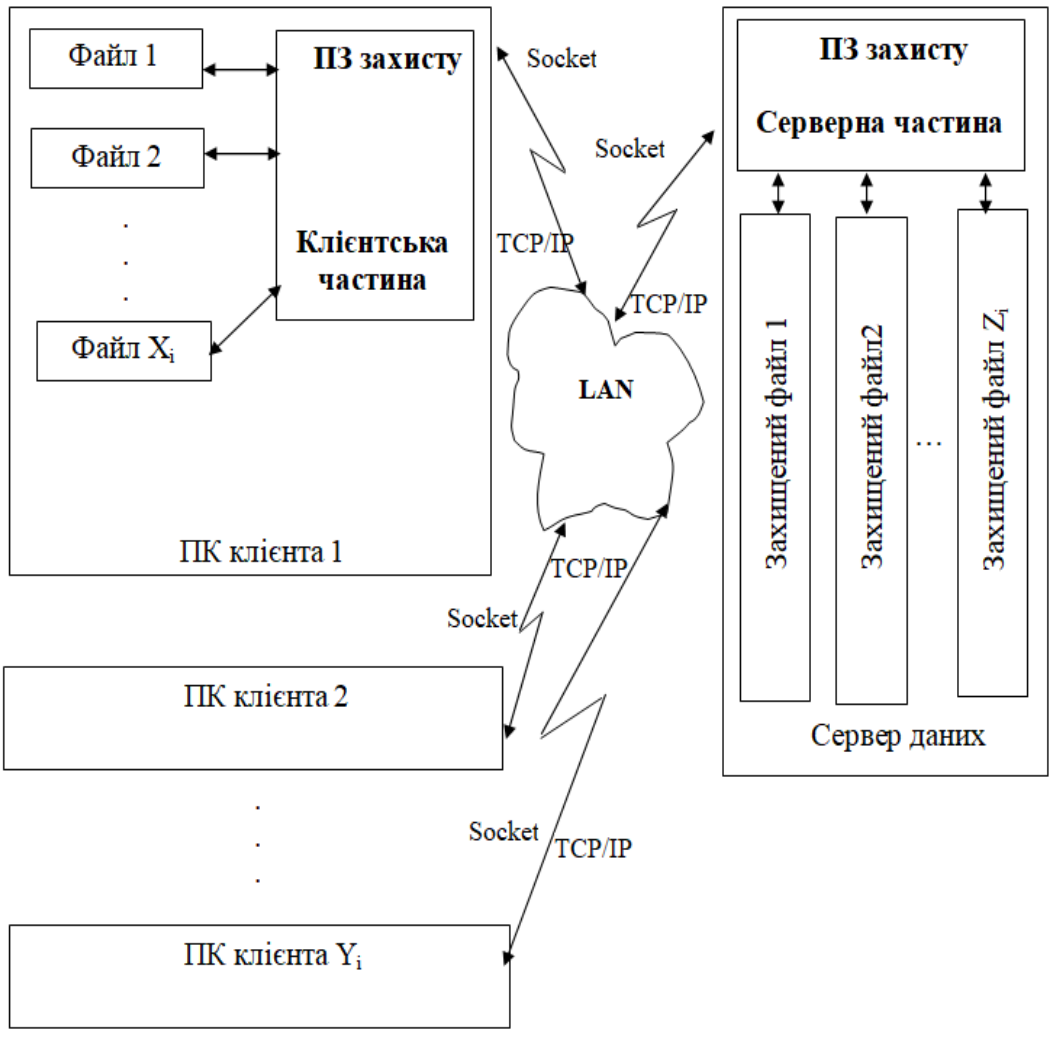


Рисунок 2 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Досліджена система кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Розроблені алгоритми дозволяють успішно вирішувати завдання кібербезпеки для захисту програмних масивів на основі використання бібліотеки Crypto API. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
3. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
4. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.
5. Смирнов С. А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2014. – Вип. 4 (41). – С. 48-52.
6. Смирнов С. А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. – Х.: ХУПС, 2014. – № 4(17). – С. 90-95.
7. Смирнов С. А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, Н. С. Якименко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2015. –Вип. 1(126). – С. 150-153.
8. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.
9. Смирнов С. А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты даннях / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Системи озброєння і військова техніка: наук. журн. – Х.: ХУПС, 2015. – № 3(43). – С. 100-107.
10. Смирнов С. А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А. А. Смирнов, С. А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України: наук. журн. –Х.: ХУПС, 2015. –№ 3(20). – С. 134-141.

УДК 004

М. Джевлах, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВІРТУАЛІЗОВАНОЇ СЕРВЕРНОЇ ІНФРАСТРУКТУРИ НА БАЗІ HCI

У статті розроблено програмне забезпечення, яке призначено для системи віртуалізованої серверної інфраструктури на базі HCI. Метою розробки є дослідження та програмна реалізація системи віртуалізованої серверної інфраструктури на базі HCI. Об’єктом дослідження є процес віртуалізованої серверної інфраструктури на базі HCI. Предметом дослідження є методи віртуалізованої серверної інфраструктури на базі HCI. Методи дослідження базуються на методах теорії комп/ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи віртуалізованої серверної інфраструктури на базі HCI. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп’ютерна інженерія, віртуалізована серверна інфраструктура, HCI

Постановка проблеми. Основними перевагами технології віртуалізації робочих місць (VDI), у порівнянні зі звичайними десктопами, є істотне зниження витрат на обслуговування парку настільних комп'ютерів і підвищення інформаційної безпеки. Незважаючи на ці важливі переваги, впровадження VDI йде повільно. Як же можна його прискорити?

VDI припускає використання віртуалізованої серверної інфраструктури для запуску віртуальних машин з копіями операційної системи й застосунків ПК. Замість настільних ПК на робочому місці користувача встановлюється тонкий або нульовий термінал з мінімальною процесорною потужністю, а настільні застосунки виконуються на віртуалізованому сервері, на якому розгорнута VDI.

Основними перевагами VDI, у порівнянні зі звичайними десктопами, є істотне зниження витрат на обслуговування парку настільних комп'ютерів (насамперед за рахунок економії робочого часу системних адміністраторів) і підвищення інформаційної безпеки при використанні конфіденційних даних. Крім того, оскільки компонентів, які можуть вийти з ладу, таких як жорсткі диски, у термінала менше, ніж у звичайних настільних ПК, витрати на ремонт клієнтських комп'ютерів скорочуються.

Однак, незважаючи на ці важливі переваги, впровадження VDI іде повільно, особливо якщо зрівняти з технологіями віртуалізації серверної інфраструктури, які давно стали фактичним стандартом для IT-інфраструктури сучасної компанії. В Україні темпи впровадження рішень VDI значно нижче, ніж у Європі й США. Почасти це можна пояснити тим, що праця системних адміністраторів і інших спеціалістів, відповідальних за обслуговування IT-інфраструктури, в українських компаніях оцінюється не так високо, як на Заході.

У результаті при заміні настільних ПК на віртуальні столи потенційна економія витрат на зарплату IT-персоналу не настільки значна й не може виправдати інвестиції на придбання потужних серверів і систем зберігання, необхідних для побудови віртуалізованого середовища. Тому в нашій країні VDI найчастіше впроваджується в організаціях, де вимоги до інформаційної безпеки робочих місць співробітників досить високі: насамперед у банках і інших організаціях фінансового сектора.

Гіперконвергентна інфраструктура (HCI) – це ПЗ-центрична архітектура із твердою зв'язаністю елементів зберігання, мереж і обчислень, інтегрованих у стандартне устаткування одного постачальника.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи віртуалізованої серверної інфраструктури на базі HCI"

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи віртуалізованої серверної інфраструктури на базі HCI.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем віртуалізованої серверної інфраструктури на базі HCI.
– Дослідження системи віртуалізованої серверної інфраструктури на базі HCI.
– Програмна реалізація системи віртуалізованої серверної інфраструктури на базі HCI.

Об'єктом дослідження є процес віртуалізованої серверної інфраструктури на базі HCI.

Предметом дослідження є методи віртуалізованої серверної інфраструктури на базі HCI.

Методи дослідження базуються на методах теорії комп/ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Опис функціонування системи

Технологія VDI

Кожний співробітник, приходячи на роботу, повинен одержати доступ до своїх програм. IT відділ повинен забезпечити безперервну якісну роботу всіх застосунків. Класичний спосіб – це виділений кожному користувачеві комп'ютер, що вимагає первісного налаштування й подальшого обслуговування. Альтернативний спосіб рішення завдання – VDI, служби віртуальних робочих столів.

У сучасному бізнесі доступ до корпоративних сервісів повинен бути доступний співробітникам з будь-яких доступних пристроїв і не обмежується стаціонарним комп'ютером. Тому VDI у реалізації зараз став складніше, ніж був ще кілька років назад.

Проблематика (ПК)

Нема сенсу впроваджувати нову технологію заради технології. Якщо в компанії немає проблем з експлуатацією парку комп'ютерів, користувачі задоволені, керівництво досить, то потрібно серйозно задуматися потрібно чи щось міняти. Інша справа якщо є проблеми, які не вдається вирішити протягом довгого років. Нижче перераховані класичні проблеми, з якими зіштовхуються IT відділи при обслуговуванні інфраструктури персональних комп'ютерів:

– простій у роботі, співробітник не може виконувати свої безпосередні обов'язки під час виконання процедур по обслуговуванню ПК.
– персонал, для обслуговування ПК необхідний штат співробітників. Чим більше комп'ютерів у компанії, тим більше штат.
– програмне забезпечення, установлене на ПК жадає від IT співробітників своєчасного відновлення, налаштування, оптимізації.
– безпека, особистих даних користувачів змішуються з корпоративною інформацією. Співробітники мають фізичний доступ до інформації, що зберігається на дисках ПК.
– застарілий парк ПК, у деяких компаніях комп'ютери не міняються десятиліттями, швидкість роботи на таких пристроях украй низька.
– філіальна мережа, викликає складності із часом реагування на інциденти, якщо потрібне особиста присутність адміністратора для його рішення.
– і багато чого іншого.

Керівники IT з більшим інтересом ставляться до нових технологій, відвідують виставки, семінари, слухають представників вендорів. Якщо розглядати VDI, то реальну картину до впровадження, під час впровадження й після впровадження представити по маркетингових слайдах неможливо. Потрібно співробітничати з командою, що вже робила подібні проекти й зможе попередити про прийдешні труднощі.

Основні принципи VDI

Якщо раніше VDI був дивиною для IT, то зараз складно знайти велику компанію, де його немає зовсім. Часто це пілотні проекти, які були зроблені безкоштовно й працюють роками після впровадження. Нижче перераховані основні концепції які описують робочий процес, якої він повинен бути після впровадження VDI. Що повинна принести нова технологія і як вона спростить роботу користувачам і підніме на новий щабель знань адміністраторів:

– Співробітник зі свого робочого місця, ноутбука або мобільного пристрою підключається до свого віртуального робочого місця, що перебуває на серверах організації.

– Користувач одержує доступ тільки до дозволеним адміністратором застосункам. Всі користувачі компанії діляться на групи, у кожної групи є список доступних застосунків.

– Керівництво розуміє, скільки і які ліцензії потрібно для роботи компанії і яких співробітників використовують ці застосунки.

– Програми налаштовуються й обновляються централізовано адміністратором і не вимагають переривання робочого процесу співробітників.

– Кожний користувач одержує доступ до виділеної віртуальної машини, запущеної на сервері. Віртуальна машина створюється й запускається автоматично. Якщо співробітник не працює, то серверні ресурси не використовуються.

– Всі віртуальні машини ізольовані друг від друга, тому сесії користувачів не перетинаються й не впливають один на одного.

– Всі дані користувача зберігаються на серверах компанії й надійно захищені від втрати у випадку збоїти або поломки пристрою користувача

– Після впровадження проекту vdi значно знижується навантаження на службу технічної підтримки, так як не потрібно особистої присутності для рішення інцидентів. Всі процедури уніфіковані, стандартизовані й надійні. Один адміністратор може управляти 1000 і більше робочих місць.

– Саме робоче місце користувача теж змінюється й, в остаточному підсумку, перетворюється в тонкий клієнт, пристрій, що лише транслює зображення на монітор і не може зберігати яку-небудь інформацію на своїх дисках.

– Користувач може підключитися до свого віртуального робочого місця vdi з будь-якого тонкого клієнта, що перебуває в корпоративній мережі.

– Масштабування кількості робочих місць або філій відбувається в рази швидше.

– Це, звичайно, не все. Кожна компанія може знайти свої плюси від впровадження vdi.

Склад проекту VDI

Проект VDI «під ключ» – це програмно-апаратний комплекс, що складається із трьох основних елементів: устаткування, ліцензії, роботи з гарантійною підтримкою.

Склад устаткування, виробник програмного забезпечення для VDI можуть варіюватися залежно від переваг замовника, результатів тестування, корпоративних політик. Можна умовно розділити необхідне для проекту устаткування на серверні потужності, систему зберігання даних, мережа передачі даних.

Склад ліцензій залежить від необхідного замовникові функціонала, результатів тестування продуктів, набору вже наявних у замовника ліцензій. Для реалізації проекту VDI потрібні ліцензії двох типів: ліцензії на продукт VDI і ліцензії Microsoft.

Склад робіт із впровадження й подальшій технічній підтримці обговорюється із замовником і, по можливості, частину дій, які замовник може зробити самотужки залишається за ним.

Комбінації трьох елементів складаються в різні комерційні пропозиції (КП), які відрізняються друг від друга за ціною й функціональними можливостями.

Можливості VDI продуктів

Так як 30% вартості проекту VDI становлять ліцензії VDI, всім замовникам цікаво, чим саме друг від друга (крім ціни) відрізняються функціональні можливості продуктів і редакцій продуктів. На це питання єдино правильної відповіді немає. Але можна перелічити загальний функціонал, що є в сучасних продуктах VDI лідируючі позиції серед яких займають: VMware Horizon, Citrix XenDesktop, MS RDS. Про правила ліцензування кожного продукту буде розказано в окремих статтях, а поки подивимося, який загального функціонала містять у собі ліцензії VDI.

1. Центральна консоль керування всією інфраструктурою VDI, – через консоль ви створюєте віртуальні машини VDI з «золотого образа», через консоль установлюєте правила включення, вимикання ВМ. Тут адміністратор призначає робочі станції VDI, які будуть доступні користувачам і багато чого іншого.

2. Керування застосунками за допомогою шарів.

3. Можливість створення для користувачів наступних видів віртуальних робочих місць:

- виділена віртуальна машина, що не буде прив'язана до «золотого образа»;
- віртуальна машина з «золотого образа», з можливістю збереження інформації;
- організація доступу до фізичного комп'ютера (крім Microsoft);
- обнуляєма після виходу віртуальна машини з «золотого образа»;
- віртуальна машина зі збереженням змін.

4. Керування профілями користувачів, відділення даних від операційної системи. Користувачі з однієї групи одержують доступ до однакових віртуальних машин, але після входу користувача в сесію відбувається персоналізація. Завантажується профіль користувача, підключаються переспрямовані папки й мережні диски, підключаються мережні й локальні принтери, стають доступними для запуску пакетованого застосунка. Базовий функціонал надає Microsoft в Roaming Profile, більше розширений в VMware – Persona management, і в Citrix – Profile management.

5. Убудовані механізми підключення користувачам принтерів.

6. Існують клієнти для доступу до VDI для операційних систем: Windows, Linux, iOS, Android і через браузер з підтримкою HTML5 (крім Microsoft).

7. Підтримка роботи в локальній мережі LAN, і віддалений доступ WAN.

8. Підтримка аудіо й відеоконференцій в Microsoft Lync, Skype, Cisco, приблизно, з однаковим набором обмежень.

9. Можливість роботи USB накопичувачами, підтримка смарт карт, ключів E-token.

10. Проброс у сесію локальних дисків пристрою, з якого відбувається підключення для обміну файлами.

11. Підтримка локально підключених сканерів, принтерів і інших USB пристроїв.

Різниця, як завжди, криється в дріб'язках, інновація нових версій і саме вони в проектах часто схиляє чашу вибору убік того або іншого виробника. Досить, складно складе таблицю порівняння, із вказівкою параметрів, що розрізняються, продуктів, так як вона занадто швидко застаріє з виходом нових версій, update-тів, патчів.

У цілому, технологія VDI зараз розвилася до дуже високого рівня й, якщо говорити про прості офісні комп'ютери, які не виконують специфічних завдань, то переводити їх у віртуальне середовище можна не побоюючись за результат. Звичайно, якщо робити проект відповідно до рекомендацій виробників. Для заміни комп'ютерів, що використовують 3D графіку потрібне тестування й усвідомлений вибір.

Обґрунтування проекту VDI

Найважливішу роль у проекті VDI грає керівник IT відділу замовника, що повинен довести бізнесу (своєму керівництву), що цей проект для бізнесу буде корисний в економічному плані. Для порівняння поточних витрат на зміст парку ПК і, як альтернативи, проекту VDI складається таблиця техніко-економічного обґрунтування. У неї максимально докладно вносяться по категоріях всі існуючі капітальні й операційні витрати, після чого можна зрівняти два вектори розвитку.

У спрощеному варіанті всі розрахунки зводяться до вартості робочого місця в рік. Ціна одного робочого місця ПК зараз становить 900$ доларів у рік, а витрати на робоче місце VDI складуть 800$.

Нижче буде наведений простий розрахунок, що покаже із чого складається вартість робочого місця VDI і як вона виглядає в порівнянні з вартістю звичайного ПК. У розрахунки заставляються витрати компанії на електроенергію, обслуговування, хоча це, безсумнівно, могло б зіграти на руку VDI, але й створити ґрунт для непотрібної дискусії, так як у всіх ці витрати різні.

Отже, вартість робочого місця VDI складається із серверного устаткування, системи зберігання даних і мережі зберігання даних, ліцензій на VDI, ліцензій на Microsoft і вартості тонкого клієнта. Уже після основних витрат щороку потрібно оплачувати технічну підтримку з підпискою або тільки підпискою, щоб мати можливість обновлятися.

Для VMware і Citrix вважалася архітектура, коли файли віртуальних машин зберігаються на локальних SSD дисках, а для Microsoft RDS, що не вміє так працювати, архітектуру зі зберіганням файлів на SSD дисках системи зберігання, тому вона вийшла дорожче. Я не привожу тут докладні розрахунки, щоб не захаращувати текст.

У перший рік, незважаючи ні на що, нижче всього виявляється вартість VDI від Microsoft , потім іде Citrix, а VMware через високу ціну на ліцензії й технічну підтримку виявляється найдорожчим. Різниця в ціні між варіантом покупки ліцензії Windows server Datacenter і варіантом придбання річної підписки MS VDA мінімальна, але на другому році використання ліцензії не зажадають додаткових вкладень, а підписку прийдеться продовжувати.

Щороку потрібно буде оплачувати підписки, усього виходить 5 варіантів для VDI і один простій для персональних комп'ютерів, які до кінця п'ятого року потрібно буде замінити. Найменше вкладень зажадає Citrix у варіанті з Windows server Datacenter, так як передплата на ліцензії Citrix коштує мізерно мало (у порівнянні з конкурентами), а серверні ліцензії не вимагають вкладень. VMware у варіанті з VDA найдорожче зв'язування через сполучення високої вартості технічної підтримки VMware і високої вартості підписки MS VDA.

Переваги й недоліки

Напевно, не варто говорити, що у всього є свої переваги й недоліки. Такі є й у технології віртуалізації робочих місць. Щоб зрозуміти, чи потрібна вона вам, потрібно розуміти переваги й недоліки цієї технології. Багато про що вужі було написано в цій статті, але спробуємо узагальнити.

До переваг технології можна віднести:

– Віртуальні декстопи набагато безпечніші, ніж фізичні. Дані зберігаються в дата-центрі – їх набагато складніше украсти або ушкодити. Дата-Центр апріорі краще захищений, чим робоче місце співробітника. Тут і фізична охорона, і резервне копіювання, і можливість у будь-який момент заблокувати певне робоче місце, якщо на ньому замічена підозріла активність.

– Простота керування – віртуальними комп'ютерами простіше управляти, чим звичайними.

– Економія засобів – простота керування знижує витрати на адміністрування комп'ютерного парку. Тим більше, що тепер не потрібно витрачатися на заміну компонентів звичайних комп'ютерів, які періодично виходять із ладу.

– Скорочення часу простою – віртуалізація дозволяє скоротити час простою при збої до мінімуму. У випадку з фізичними ПК необхідно час на покупку (вибір, оплата, доставка) і заміну комплектуючих. Типовий приклад – вихід з ладу жорсткого диска локального ПК. Жорсткі диски настільних комп'ютерів, на жаль, не так надійні, як нам би цього хотілося й через 3 роки збільшується ймовірність їхнього виходу з ладу. Скільки часу знадобиться на усунення збоїти? Покупка нового диска, переустановка операційної системи, відновлення даних з резервної копії – мінімум полудня або хоча б півтора-друга година, якщо жорсткий диск був у наявності. Відновлення ВМ зі снапшота – справа декількох хвилин. От і вся різниця.

Тепер про недоліки. Найбільший недолік віртуалізації робочих столів – необхідність серйозних вкладень. Тут діє правило: якщо хочеш гроші заощадити, спочатку прийде їх витратити. Хоча знов-таки багато чого залежить від поставлених цілей і розв'язуваних завдань. Якщо ви – починаюча компанія, який потрібні потужні комп'ютери і якої не хочеться (чи ні можливості) витрачатися на їхнє придбання (ще не зрозуміло – піде чи справа ні), тоді доцільно орендувати VDI і серйозних вкладень не буде. А зекономлені засоби можна смів витратити на рекламу своєї компанії – так буде вигідніше.

Зовсім інша справа, якщо ви – велика компанія, що бажає забезпечити безпека своїх даних (зберігання яких ви навряд чи довірите сторонньому дата-центру) і скоротити витрати на IT, тоді прийде інвестувати серйозні засоби – вам знадобиться потужне "залізо", система зберігання даних, а також програмне забезпечення віртуалізації. Звичайно, можна використовувати й гібридну схему – наприклад, використовувати орендовані VDI для певних співробітників (співробітники call-центра, наприклад), що дозволить заощадити гроші на покупку комп'ютерних систем і їхню модернізацію, але половинчасті рішення для великого бізнесу не дуже привабливі, тому або прийде витратитися або VDI вам не підходить.

Якщо плануєте створювати інфраструктуру віртуалізації самотужки, зверніть увагу на вже готові системи. Застосування таких систем допоможе заощадити час, а в перспективі – гроші. Прикладом таких систем можуть бути HPE Apollo Systems, PureFlex System і деякі інші. Крім серверної системи ще знадобиться система зберігання даних. Можемо порекомендувати рішення HPE 3PAR, Dell EMC XtremIO, Fujitsu AF250 S2.

Vdi на базі hci

Як же підвищити ефективність впровадження VDI? Останні п'ять років ряд вендорів пропонують для цього так звані гіперконверговані комплекси (HyperConverged Appliance або HyperConverged Infrastructure, HCI), які просуваються як альтернатива класичному набору з інтегрованих між собою серверів і системи зберігання. Це рішення часто використовується для розгортання інфраструктури віртуальних десктопів.

Гіперконвергентна інфраструктура являє собою об'єднані в кластер стієчні або модульні сервери, на базі яких розгорнуте програмно-визначаєме сховище (Software Defined Storage, SDS). Замість окремого дискового масиву за допомогою спеціального програмного забезпечення SDS реалізується віртуальне дискове сховище, що складається із внутрішніх дисків серверів HCI. Відмова від використання окремого дискового масиву дозволяє істотно знизити вартість як зберігання даних, так і всієї апаратної платформи, що застосовується для впровадження VDI.

Крім того, гіперконвергентний комплекс – це повністю готовий до роботи інтегрований продукт, що набагато простіше встановити, настроїти й обслуговувати, чим набір серверів і СЗД. Тому він краще підходить для проектів впровадження VDI у невеликих організаціях і віддалених філіях компаній, де немає свого IT-фахівця з обслуговування серверного устаткування.

Ще одна перевага гіперконвергентного підходу – масштабування. Покупець може приступитися до реалізації пиіотного проекту впровадження VDI з розгортання гіперконвергентного комплексу в мінімальній конфігурації (звичайно три або чотири вузли), а потім – у міру збільшення в компанії числа віртуальних робочих столів – докуповувати

вузли й приєднувати їх до інфраструктури, нарощуючи процесорні потужності і ємність програмно-визначаємого сховища апаратної платформи VDI.

Як упоратися з boot storm

Для ефективної підтримки віртуальних десктопів система зберігання даних у гіперконвергентній інфраструктурі повинна демонструвати високі показники продуктивності уведення-виводу (Input/Output Per Second, IOPS) на рівні дорогих дискових масивів середнього або старшого класу. Справа в тому, що при використанні в організації віртуальних десктопів більшість із них активуються користувачами майже одночасно на початку робочого дня, і для кожного екземпляра виконується зчитування даних його операційної системи й застосунків, які централізовано розміщаються на системі зберігання, що обслуговує VDI (такий процес одержав назву boot storm).

Коли мова йде про десятки, сотні й навіть тисячі віртуальних робочих столів, необхідно виконати це зчитування максимально швидко, інакше користувачам щодня ранком прийде довго чекати, поки їхнє робоче місце буде готово до роботи. Крім того, навантаження на СЗД, що обслуговує інфраструктуру VDI, різко зростає під час сканування всіх віртуальних десктопів на віруси й установки відновлень або заплаток операційної системи й прикладного ПЗ, які в багатьох організаціях виконуються щодня (правда, в останньому випадку основне навантаження пов'язана з операціями не читання, а запису).

Застосування накопичувачів на основі флеш-пам'яті як в окремому дисковому масиві, що обслуговує VDI, так і в гіперконвергентних комплексах дозволяє істотно підвищити показники IOPS для системи зберігання й ефективно вирішити проблему boot storm. Коли для розміщення образів використовуються флеш-накопичувачі, завантаження навіть декількох сотень віртуальних робочих столів займає всього кілька секунд, а на підготовку робочого місця користувача йде менше часу, чим у випадку стандартних настільних ПК.

Крім того, технології SDS у сполученні із флеш-пам'яттю забезпечують істотне зниження часу доступу до даних, розташованим на іншому сервері (вузлі) інфраструктури, тому по швидкості читання даних програмно-визначаєме сховище на базі флеш-накопичувачів не уступає традиційному дисковому масиву з окремим RAID-контролером.

Розробка структурної схеми

Що являє собою гіперконвергентна інфраструктура?

Гіперконвергентна інфраструктура (HCI) поєднує обчислювальні, мережні ресурси й ресурси зберігання в єдину систему. Це оптимізоване рішення на базі ПЗ й серверів x86 заміняє спеціалізоване устаткування. Гіперконвергентна інфраструктура дає можливість спростити середовище ЦОД і поліпшити його масштабованість.

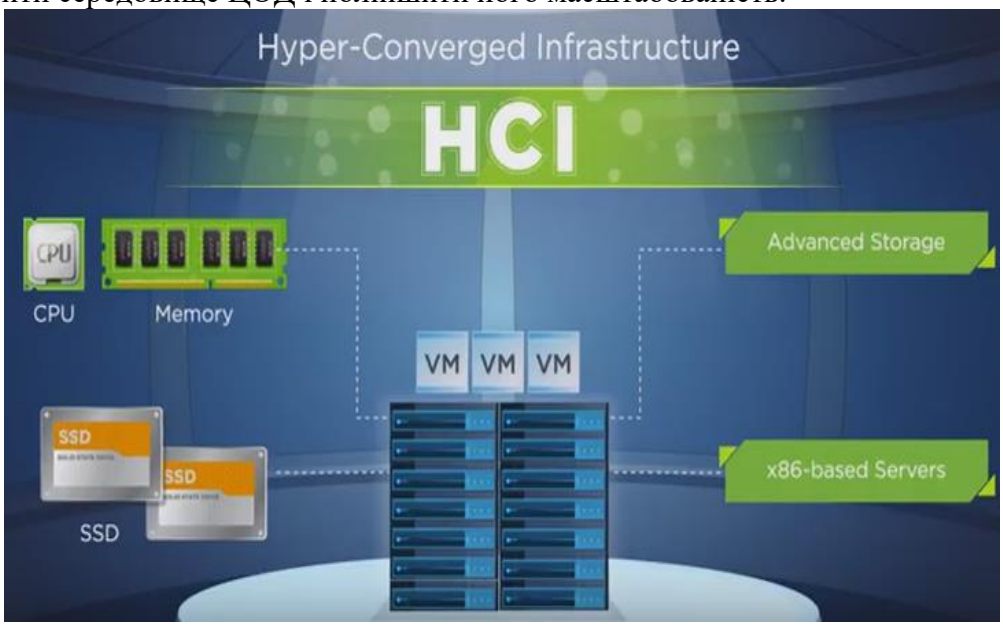


Рисунок 1 – Структурна схема системи

Традиційна трирівнева архітектура вимагає більших витрат на створення, складна в експлуатації й масштабуванні. Не потрібно чекати, поки IT-інфраструктура зможе підтримувати потреби застосунків. Розгорніть гіперконвергентну інфраструктуру без втрати контролю, підвищення витрат і зниження рівня безпеки.

Принцип роботи гіперконвергентної інфраструктури:

– Всі важливі процеси ЦОД виконуються на тісно інтегрованому програмному рівні, а не на спеціалізованому устаткуванні.

– Гіперконвергентна платформа складається із трьох програмних компонентів: засобів віртуалізації сховища, засобів віртуалізації обчислювальних ресурсів і системи керування.

– ПЗ для віртуалізації абстрагує й поєднує в пули базові ресурси, а потім динамічно виділяє їхнім застосункам, які виконуються у ВМ або контейнерах.

– Конфігурація визначається політиками, які враховують потреби застосунків, що усуває необхідність у використанні таких складних об'єктів, як дискові й логічні томи.

– Розширені можливості керування скорочують число завдань, виконуваних вручну, і допомагають повністю автоматизувати експлуатацію.

Розходження між гіперконвергентною й конвергентною інфраструктурою

Гіперконвергентні й конвергентні IT-інфраструктури поєднують чотири компоненти ЦОД. При цьому гіперконвергентні системи роблять це за допомогою програмного забезпечення (тому вони не мають прив'язки до певного устаткування), а конвергентні рішення залежать від устаткування. Для створення конвергентної інфраструктури ЦОД використовуються в основному ті ж продукти, що й у традиційної IT-середовищу, тільки зі спрощеною архітектурою й оптимізованим керуванням.

Переваги гіперконвергентної інфраструктури перед традиційної трирівневою архітектурою

Спрощення експлуатації

Усунете процеси, виконувані вручну, і необхідність у розрізнених групах фахівців для керування різними процесами експлуатації. Один об'єднаний IT-відділ може виконувати моніторинг обчислювальних ресурсів і сховища й управляти ними, завдяки чому забезпечується економія часу співробітників.

Скорочення витрат

Скоротите капітальні витрати завдяки використанню горизонтально й вертикально масштабованої архітектури на базі стандартних серверів x86 і економічних спеціалізованих мереж. Надалі можна додавати ресурси в міру необхідності без переривання процесів.

Підвищена адаптивність

Прискорте реагування на швидко мінливі потреби бізнесу. Устаткування можна запустити за кілька годин, а робітники навантаження ініціалізуються за кілька хвилин. Підвищте продуктивність важливих застосунків, наприклад реляційних баз даних.

Впровадження гіперконвергентної інфраструктури: три фактори, які варто врахувати

Переваги гіперконвергентної інфраструктури

Гіперконвергентна інфраструктура допомагає усунути розрізненість, характерну для традиційної IT-середовища, і реалізувати комплексне керування за допомогою єдиного засобу, завдяки чому можна знизити операційні й капітальні витрати, пов'язані з IT-інфраструктурою, без збитку для безпеки, гнучкості або масштабованості.

Яким образом рішення інтегрується з існуючим середовищем?

Для реалізації максимальних переваг і наступного переходу до повністю програмно-визначаємого ЦОД гіперконвергентна інфраструктура не повинна бути прив'язана до конкретної апаратної платформи. Гіперконвергентна інфраструктура VMware надає максимальну волю вибору й гнучкість, завдяки чому можна вибрати кращу платформу, забезпечити повну інтеграцію з наявною інфраструктурою, а також зберегти й оптимізувати існуючі технології.

Чи надає рішення можливість ефективно й економично збільшувати обсяг ресурсів у міру необхідності в зручний час, у будь-якому місці й зручному способі?

Масштабування ЦОД може бути дорогим і складним процесом. Гіперконвергентна інфраструктура VMware забезпечує масштабованість і зручність, допомагаючи прискорити реагування на швидко мінливі потреби бізнесу. На даний момент VMware – це єдиний постачальник, що пропонує повний набір продуктів для створення повністю програмно-визначаємого ЦОД у виробничому середовищі. Завдяки цьому забезпечується адаптивність для розгортання застосунків, стандартизації IT-рішень у різних середовищах і підготовки IT-середовища до використання загальнодоступних хмар.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віртуалізованої серверної інфраструктури на базі HCI. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем віртуалізованої серверної інфраструктури на базі HCI. Досліджена система віртуалізованої серверної інфраструктури на базі HCI. На основі отриманих результатів досліджень створена програмна реалізація системи віртуалізованої серверної інфраструктури на базі HCI. Розроблені алгоритми дозволяють успішно вирішувати завдання віртуалізованої серверної інфраструктури на базі HCI. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Мохамад Гани Абу Таам Разработка математической gert-модели технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / А.А.Смирнов, Мохамад Гани Абу Таам // Информационные системы в управлении, образовании, промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 498 с.
2. Мохамад Гани Абу Таам метод управления доступом в интеллектуальных узлах коммутации / Мохамад Гани Абу Таам, А.А.Смирнов // Информационные технологии и защита информации в информационно-коммуникационных системах: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – 486 с.
3. Мохамад Гани Абу Таам Математическая gert-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.
4. Мохамад Гани Абу Таам структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Гани Абу Таам // Системи управління, навігації та зв'язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120-125.
5. Мохамад Гани Абу Таам Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Гани Абу Таам, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 9(125). – Х.: ХУПС – 2014. – С. 105-110.
6. Мохамад Гани Абу Таам Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 4 (41). – Харків: ХУПС. – 2014. – С. 48-52.
7. Мохамад Гани Абу Таам Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Харків: ХУПС. – 2014. – С.90-95.
8. Мохамад Гани Абу Таам Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС – 2015. – С. 150-153.
9. Мохамад Гани Абу Таам Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – Випуск 3(43) – Х.: ХУПС – 2015. – С. 100-107.
10. Мохамад Гани Абу Таам Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Гани Абу Таам, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 3(19). – Х.: ХУПС. – 2015. –

С. 134-141.

УДК 004

О. Гирба, магістр гр. КІ-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОБРОБКИ НАВІГАЦІЙНИХ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено для системи обробки навігаційних даних. Метою розробки є дослідження та програмна реалізація системи обробки навігаційних даних. Об'єктом дослідження є процес обробки навігаційних даних. Предметом дослідження є методи обробки навігаційних даних. Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи обробки навігаційних даних. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, навігаційні дані

Постановка проблеми. Одним із сучасних досягнень науково-технічного прогресу є розробка системи GPS, за допомогою якої мандрівник може визначати свої координати, а пілот посадити літак у зоні з нульовою видимістю. У найближче десятиліття можливості глобальної системи позиціонування значно розширяться [1]. Можливості системи глобального позиціонування в найближчі 10 років стануть набагато ширше. Користувач зможе визначати свої координати з точністю до метра. Можливості системи GPS будуть розширюватися за рахунок модернізації, що припускає: введення додаткових каналів сигналу на супутнику, збільшення потужності сигналу й удосконалення системи його корекції, використання спрямованих антен, а також інтеграцію з телевізійними й телефонними стільниковими мережами [1-5]. За допомогою GPS літаки зможуть приземлятися в повній темряві. Система зможе відслідковувати місцезнаходження повітряних судів на всьому протязі польоту. Найближчим часом GPS допоможе контролювати рух автомобільного транспорту, забезпечуючи безпеку дорожнього руху, удосконалена система зможе бути застосована в електроенергетиці, у телекомунікаціях, при видобутку корисних копалин, картографії й навіть у сільському господарстві. Крім того, будь-який мандрівник зможе скористатися GPS на всій території земної кулі [2-5]. Якщо провести огляд сучасних систем GPS, то ми побачимо, що провідні світові держави мають свої супутникові системи, які забезпечують роботу приймача GPS. У США це система Navstar, у Європейському Союзі – Galileo [6-8]. В зв'язку з тим, що Україна поки не розвертає свою систему супутників для реалізації системи GPS, то актуальним буде розробка вітчизняного програмного забезпечення даної системи.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи обробки навігаційних даних.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи обробки навігаційних даних.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем обробки навігаційних даних.
– Дослідження системи обробки навігаційних даних.
– Програмна реалізація системи обробки навігаційних даних.

Об'єктом дослідження є процес обробки навігаційних даних.

Предметом дослідження є методи обробки навігаційних даних.

Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу

Сполучення мобільних пристроїв з GPS

На даний момент існує, як мінімум, три найбільш затребувані способи спільного використання GPS і КПК.

По-перше, до наладоника можна докупити опціональний модуль. Останній може помітно розрізнятися по способу сполучення, але в основному найбільш популярні зараз карткова модифікація й Bluetooth-варіант. Перший не дуже зручний через те, що займає один або єдиний слот розширення, зате відносно дешевий, ну а другий цілком ергономічний – не прийдеться піклуватися про точне позиціонування, от тільки ціна його, як правило, досить висока.

Другим способом є збагатити наладонник GPS-функціями при їхній відсутності в штаті, це є з'єднання звичайного навігатора й КПК за допомогою спеціального кабелю. Подібний варіант гарний своєю роздільністю й повноцінністю GPS-частини: при відсутності потреби в КПК можна відправлятися в дорогу лише з навігатором, не обтяжуючи себе додатковою ношею.

Ну й по-третє, існує можливість сполучити обоє пристрої в одному корпусі, одержавши КПК із інтегрованим модулем GPS. Пристрій значно мобільніший багатьох персональних GPS-навігаторів. При цьому кишенькові комп'ютери мають відмінний кольоровий екран, про яке спеціалізовані приймачі можуть тільки мріяти. Дисплеям наладоників властива чутливість до натискань, більш по мірках навігаторів розміри, порівняно високий дозвіл, багата палітра кольорів і т.д. Загалом, звичайні приймачі програють по всіх статтях, будучи оснащені несенсорним, часто монохромним екраном зі скромними характеристиками й досить високою інертністю.

Зовнішністю КПК, як правило, наділені більш привабливою, ніж навігатори. Правда, у подорожі це навряд чи придасться, а от відсутність у корпусів наладоників водонепроникності, а також їхні слабкі характеристики до фізичних навантажень досить недоречні.

Функціональність GPS-приймача – одна з основних якостей подібних пристроїв, оскільки в подорожі дизайнерські ізиски ніхто не оцінить, та й ергономіка відійде на другий план. Тому спеціалізовані пристрої настільки популярні: вони націлені виробником на навігацію, а тому мають весь базис необхідних функцій. Окремо завантажуються карти, але останнім часом багато продавців стали комплектувати навігатори подібними бонусами штатно. Як же обстоять справи із цим у КПК. Майже навпаки. Справа в тому, що наладоники – багатофункціональні пристрої, і “заточувати” їх під якесь певне завдання було б украй недоцільно. Ще більш мрячна перспектива вкласти в софтверну частину КПК весь його потенціал: навіть за умови використання карти пам'яті це навряд чи здійсненно й майже ніколи не потрібно, оскільки кожний купує КПК для своїх власних потреб. Через це GPS-здатності КПК звичайно не забезпечені програмним комплектом. Як правило, користувачеві доводиться самому вишукувати потрібне.

Якщо розглядати апаратну половинку КПК із GPS і персонального навігатора, то базових розходжень тут мало – звичайно приймачі так само, як і КПК мають 12-ти канальність і підтримку WAAS, а також інші основні характеристиками. Зате опціональності в наладоників відсутні. Ще одна перевага КПК з інтегрованим навігаційним модулем перед звичайними GPS-приймачами – наявність слота розширення, а точніше, підтримка SDIO, тобто здатність працювати з периферією. Подібний дріб'язок додасть наладонику функціональності, оскільки дозволить взяти в подорож, скажемо, камеру, Bluetooth-адаптер або GSM-модуль, а також багато чого іншого – на сьогоднішній день спектр доступного устаткування досить великий, і кожний зможе вибрати щось цікаве й корисне конкретно для себе. GPS-навігатори, як правило, позбавлені подібної можливості, а роздільні набори GPS і

КПК не занадто зручні, оскільки далеко не всі наладоники оснащені двома слотами розширення.

Розрахунок часу старту GPS навігатора

Час «старту» необхідний навігаційному приймачу на визначення позиції після включення, залежить від наявної в пам'яті початкової інформації. Виділяються наступні режими:

- «Холодний» старт («автопошук») – час, позиція, альманах і ефемериди невідомі
- «Теплий» старт – позиція й ефемериди невідомі, час і альманах відомі
- «Гарячий» старт («перезахват») – альманах, ефемериди відомі, час і позиція відомі з деякою помилкою

Навігаційні повідомлення передані із супутників містять два типи даних – ефемериди й альманах супутників. В альманасі передаються параметри орбіти, за допомогою яких можна обчислити зразкове місце розташування супутників з достатньо великим ступенем погрішності. Альманах, що зберігається в пам'яті приймача, постійно обновляється, тому що кожний супутник передає дані альманаху для всіх супутників угруповання. Час «життя» альманаху становить 2-3 місяці. Далі, величина накопиченої помилки в розрахунках буде неприпустимою.

Дані ефемерид містять параметри, що дозволяють більш точно обчислити поточне місце розташування супутників. На відміну від альманаху, кожний із супутників передає, тільки свої власні ефемериди. Час «життя» ефемерид не перевищує 4-6 годин.

Інформація даних ефемерид і альманаху, передана із супутників, постійно коректується. Це відбувається один раз у добу. Мережа наземних станцій, одержує інформацію із супутників, за аналогією зі звичайними користувачами, аналізує виміри, порівнює їх з опорними, розраховує коригувальні виправлення й передає їх на головну станцію, з якої здійснюється передача даних на супутники.

«Холодний» старт приймача може бути зв'язаний не тільки з його тривалою бездіяльністю, але переміщенням на велику відстань у виключеному стані. Якщо перший випадок пов'язаний із застарілим альманахом і помилкою у визначенні поточного точного часу, то в другому випадку приймач, не знаючи про своє переміщення, буде намагатися знайти супутники, яких повинні бути видимі на «старому» місці. Користувач може «допомогти» приймачу й зменшити час «холодного» старту, указавши на базовій карті, зразкове «нове» місце розташування. Під час «холодного» старту приймач сканує весь діапазон можливих значень частот і тимчасових затримок навігаційних сигналів. При цьому, у багатоканальных приймачах, кілька каналів можуть використовуватися для пошуку одного супутника, щоб прискорити час його захвата. Після того, як сигнал хоча б від одного супутника буде отриманий і розібраний, приймач буде мати повну інформацію про альманах всього угруповання й, по суті, перейде до «теплого» старту

При «теплому» старті, приймач, включений після 6-і годин бездіяльності, почне «пошук» сигналів супутників, використовуючи значення поточного часу й дані, що зберігаються в пам'яті, альманаху. Буде здійснюватися пошук тільки тих супутників, які, по теоретичних розрахунках перебувають у видимій півкулі й повинні бути доступні приймачу. Відповідно, відомий досить вузький діапазон частот і часових затримок, що потрібно просканувати у процесі пошуку сигналів. Ця інформація істотно прискорює час захвата супутників, у порівнянні з «холодним» стартом, коли пошук ведеться на широкому діапазоні всіх можливих значень затримок і частот

Варто відзначити, що в момент включення, багатоканального приймача починає пошук сигналів з декількох супутників одночасно. Інформація передана із супутників прив'язана до єдиної шкали часу, містить однакову структуру й досягає антени приймача, приблизно в один й той же час. Тому дані ефемерид, одночасно захоплених супутників, надійдуть у приймач майже що одночасно. Якщо кількість таких супутників більше або рівняється трьом, то це дозволяє приймачу відразу ж розрахувати позицію. У випадку, коли

сигнали блокуються перешкодами, то може знадобитися досить тривалий час на визначення позиції.

Наявність повністю отриманих ефемерид, не гарантує використання цього супутника у підрахунку позиції. Інформація передана в ефемеридах може бути неправильною, помилковою, або пов'язаною з несправністю в роботі супутника. Це може бути зв'язано не тільки з несправністю супутника, але й діагностичними роботами проведеними на його борті, процесом уведення його в експлуатацію або тестуванням нових режимів.

«Гарячий» старт пов'язаний з короткочасним вимиканням приймача (до 6-і годин) не вимагає тривалого часу на визначення позиції. Це пояснюється тим, що отримані раніше ефемериди містять «свіжі» дані, використовувані для визначення точних координат супутників і можуть використовувати в обчисленні позиції. У випадку включення приладу після граничного часу, ефемериди розглядаються застарілими й починає діяти принцип «теплого» старту. Якщо на момент включення приймача видимими залишилися менш 3-х супутників з «свіжими» ефемеридами, то для визначення позиції буде потрібно якийсь час на збір даних ефемерид нового супутника.

Дані ефемерид передаються в складі трьох пакетів. Кожний з пакетів містить однаковий часовий ідентифікатор (IOD – issue of data) по якому можна об'єднати загальну інформацію. Інформація ефемерид передана із супутників кожні 30 секунд, змінюється раз в 2 години, і містить однаковий на цей час IOD. Якщо один з пакетів був пропущений, або отриманий з помилками, то можна виділити аналогічний пакет з наступного повідомлення, перевірити його ідентифікатор і не чекаючи наступних пакетів, використовувати його з раніше отриманими. Це дозволяє приймачу прискорити час «старту».

Існує мінімальний можливий час, необхідний приймачу на «старт», і це визначається структурою переданого сигналу із супутників. Виробники навігаційної апаратури, використовуючи стандартні методи навігації, можуть наблизитися до цього часу, але зменшити його не зможуть. Одним з методів, призначених для рішення цієї проблеми, є Assisted-GPS (A-GPS). Його принцип полягає в обчислення точного місця розташування супутників без інформації ефемерид, на одержанні яких потрібен час. Обчислення здійснюється на використанні точних моделей орбіт супутників, доступних через спеціальні Інтернет – сервіси.

З іншого боку, максимальний час «старту» може значно перевищувати заявлене в технічній специфікації на навігатор час. Це пояснюється навколишніми умовами, у яких відбувається «захват» супутників і «старт» приймача. Якщо приймач перебуває в умовах сильних фізичних перешкод, то навігаційний сигнал піддається зовнішньому впливу, містить помилки й неправильно декодується. Більше, того геометричний фактор цих супутників, що є одним із критеріїв точно визначення позиції, сильно погіршується. Всі ці умови можуть значно збільшити час «старту» приймача.

Обчислення радіуса окружності помилки для оцінки точності GPS-вимірів

Показник CEP – окружність можливої помилки (Circular Error of Probability) один з можливих шляхів оцінити точність вироблених GPS вимірів у даній точці тепер. Завдяки великій кількості факторів зовнішнього середовища впливаючих на виміри – в одній точці показання приладу будуть різними в різні моменти часу. До таких факторів відносяться вплив іоносфери, вплив нижніх шарів атмосфери, багатопроменевість, наявність перешкод на шляху сигналу. Показник CEP використовує опорну точку, або задаваєму користувачем, або що обчислюється як середнє геометричне між всіма вимірами, для того, щоб побудувати серію окружностей що показують відповідно 50, 90, 95, 99% можливої помилки.

Для того, щоб визначити CEP повинна бути взята серія вимірів зроблена в одній точці. Наприклад, включений і нерухливий GPS з інтервалом в 2-5 сік реєструє точки треку, які потім завантажуються, конвертуються в shape-файл і аналізуються.

Очевидна регулярність розташування точок пов'язана з розрішенням цифрових значень видаваних GPS. Наприклад точність із якої GPS Garmin 12 видає координати – 0.000005 десяткових градусів по довготі, і 0.000005 по широті.

Для обчислення CEP дані повинні бути спроектовані. Для обчислення виміряються відстані між середньою точкою й кожним виміром, а потім вираховується на якій відстані перебуває потрібний відсоток точок.

Рисунок 1а

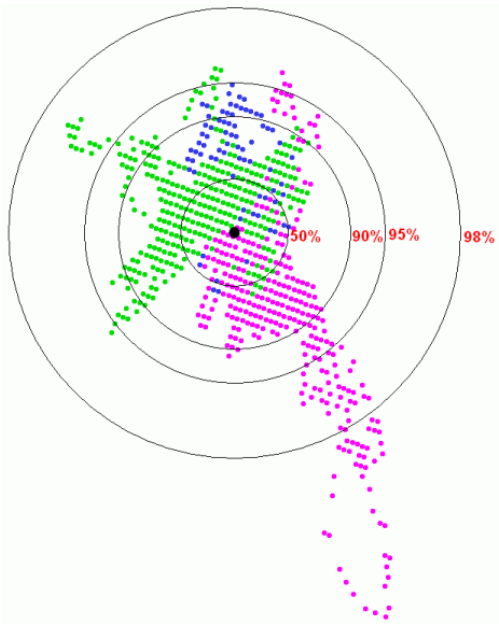


Рисунок 1б

Рисунок 1а – Показання 3-х 40-хвилинних сесій прийому координат, по 1022 виміри через 2 сек у сесії (усього 3066 вимірів).

Рисунок 1б – Обчислені значення CEP (50, 90, 95, 98), щодо середнього значення (чорна точка в центрі), графік являє собою візуальне подання обчислених значень CEP (різним кольором показані різні серії вимірів, усього 3 серії).

Результати обчислення CEP 4 різних окружностей: Average = 6.999e+006 5.82936e+006, SD = 7.00012e+006 5.83025e+006, Circular Error Probabilities (CEP), 50% = 42281, 90% = 7.36774, 95% = 9.52791, 98% = 14.2946.

Приклад показує, що 50% точок перебувають на відстані 4 метра від середнього значення, 98% точок на відстані 14.2 метра від середнього. З діаграми також видний розкид помилки.

Конвертування карт для завантаження в GPS

Іноді буває так, що карти, які хотілося б завантажити в GPS є у форматі від GPS далекому. Опишемо процес рішення тих самих проблем – як до них підходити взагалі, де чекати підводних каменів, і так далі.

Є векторна карта у форматі "ГІС ІНГЕО-4". Завдання, яке треба буде розв'язати, складається із двох великих частин. По-перше, необхідно вихідну базу даних перетворити в один з форматів так званого торованого ланцюжка перетворень. Інакше кажучи, необхідно невідому базу даних привести до того формату, з якого ми вже вміємо одержувати карту для GPS. По-друге, необхідно, щоб дані, наведені до потрібного формату, були коректні для GPS, – важливіше всього домогтися, щоб координати об'єктів, вивантажених з невідомої бази, були коректні й у відомій системі координат.

В "ГІС ІНГЕО-4" дані перетворяться в DXF-формат (autocad-овский) і в MIF-формат (MapInfo-шний формат обміну). Дані зберігаються в локальній декартовій системі координат, що якось потрібно перетворювати в систему координат, зрозумілу подальшим програмам технологічного ланцюжка.

Перетворення координат і експорт.

Перетворимо карту у формат Пулково-1942. Для початку необхідно прийняти кілька допущень. По-перше, припустити, що координати карти в "ГІС ІНГЕО-4" є прямокутні

декартові. По-друге, припустити, що вихідна карта ІНГЕО є зміщеною й розтягнутою, але не поверненою щодо координат Пулково-1942.

Виходячи із цих припущень і знання основ лінійної алгебри можна записати, як нові координати (Пулково-1942) обчислюються з бази ІНГЕО:

nx = xx * sx + dx ny = yy * sy + dy, (1)

де xx,yy – координати точки в базі ІНГЕО, sx,dx – відповідно, розтягання й зсув по осі x, а sy,dy – розтягання й зсув по осі y. Як видно, я припускаю, що спочатку до точок ІНГЕО потрібно застосувати розтягання, а потім зсув, щоб одержати Пулково-1942.

Для обчислення параметрів розтягання й зсувів, необхідно мати хоча б дві точки на карті, для яких ми знаємо й старі й нові координати. Загалом кажучи, точок потрібно як мінімум дві, можна більше, але не обов'язково чим більше тим краще. Справа в тому, що задаємочи дві точки, і обчислюючи по них параметри перетворення, ми домагаємося того, що ці дві точки будуть однозначно збігатися на місцевості й карті, – тобто в них прив'язка буде абсолютно точною. Погрішність прив'язки точок, що відстоять недалеко від двох точок прив'язки, буде невелика, але вона буде зростати при видаленні від них. Якщо прив'язувати карту по багатьом точкам, то неможливо буде знайти параметри перетворення, що абсолютно прив'язують всі ці точки, зате карта в цілому, можливо, буде прив'язана краще. Формули для обчислення параметрів прив'язки у випадку більше двох точок прив'язки можна виписати, наприклад, скориставшись будь-яким методом апроксимації лінійної функції – хоч методом найменших квадратів.

Отже, точка1 має координати на місцевості (nx1=439395, ny1=6072078), а в карті (xx1=3208.34, yy1=5030.94); а точка2 – (nx2=433902, ny2=6068556) на місцевості, і (xx2=-397.74, yy2=-427.93) у карті.

Помітимо із самого початку, що в Пулково перша координата задає зсув по горизонталі, а друга по вертикалі, а в ІНТЕГРО, як і в WGS84, навпаки. Тому щоб обчислити параметри перетворень коректно, необхідно поміняти місцями координати в карті. Тоді перша точка на карті буде мати координати (xx1=5030.94, yy1=3208.34), а друга (xx2=-427.93, yy2=-397.74);

Підставивши координати двох точок в (1) одержуємо систему рівнянь, з яких перебувають параметри перетворень у такий спосіб:

sx = (nx 1-nx2)/(xx 1-xx2)

dx = (nx2*xx 1-nx1*xx2)/(xx 1-xx2)

sy = (ny 1-ny2)/(yy 1-yy2)

dy = (ny2*yy 1-ny1*yy2)/(yy 1-yy2),

підставляючи куди наші координати одержуємо: sx = 1.0062522097064, dx = 434332.6055081, sy = 0.976683822876919, dy = 6068944.46622371

Тепер можна переходити до вивантаження об'єктів з ІНГЕО. Вибираємо там сервіс-експорт-MID/MIF. Вибираємо шари, які необхідно експортувати (наприклад, тільки вулиці), указуємо, куди експортувати, і на наступному вікні задаємо параметри трансформації координат. Задаємо перше перетворення: "збільшення-стиск", 1.0062522097064 по X і 0.976683822876919 по Y. Потім задаємо два послідовних перетворення, що приводять до того, що X і Y поміняються місцями (відбиття відносно прямій y=x): друге перетворення: "поворот" на 90 градусів, третє перетворення: "збільшення-стиск" на -1 по X і 1 по Y. І останнє перетворення: "зсув", 10434332.6055081 по X і 6068944.46622371 по Y. Цифри 10 я приписав до споконвічного зсуву по X, рівному 434332.6055081, для того, щоб формально привести використовувані координати до виду Пулково-1942, де, як відомо, до зсуву по X приписується ліворуч номер зони, що для України є 10 (центральний меридіан – 57). Натискаю OK і в обраній директорії зберігаються файли MID і MIF для кожного із шарів. Дані вивантажені.

Імпорт даних у відомий формат.

Всі вивантажені шари лежать у файлах MID і MIF. Для початку перейменую їх у коротких, мовців назви, якщо це ще не так. Далі конвертуємо MIF-MID-файли у формат SHP. Найкраще створити bat-файл, що запускає перекачування в SHP і внести в нього рядка типу:

mifshape.exe point streets streets_pt
mifshape.exe text streets streets_t
mifshape.exe line streets streets_l
mifshape.exe poly streets streets_p

(за умови, що експортовані файли streets.mif і streets.mid лежать у тім же каталозі, що й конвертер mifshape). Програма створювала по трьох файлу для кожного типу даних, які будуть скачані з MIF-формату: для точок, для тексту, для ліній, і для замкнутих полігонів.

Після завершення цього процесу, ми одержали набір SHP-файлів (із супутніми їм) для всіх даних, які ми хочемо бачити на карті. Якщо всі перетворення були виконані вірно, то координати в них більш-менш коректні. На цьому етапі, можна сказати, завершується робота по підготовці карти, специфічна для завдання; далі йдуть дії, виконувані по тому самому алгоритму при підготовці будь-якої карти, будь вона оцифрована або отримана яким-небудь іншим шляхом.

Підготовка карти для GPS

Коротко відзначимо ті проблеми, що відносяться саме до вивантаженої карти з невідомої бази даних.

Для кожного файлу програма спочатку запросить як відображати об'єкти даного файлу в GPS (чи це дороги, чи струмки, чи ще що), потім запропонує вибрати джерело для підписів до об'єктів, потім запросить використовувану систему координат. У наступному вікні можна вибрати, у які шари потрібно завантажувати карту (про шари як-небудь потім), і нажавши там на Finish, ми нарешті-те побачили результати своєї праці.

Або ж побачили зовсім не те що очікували. На жаль, пророчити, якого роду проблеми можуть виникнути, дуже складно.

Після того, як всі шари завантажені й карта вийшла в більш-менш пристойному вигляді, необхідно перевірити, наскільки добре вона прив'язалася. Як мінімум для цього потрібно перевірити які координати відображає програма для точок, по яких обчислювалося перетворення – вони повинні збігатися з реальною місцевістю. Як правило, є в наявності деяка погрішність прив'язки, і на цьому етапі її можна виправити. Для цього зручно завантажити якнайбільше точок і треків, і спробувати побачити, є чи деяка загальна тенденція в їхній помилці. Наприклад, якщо вони всі виявилися зрушені в одну сторону, то за допомогою інструмента Transform можна спробувати внести корекцію в карту. У цей інструмент може виконувати просто зрушення, що задається однією точкою (шляхом вказівки її старої й нової позицій); аффінне перетворення, що задається трьома точками й квадратичне перетворення, що задається шістьома точками. Найкраще спробувати виправити ситуацію за допомогою простого зрушення, а якщо це не вийшло, тоді вже намагатися застосовувати аффінне перетворення, попередньо зберігши карту в безпечне місце, через деяку непередбачуваність поводження об'єктів карти при такому складному перетворенні.

Завантаження карти в GPS

Після того як карта виходить прив'язаною із задовільною точністю, все інше виконується як з будь-якою іншою картою. А саме, настроюються властивості карти (її ID і NAME, обов'язково CODEPAGE – 1251, якщо ви хочете, щоб український текст відображався коректно), потім карта зберігається в форматі MP, і з тої ж програми викликається програма, що готовить файл IMG, заливається безпосередньо в GPS за допомогою розробленого програмного забезпечення або його візуального розширення img2gps.

Розробка структурної схеми

На рисунку 2 представлена структурна схема роботи системи. При розробці системного програмного забезпечення обробки навігаційних даних використовувалася

технологія GPS (Global Positioning System) – "Система глобального позиціонування" система визначення місця розташування об'єктів, заснована на використанні штучних супутників Землі (більш докладно розглянуто вище).

Розроблена програма є універсальною системою, що може використовуватися у всіх мобільних пристроях, підтримуючих систему навігації GPS і маючих віконний інтерфейс на основі операційної системи Windows.

Коли користувач набудовує й запускає розроблену програму, відбувається пошук штучних супутників Землі для визначення координат. Сучасні приймачі GPS вбудовані в мобільні пристрої одночасно можуть приймати дані з 12 супутників, що забезпечує високу точність позиціонування (50 – 100 метрів).

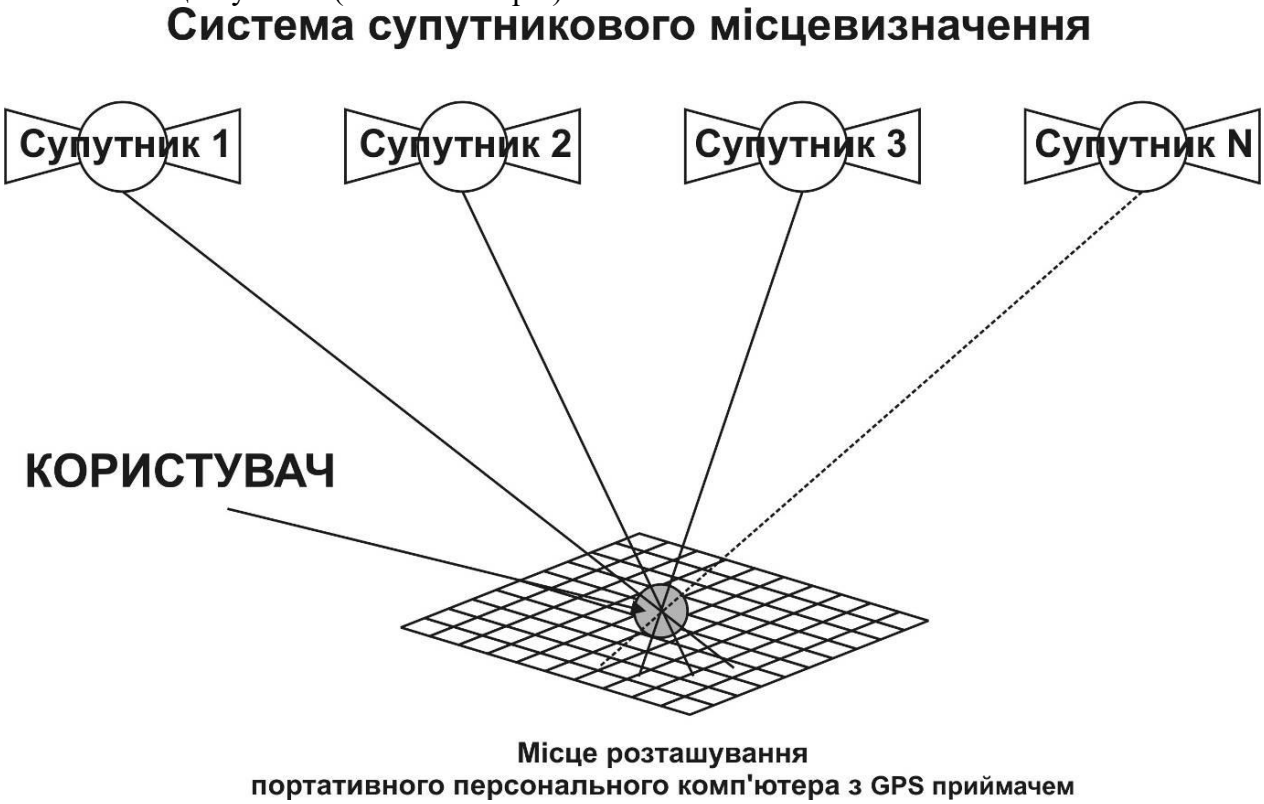


Рисунок 2 – Структурна схема роботи системи

На схемі представлена геопараметрична сітка з поточним місцем розташування об'єкта й система супутників, що забезпечує визначення місця розташування. При поганому зв'язку із супутниками (знаходження в приміщеннях) необхідно, принаймні 3 супутники, що знаходяться не на одній лінії для визначення поточного положення.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів обробки навігаційних даних. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем обробки навігаційних даних. Досліджена система обробки навігаційних даних. На основі отриманих результатів досліджень створена програмна реалізація системи обробки навігаційних даних. Розроблені алгоритми дозволяють успішно вирішувати завдання обробки навігаційних даних. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.

2. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
3. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
4. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
5. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
6. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
7. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.
8. Коваленко А.С. Експертна система технічного діагностування інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2015. – № 1(41). – С. 106-111.
9. Коваленко А.С. Удосконалення методу технічного обслуговування об’єктів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко, О.П. Доренський // Системи озброєння і військова техніка. – Х.: ХУПС, 2016. – № 2(46). – С. 109-114.
10. Коваленко А.С. Метод визначення оптимального комплексу робіт з відновлення працездатності інтегрованої системи технічної діагностики в умовах ресурсних обмежень / А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2016. – Вип. 3(140). – С. 69-72.

УДК 004

З. Азатьян, магістр гр. КН-20М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНО-ДІАГНОСТИЧНОЇ СИСТЕМИ ПОЇЗДУ

У статті розроблено програмне забезпечення, яке призначено для автоматизованої інформаційно-діагностичної системи поїзду. Метою розробки є дослідження та програмна реалізація автоматизованої інформаційно-діагностичної системи поїзду. Об’єктом дослідження є процес реалізації автоматизованої інформаційно-діагностичної системи поїзду. Предметом дослідження є методи реалізації автоматизованої інформаційно-діагностичної системи поїзду. Методи дослідження базуються на методах теорії автоматизованого управління, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація автоматизованої інформаційно-діагностичної системи поїзду. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерні науки, автоматизація, інформаційно-діагностична система

Постановка проблеми. Залізничний транспорт залишається найважливішою складовою частиною транспортної системи України, на його частку доводиться понад 40% пасажирообороту, виконуваного всіма видами суспільного транспорту. Відповідно до прогнозів розвитку народного господарства очікується ріст обсягу пасажирських перевезень. Тим часом, існуючий парк пасажирського рухливого состава багато в чому застарів.

З 1992 р. поставка пасажирських вагонів локомотивної тяги зменшилася до 300 вагонів у рік. У результаті парк вагонів скоротився майже в півтора разу, а його старіння йде значно швидше, ніж відновлення. Сьогодні зношування становить у середньому 50%. Значне число пасажирських вагонів уже виробили свій нормативний термін служби. У сучасний час із загального парку вигонів порядку 1500 вимагають списання по терміну служби [1]. Більше 7 тис. вагонів мають вік понад 20 років, вони застаріли фізично й морально, не відповідають сучасним вимогам перевезення пасажирів. Близько 80% вагонів не обладнані системами кондиціювання повітря, що значно знижує комфортність поїздок. Така ситуація диктує необхідність якнайшвидшого відновлення парку [1-5].

Підвищення ефективності роботи пасажирського комплексу залізниць України ставиться до числа найбільш відповідальних і актуальних завдань, що стоять перед галуззю. Важливу роль у їхньому рішенні покликана зіграти концепція Програми оновлення парку вагонів, яка розрахована до 2028 року.

Основні напрямки Комплексної програми, які повинні забезпечити її ефективність, можна сформулювати в такий спосіб [6]:

– збільшення коефіцієнта використання потужностей вагонних депо й зменшення їхньої кількості за рахунок концентрації потужностей у більш оснащені й, як наслідок, зменшення експлуатаційних витрат;

– визначення найбільш оснащених і ефективних ремонтних депо, їх дооснащення до рівня ремонтних заводів і виділення в дирекцію з ремонту рухливого состава;

– відновлення парку за рахунок поставки нового пасажирського рухливого состава й проведення комплексного ремонту із продовженням терміну служби;

– ліквідація до 2028 р. дефіциту парку пасажирського рухливого состава й виключення з експлуатації вагонів із простроченим терміном служби;

– розробка нової системи експлуатації, технічного обслуговування й ремонту пасажирських вагонів.

Старіння парку пасажирського рухливого состава значно ускладнило його технічний зміст. Це негативно позначається на безпеці руху й приводить до значного збільшення ремонтних витрат. Поліпшення показників безпеки на залізницях може бути досягнуте за рахунок модернізації морально застарілих і менш надійних вузлів вагонів з метою ліквідації відмов устаткування в шляху проходження, удосконалювання технологічного процесу ремонту й обслуговування пасажирських вагонів, впровадження більше сучасних і ефективних технологій, технічних засобів, що дозволяють знизити вплив «людського фактора».

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні інформаційно-діагностичної системи поїзду”

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація автоматизованої інформаційно-діагностичної системи поїзду.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем реалізації автоматизованої інформаційно-діагностичної системи поїзду.

– Дослідження автоматизованої інформаційно-діагностичної системи поїзду.

– Програмна реалізація автоматизованої інформаційно-діагностичної системи поїзду.

Об’єктом дослідження є процес реалізації автоматизованої інформаційно-діагностичної системи поїзду.

Предметом дослідження є методи реалізації автоматизованої інформаційно-діагностичної системи поїзду.

Методи дослідження базуються на методах теорії автоматизованого управління, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У промисловій автоматиці звичайно використовують стандарт 4-20 ма для передачі значень. Незважаючи на те, що складні розподілені системи управління грають усе більшу роль в автоматизації виробництва, зв'язок приладів з контролерами по колишньому виглядає як з'єднання " точка-точка". Однак в останні роки все більш широко поширюється концепція впровадження локального інтелекту в промислові прилади й забезпечення зв'язку між рівноправними вузлами мережі. Успіх цього підходу залежить від комунікаційної мережі, що зв'язує пристрої, розташовані на об'єктах управління. Недавно були розроблені кілька запатентованих мереж, широко відомих за назвою "системи fieldbus". Даний розділ присвячений поглибленому порівняльному вивчанню трьох перспективних протоколів fieldbus, а саме: Controller Area Network (CAN), Process Fieldbus (PROFIBUS) і Field Instrumentation Protocol (FIP). Досліджуються основні характеристики цих мереж (реакція в реальному масштабі часу, працездатність, придатність для управління процесом). Проведені дослідження показують, що Profibus і FIP – сильні суперники в приладовому оснащенні процесів управління. У той час, як в FIP реалізуються нові концепції, наприклад поділ пропускної здатності шини, шляхом виділення інтервалів часу при використанні синхронізованих тактових генераторів, Profibus ґрунтується на звичайній передачі маркера із циклічним інформаційним обслуговуванням для задоволення потреб у реальному часі. Вивчення витрат на впровадження показує, що протоколи Profibus можуть бути реалізовані з незначним додатковим устаткуванням, оскільки основна передача даних асинхрона й ведется посимвольно. Що стосується CAN, те вони прекрасно підходять там, де потрібно досить незначний час очікування (порядку 5 мс) і необхідно з'єднати велике число при малих витратах.

Мережа fieldbus зв'язує промислові прилади (сенсори, виконавчі механізми, пристрої вводу-виводу й локальні регулятори) на виробничому рівні. Вона має нові функції, такими, як автоматичне калібрування промислових приладів, самотестування, завантаження на згадку значень параметрів, конфігурування, діагностика в реальному часі, попереднє обчислення вимірюваних величин, моніторинг мережі й т.д. Подібні мережі знижують витрати на кабелі й поліпшують доступ до устаткування. У кожному разі fieldbus повинна забезпечувати виконання критичних вчасно операцій. Отже, інтелектуальні промислові прилади збільшують робоче навантаження fieldbus у міру зростання числа їхніх функцій.

Загальні вимоги до системи fieldbus

Fieldbus – це повністю цифрова двунаправлена багатоточкова комунікаційна система, використовувана для зв'язку приладів на об'єктах із системами в операторській. Одне із самих основних властивостей системи fieldbus полягає в тому, що вона підтримує двунаправлений зв'язок з безліччю змінних величин. Фізично в fieldbus можуть використовуватися три види топологій міжз’єднань: двухточкова, деревоподібна й багатоготочкова. Середнє число приладів, під’єднаних до мережі може коливатися від 50 до 200 при довжині мережі 100 – 1000 м. Крім фізичного з'єднання приладів мережа повинна забезпечувати виконання наступних функцій:

– взаємодія устаткування, що надійшло від різних виготовлювачів;

– просте додавання й видалення пристроїв;

– від'єднання пристрою для проведення ремонту й наступне його включення в мережу, при яких не створюються перешкоди для роботи інших пристроїв і користувальницького завдання, а також не виявляються впливи на динаміку всієї мережі;

– сигналізацію про те, що промисловий прилад вийшов з ладу або перебуває в ремонті;

– можливість перевірки всього комплексу устаткування із заданої точки або із всіх точок мережі;

– здатність визначати поточний стан будь-якого під’єднаного пристрою за допомогою спеціального пристрою мережі fieldbus;

– можливість пристроїв мережі fieldbus подавати запит на самоконтроль приладу, виявляти в мережі новий пристрій, подавати запит на ідентифікацію приладу;

– просту модифікацію процесу, фізичне додавання або видалення приладів при незначній модифікації користувальницького програмного забезпечення.

На користувальницькому рівні система fieldbus повинна володіти:

– можливістю пересилати циклічні й ацикличні дані;
– двома або чотирма рівнями пріоритетів для повідомлень;
– здатністю: зчитувати й записувати значення змінних у режимах " точка-точка", груповому або широкомовному;
– пускати в хід виконавчі пристрої;
– визначати поточний стан сенсорів і їхнього порушення;
– запам'ятовувати конфігурацію пристроїв;
– проводити точну ідентифікацію приладу;
– синхронізувати роботу двох станцій.

Кожна система fieldbus повинна, у такий спосіб підтримувати загальну Службу повідомлень fieldbus (FMS), щоб забезпечувати виконання перерахованих користувальницьких вимог. Специфікації fieldbus повинні підтримувати також тимчасово під'єднані пристрої. Горизонтальний інформаційний потік в fieldbus характеризується головним чином передачею коротких повідомлень у заданий час. Інтеграція fieldbus у глобальне середовище повинна бути можлива для вертикальних інформаційних потоків, спрямованих на диспетчерський рівень. Більша частина горизонтальних інформаційних потоків буде в основному циклічного типу із часом циклу довжиною 0,25..2 із із типовою довжиною 1..5 байт на одне присоединенное пристрій, із затримками в передачі повідомлень порядку 100 мс.

Система Profibus

Стандарт визначає необхідні функції, що дозволяють пересилати дані між пристроями, виготовленими різними виробниками. Фізичний рівень, рівень каналів передачі даних і управління системою fieldbus для обох рівнів визначені в стандарті DIN 19245-1. Специфікації повідомлень fieldbus (Fieldbus Message Specification- FMS), аналогічні Специфікаціям виробничих повідомлень (Manufacturing Message Specification MMS); інтерфейс нижнього рівня (Lower Layer Interface LLI) і управління системою fieldbus на сьомому рівні визначені в DIN 19245-2. Цей стандарт націлений на реалізацію протоколу за допомогою однієї комерційно доступної інтегральної схеми, що містить однокристальний мікроконтролер і внутрішній універсальний синхронний приймачепередатчик, що мінімізує вартість взаєбагато з'єднання пристроїв, розташованих на об'єктах. Мережа містить провідні й ведені станції. Провідна станція може управляти системою й передавати повідомлення, коли вона має право доступу (маркер). На відміну від її ведена станція може лише підтверджувати отримане повідомлення або пересилати інформацію з удаленному запиту. Маркер циркулює по логічному кільцю, утвореному провідними станціями. Таким чином, може бути реалізована або централізована система, або система, що повністю працює в режимі точка-точка , або гібридна. Швидкість передачі лежить у діапазоні від 9,6 Кбіт/с до 2 Мбіт/с. Для критичних вчасно завдань рекомендується система з 32 провідними станціями. Можлива як ациклічна, так і циклічна передача даних з 255 байтами в кадрі.

PROFIBUS-PA і FOUNDATION™ fieldbus мають ряд загальних характеристик (таблиця 1, таблиця 2):

– обидві системи задовольняють вимогам специфікацій фізичного рівня H1 IEC/ISA, які визначають середовище передачі даних;
– обидві системи іскробезпечні й здатні по тим самим проводам передавати як дані, так і електроживлення для підключених до мережі пристроїв, що дозволяє використовувати їх у вибухонебезпечних зонах;
– обидві системи підтримуються міжнародними організаціями, що поєднують як кінцевих користувачів, так і постачальників;
– обидві системи можуть бути розгорнуті як цифрова заміна аналогових каналів 4-20 ма з використанням тих же самих, уже існуючих ліній зв'язку;

– обидві системи підтримують роботу в багатоточечному режимі, завдяки чому знижуються витрати на монтаж і обслуговування кабельного господарства.

Однак між мережними системами є й істотні розходження (таблиця 1, таблиця 2). Хоча обидві системи здатні управляти подіями в самій мережі, застосовувана в PROFIBUS-PA комунікаційна модель «головний-підлеглий», а також відсутність протоколу системного адміністрування роблять PROFIBUS-PA незадовільним рішенням для управління розподіленими процесами. FOUNDATION™ fieldbus, навпроти, створювалася не тільки для організації обміну цифровою інформацією між керуючим пристроєм мережі й пристроями нижнього рівня (польового устаткування), але й для розподіленого управління, включаючи підтримку функції автоматичного конфігурування (plug-and-play), що істотно розширює границі сумісності устаткування. FOUNDATION™ fieldbus при передачі даних одночасно підтримує маркерний доступ і обмін за розкладом. Таким чином, дані, передані між функціональними блоками прикладної програми, що виконується на різних вузлах мережі, можуть бути точно синхронізовані за часом. Виконання функціонального блоку координується з передачами по шині, тому що кожний пристрій містить синхронізуємий таймер. Таким чином, контур управління, розподілений між декількома пристроями, може завершити операцію в найкоротший час. Це, у свою чергу, приводить до зменшення часу запізнювання й збільшенню швидкодії контуру.

Таблиця 1 – Порівняння комунікаційних протоколів

	PROFIBUS-PA	FOUNDATION fieldbus
Фізичний рівень	Стандарт IEC 61158-2	Стандарт IEC 61158-2
Швидкість обміну	31,25 кбіт/с	31,25 кбіт/с
Живлення пристроїв по лінії зв'язку	Так	Так
Використання існуючої кабельної інфраструктури	Так	Так
Робота у вибухонебезпечних зонах	Так	Так
Канальний рівень	802.4 (передача маркера, « ведучий-підлеглий»)	ANSI S50.02-3,4; TS-61158-3,4 (спеціально розроблений для польової шини)
Зв'язок «точка-точка»	Немає	Так
Синхронізація за часом	Немає	Так
Періодичні сеанси обміну	Опитування виконується провідним пристроєм	Планована підписка вузлів на дані, публікуємі іншими вузлами
Прикладний рівень	Розширення DP	Fieldbus Messaging (FMS) — обмін повідомленнями
Функціональні блоки	Типи блоків обмежені профілем пристрою	Повністю визначені й можуть бути розширені виробником пристроїв
Мова опису пристроїв	Немає	Так
Системное адміністрування	Немає	Так
Пошук тегу	Немає	Так
Присвоєння адреси	Немає	Так
Виконання функціонального блоку за розкладом	Немає	Так

Таблиця 2 – Порівняння переваг

Переваги польової шини	PROFIBUS-PA	FOUNDATION fieldbus
Початкова економія на вартості монтажних матеріалів	Так	Так
Ідентифікація пристрою	Так	Так
Діагностична й регламентна інформація	В обмеженому обсязі	Так
Віддалене конфігурування пристроїв	В обмеженому обсязі	Так
Віддалене калібрування	Немає	Так
Управління на рівні датчиків і виконавчих механізмів (польових пристроїв)	Немає	Так
Обробка аварійних подій і тренди	Немає	Так
Розширене подання про контрольований процес	Так, однак імена тегів і параметрів не зберігаються в пристрої	Так
Воля вибору постачальника устаткування	Обмежена	Так
Підтримка декількох провідних вузлів	Обмежена. Додавання наступного провідного пристрою впливає на тривалість циклу опитування	Так. Кількість провідних вузлів не впливає на характеристики шини
Класи вироблених пристроїв	Пристрої цифрового й аналогового вводу/виводу з функціями збору даних	Пристрої цифрового й аналогового вводу/виводу з функціональними блоками

Прикладний рівень в FOUNDATION™ fieldbus забезпечує підтримку квітованої взаємодії між клієнтом і сервером, що може використовуватися для зміни оператором значень вставок, віддаленого завантаження й налаштування параметрів конфігурації. Крім того, підтримується розсилання оповіщень про аварійні події і їхні підтвердженя. Це засновано на тому же прикладному рівні, що використовується в PROFIBUS-FMS. В PROFIBUS-PA один ведучий вузол використовує протокол DP для опитування підлеглих вузлів, що містять функціональні блоки вводу/виводу. Час опитування всіх вузлів мережі залежить від кількості вузлів і ряду інших факторів, тому детермінованим може бути тільки час початку опитування. На прикладному рівні PROFIBUS-PA замість FMS використовує розширення DP, що приводить до обмеження можливостей по віддаленому конфігуруванню, а також по читанню й запису.

Система FIP

FIP являє собою багатопрофільну систему реального часу для управління процесами й комплексними автоматизованими виробництвами (CIM). Швидкість передачі даних лежить у межах від 31,25 Кбіт/с до 2,5 Мбіт/с. Зв'язок не будується за принципом зв'язку джерела із приймачем. Адреса джерела являє собою ім'я точно ідентифікованого об'єкта. Наприклад, вимірювана змінна процесу це об'єкт. Всі технологічні об'єкти, підключені до мережі, знають і називають об'єкт по його унікальному імені. Арбітр мережі посилає об'єкт у запропонованому порядку в організований список. Система FIP має головним чином періодичний трафік. Аперіодичні інформаційні повідомлення типу подій передаються у вигляді обміну запитами, що супроводжують циклічну передачу даних, з аперіодичним відкриттям вікон аперіодичної передачі даних. FIP це система fieldbus, що функціонує як розподілена база даних реального часу. Часова й просторова несуперечність даних гарантується завдяки локальним зчитуванню й запису даних, про що буде сказано далі.

Система CAN

CAN являє собою протокол послідовного зв'язку, ефективно підтримуючий розподілене управління в реальному часі з дуже високим рівнем захисту. Система має широкий діапазон застосувань: від високошвидкісних мереж до недорогого ущільненого монтажу. Різні підсистеми зв'язуються між собою с допомогою CAN при швидкості передачі 1 Мбіт/с. Інформація посилає по каналі у вигляді повідомлень фіксованого формату.

Вузол CAN не використовує якої-небудь інформації про конфігурацію системи (адреса станції). Змісту повідомлення привласнюється ім'я (ідентифікатор). Ідентифікатор не вказує на саме повідомлення, але описує інформацію, що втримується в ньому. Таким чином, всі вузли мережі можуть вирішувати, фільтруючи повідомлення, чи належно оброблятися на них ця інформація чи ні. Як наслідок з концепції передачі повідомлення, будь-яке число вузлів може одержувати й одночасно відпрацьовувати те саме повідомлення. Отже, погодженість даних у системі досягається шляхом групового використання даних і обробки помилок. Завжди, коли канал вільний, будь-який вузол мережі може почати передачу повідомлення. Конфлікти в системі дозволяються за допомогою поразрядного арбітражу. Під час арбітражу кожний передавач порівнює рівень переданого біта з рівнем біта в каналі. Коли посилає рецессивний рівень, а виявляється домінантний, блок уважається програвшим арбітраж і повинен бути відкликаний без посилки біта.

Загальне число блоків, що може бути охоплено мережею CAN, обмежено лише часом затримки й електричним навантаженням лінії зв'язку.

Багаторівнева структура

Кожний мережний протокол звичайно порівнюють із багаторівневої ISO-Моделлю й між ними встановлюють відповідність. Систему PROFIBUS можна прямо звести до ISO-Моделі з порожніми рівнями 3. Апаратура, канал передачі даних і управління визначені в розділі 1; FMS, LLI і управління рівнем в у розділі 2. Канальний рівень ділиться на підрівні Medium Access Control -MAC (рівень доступу в середовище) і Fieldbus Logical Control – FLC (логічне управління fieldbus). MAC забезпечує протокол доступу в гібридне середовище. FMS описує об'єкти зв'язку, сервіс і відповідну модель із погляду партнера по комунікації. Основними завданнями LLI є організація відображення FMS і FMA** на FDL***, установлення зв'язку, відключення, диспетчеризації зв'язку й управління потоками, FMA виконує контекстне конфігурування й виправлення помилок.

Система CAN має трьохрівневу структуру: фізичний рівень, рівень пересилання й об'єктний рівень. Рівень пересилання відтворює повідомлення, одержувані на об'єктному рівні, і приймає повідомлення, які варто передати на об'єктний рівень. Рівень пересилання відповідає за бітове тактування й синхронізацію, кадрування повідомлень, арбітраж і т.д. Об'єктний рівень займається фільтрацією повідомлень, а також обробкою статусу й повідомлень.

Система FIP є також трьохрівневою моделлю з фізичним рівнем, рівнем передачі даних і рівнем додатків. Рівень передачі даних відповідає за всі функції управління в реальному часі, а саме: за вибір у реальному часі циклів сканування, підтвердження управління якістю й передачі змінної, связность елементів розподіленої бази, синхронізоване квантування й управління, вибір безлічі диспетчерських послуг без внесення перешкод у трафик реального часу й т.д.

Фізичний рівень

Система PROFIBUS визначає як середовище лише екрановану кручену пару з характеристичним імпедансом 100...130 Ом. Довжина кабелю не перевищує 1200 м. Довжина лінії й число зв'язаних станцій можуть бути збільшені шляхом установки повторювачів (не більше трьох). Кабель шини повинен кінчатися так, як це описано в стандарті EIA RS-485. Кожна станція, призначена для закінчення лінії, повинна забезпечувати напруга +5В на контакті 6 мережного з'єднання й струм не менш 10 мА.

Максимальна відстань між вузлами може становити 2 км при 256 станціях у мережі. В CAN не визначаються характеристики драйвера/приймача й середовища, що дозволяє оптимізувати відповідно до застосування середовище передачі й реалізацію рівня сигналів.

Метод передачі

У системі PROFIBUS кожний біт кодується без повернення до нуля й передається диференціальною напругою. Під час періоду мовчання незаземлена диференціальна лінія переводиться кінцевим пристроєм в одиницю. Вона передає дані як символ-орієнтовані. Система FIP передає код і інформацію таймера, кодуючи їх за допомогою Manchester II. Швидкості передачі даних визначені рівними 31,25 Кбіт/с, 1 і 2,5 Мбіт/с. Арбітраж в FIP заснований на призначенні ремінного вікна кожному вузлу для періодичних даних і призначенні вікна по запиті для аперіодичних (мал. 2); існує необхідність глобальної синхронізації тактового генератора. Аналогічно в CAN здійснюється передача двох логічних значень, що взаємно доповнюють: рецессивного й домінантного. При одночасній передачі домінантного й рецессивного бітов результуючий канал буде домінантним. Для апаратної реалізації логічного "I" використовується логічний "0". Біт кодується без повернення до нуля. Час передачі кожного біта ділиться на не перекривають один одного сегменти: синхронізацію, проходження, фази / і 2.

Сегмент синхронізації використовується для синхронізації різних вузлів системи. Передбачається, що фронт імпульсу лежить усередині цього сегмента. Сегмент проходження служить для компенсації часу фізичної затримки. Він дорівнює подвоєній сумі часу проходження сигналу по лінії.

Фазові сегменти використовуються для компенсації фазової помилки фронту імпульсу. Ці сегменти можна вкоротити або подовжити. Рівень каналу зчитується наприкінці фази. Всі контролери CAN синхронізують на старті кадру. Таким чином, необхідний типовий допуск на генератор, що становить 1,58 % при швидкості передачі інформації з каналу, рівної 125 Кбіт/с. Оскільки системи FIP і CAN працюють при глобальній синхронізації тактових генераторів, їм на відміну від PROFIBUS потрібні тверді допуски на частоту тактових генераторів.

Обґрунтування вибору інтерфейсів послідовної передачі даних АСУ

Сучасні системи автоматизації традиційно використовують як обмін даними послідовний спосіб передачі даних. Послідовні інтерфейси відрізняються по швидкості передачі, довжині зв'язку, способі передачі, принципі передачі й топології структури шини. Параметри типових стандартних інтерфейсів послідовної передачі, представлені в таблиці 3.

Таблиця 3 – Характеристики типових стандартних інтерфейсів послідовної передачі

Інтерфейс	Стандарт	Швидкість передачі	Довжина (м)	Спосіб передачі	Принцип передачі
RS-232	EIA-232-C, CCITT v.24	19,2 Кбод	15	Рівні напруг	дуплекс точка-точка
TTY	DIN 66258-1, DIN 66248-1	19,2 Кбод	1000	Струмова петля	дуплекс точка-точка
RS-422	EIA-422, CCITT v.11	10 Мбод	1000	Різниця напруг	напівдуплекс точка-точка
RS-485	EIA-485, DIN 66259-4	1 Мбод	500	Різниця напруг	напівдуплекс багатоточка

На базі типових стандартних інтерфейсів реалізуються промислові (польові) шини типу CANBUS, BITBUS, PROFIBUS і інші. До шин, застосовуваним у виробництві систем управління купейним вагоном, пред'являються наступні основні вимоги:

– робота устаткування в широкому діапазоні температур;
– перешкодозахищеність трактів передачі даних (спосіб передачі);

– робота устаткування в реальному масштабі часу (швидкість);
– великі відстані об'єктів взаємодії (довжина);
– гнучка структура шин передачі даних (топологія шини).

Перешкодозахищеність трактів передачі даних залежить конкретно від приймачепередатчиків і фізичної лінії (тип кабелю, перетин, хвильовий опір).

Оптимальні дані для польових умов мають приймачепередатчики з диференціальними рівнями сигналів і лінії передачі на кручений парі. Системні магістралі на базі промислових шин повинні забезпечувати своєчасну й підлягаючому розрахункам передачу даних у реальному масштабі часу. Польові шини застосовуються як у централізованих, так і в розподілених системах, де відстані між об'єктами взаємодії можуть становити більше 1000 метрів. Гнучкість структури шин передачі даних припускає використання сегментированных ліній типу "лінія", "дерево", "зірка", "кільце" на базі багатоточки.

Усім вище перерахованим вимогам цілком задовольняє промислова шина PROFIBUS. Шина PROFIBUS зовсім недавно завоювала ринок промислових систем автоматизації, але вже є загальнопоширеною й визнаною в даній області застосування.

Структура протоколів PROFIBUS орієнтована на вже встановлені національні й міжнародні норми. Так, структура протоколів PROFIBUS базується на семиуровневой моделі взаємодії відкритих систем OSI (Open System Interconnection).

Інтерфейс RS-485

Інтерфейс RS-485 – широко розповсюджений високошвидкісний і завадостійкий промисловий послідовний інтерфейс передачі даних. Практично всі сучасні комп'ютери в промисловому виконанні, більшість інтелектуальних датчиків і виконавчих пристроїв, програмувальні логічні контролери поряд із традиційним інтерфейсом RS-232 містять у своєму составі ту або іншу реалізацію інтерфейсу RS-485.

Інтерфейс RS-485 заснований на стандарті EIA RS-422/RS-485. На жаль, повноцінного еквівалентного українського стандарту не існує, тому в даному розділі пропонуються деякі рекомендації із застосування інтерфейсу RS-485.

Традиційний інтерфейс RS-232 у промисловій автоматизації застосовується досить рідко. Сигнали цього інтерфейсу передаються перепадами напруги величиною (3...15…15)В, тому довжина лінії зв'язку RS-232, як правило, обмежена відстанню в кілька метрів через низьку завадостійкість. Інтерфейс RS-232 є в кожному PC – сумісному комп'ютері, де використовується в основному для підключення маніпулятора типу “миша”, модему, і рідше – для передачі даних на невелику відстань із одного комп'ютера в інший. Передача виробляється послідовно, послівно, кожне слово довжиною (5...8…8)біт випереджають стартовим бітом і закінчують необов'язковим бітом парності й стоп-бітами. Інтерфейс RS-232 принципово не дозволяє створювати мережі, тому що з'єднує тільки 2 пристрої (так зване з'єднання “точка – точка”).

Сигнали інтерфейсу RS-485 передаються диференціальними перепадами напруги величиною (0,2...8) В, що забезпечує високу завадостійкість і загальну довжину лінії зв'язку до 1 км (і більше з використанням спеціальних пристроїв – повторювачів). Крім того, інтерфейс RS-485 дозволяє створювати мережі шляхом паралельного підключення багатьох пристроїв до однієї фізичної лінії (так звана “мультиплексна шина”).

У звичайному PC-сумісному персональному комп'ютері (не промислового виконання) цей інтерфейс відсутній, тому необхідно спеціальний адаптер – перетворювач інтерфейсу RS-485/232.

Перетворювач інтерфейсу ПІ-485/232, використовується при організації зв'язку між пристроями, обладнаними інтерфейсом RS-232, але, що використовують у якості середовища передачі інтерфейс RS-485.

Деякі технічні дані перетворювача ПІ-485/232:

– взаємне “прозоре” перетворення сигналів інтерфейсів RS-232 і RS-485 з гальванічною ізоляцією між ними;
– управління напрямком передачі здійснюється з боку RS-232 по сигналу RTS;

– вимагає наявності сигналу DTR, використовуваного для живлення перетворювача (на стороні RS-232);

– організація зв'язку між різними пристроями, протокол передачі яких використовує напівдуплексний режим (запит і відповідь передаються по одній фізичній лінії, але в різні проміжки часу);

– індикація стану сигналів інтерфейсу RS-232: Rx (прийом), Tx (передача), RTS (сигнал управління передачею);

– максимальна швидкість обміну – 19200 біт/с.

Сигнал DTR установлюється при запуску програмного забезпечення підключеного з боку RS-232 пристрою. Скидання DTR виробляється при завершенні роботи програмного забезпечення. Сигнал RTS установлюється до початку передачі й скидається після повного її закінчення.

Існують і повністю автоматичні перетворювачі, що не вимагають сигналу управління передавачем, але, як правило, вони вимагають твердої вказівки швидкості обміну й довжини переданого слова (з обліком стартовий, стопових біт і біта парності).

Пристрої, що підключаються до інтерфейсу RS-485, характеризуються важливим параметром по входу приймачепередатчика: “одиниця навантаження” (“Unit Load” – UL). По стандарті в мережі допускається використання до 32 одиниць навантаження, тобто до 32 пристроїв, кожне з яких навантажує лінію в 1 UL. У цей час існують мікросхеми приймачепередатчиків з характеристикою менш 1 UL, наприклад – 0,25 UL. У цьому випадку кількість фізично підключених до лінії пристроїв можна збільшити, але сумарна кількість UL в одній лінії не повинне перевищувати 32.

Підключення перетворювача ПІ-485/232 до порту RS-232 здійснюється так званим “модемним” кабелем. Перетворювач має 9-контактний роз’єм (DB9, гніздо), персональний комп'ютер може мати роз’єми як 9-контактні (DB9, штир), так і 25-контактні (DB25, штир).

Таблиця 1 – Для 9-контактного роз’єму розпаювання кабелю здійснюється “один в один” (у дужках зазначені номери контактів)

DB9, штир – до перетворювача	DB9, гніздо – до комп'ютера
GND (5)	GND (5)
Rx (2)	Rx (2)
Tx (3)	Tx (3)
DTR (4)	DTR (4)
DSR (6)	DSR (6)
RTS (7)	RTS (7)
CTS (8)	CTS (8)
RI (9)	RI (9)
DCD (1)	DCD (1)

Цей стандартний кабель виробляється багатьма виготовлювачами.

Перетворювач ПІ-485/232 використовує в кабелі лінії до контактів 2,3,4,5,7.

Таблиця 2 – Відповідність контактів роз’ємів DB9 – DB25

Найменування контакту	DB9	DB25
DCD	1	8
Rx	2	3
Tx	3	2
DTR	4	20
GND (сигнальна)	5	7
DSR	6	6

RTS	7	4
CTS	8	5
RI	9	22

Пристрої до мережі RS-485 підключаються послідовно, з дотриманням полярності контактів A і B.

Навіть для швидкостей обміну порядку 19200 біт/с кабель уже можна вважати довгою лінією, а будь-яка довга лінія для виключення перешкод від відбитого сигналу повинна бути погоджена на кінцях. Для узгодження використовуються резистори опором 120 Ом (точніше, з опором, рівним хвильовому опору кабелю, але, як правило, використовувані кручені пари мають хвильовий опір близько 120 Ом і точно підбирати резистор немає необхідності) і потужністю не менш 0,25 Вт – так званий “термінатор”. Термінатори встановлюються на обох кінцях лінії зв'язку, між контактами A і B кручений пари. Перетворювач ПІ-485/232 уже має термінатор, і при необхідності його можна включити установкою перемички між контактами 'T' і 'T'.

У мережах RS-485 часто спостерігається стан, коли всі підключені до мережі пристрої перебувають у пасивному стані, тобто в мережі відсутня передача й всі приймачепередатчики “слухають” мережу. У цьому випадку приймачепередатчики не можуть коректно розпізнати ніякого стійкого логічного стану в лінії, а безпосередньо після передачі всі приймачепередатчики розпізнають у лінії стан, що відповідає останньому переданому біту, що еквівалентно перешкоді в лінії зв'язку. На цю проблему не так часто обертають уваги, борючись із її наслідками програмними методами, але проте вирішити її апаратно нескладно. Досить за допомогою спеціальних ланцюгів зсуву створити в лінії потенціал, еквівалентний стану відсутності передачі (так званий стан “MARK”: передавач включений, але передача не ведеться). Ланцюга зсуву реалізовані в перетворювачі ПІ-485/232, для їхнього підключення досить установити 2 перемички між контактами ‘+V’ і ‘+V’, ‘-V’ і ‘-V’ відповідно. Для коректної роботи ланцюгів зсуву необхідна наявність двох термінаторів у лінії зв'язку.

У мережі RS-485 можлива конфліктна ситуація, коли 2 і більше пристрої починають передачу одночасно. Це відбувається в наступних випадках:

– у момент включення живлення через перехідні процеси пристрою короткочасно можуть перебуває в режимі передачі;
– одне або більше із пристроїв несправно;
– некоректно використовується так званий “мультимастерний” протокол, коли ініціаторами обміну можуть бути кілька пристроїв.

У перших двох випадках швидко усунути конфлікт неможливо, що теоретично може привести до перегріву й виходу з ладу приймачепередатчиков RS-485. На щастя, така ситуація передбачена стандартом і додатковим захистом приймачепередатчика звичайно не потрібно.

В останньому випадку необхідно передбачити програмний поділ каналу між пристроями – ініціаторами обміну, тому що в кожному разі для нормального функціонування лінія зв'язку може одночасно надаватися тільки одному передавачу.

Розробка структурної схеми

На рисунку 1 зображена структурна схема системи. На схемі зображена взаємодія головного вагона (центра керування) і підлеглого вагона, а також підсистеми підлеглого вагона.

Розглянемо цю схему докладніше:

– система керування вагону купе провідника підробно розглянута на рисунку 3.6;
– температурний датчик дозволяє уточнювати поточну температуру у вагоні;
– відеосистема дозволяє переглядати поточний відеосигнал з центра керування;
– аудіосистема аудіо сповіщення та радіо;
– кнопка виклику провідника;

– термінал доступу до мережі дозволяє виходити в Інтернет за при наявності у пасажирів ноутбука апаратними засобами вагону через (Wi-Fi);
– дверний датчик контролює поточне положення;
– віконний датчик контролює поточне положення;
– динамічне табло показує наступну станцію та рекламні пропозиції.

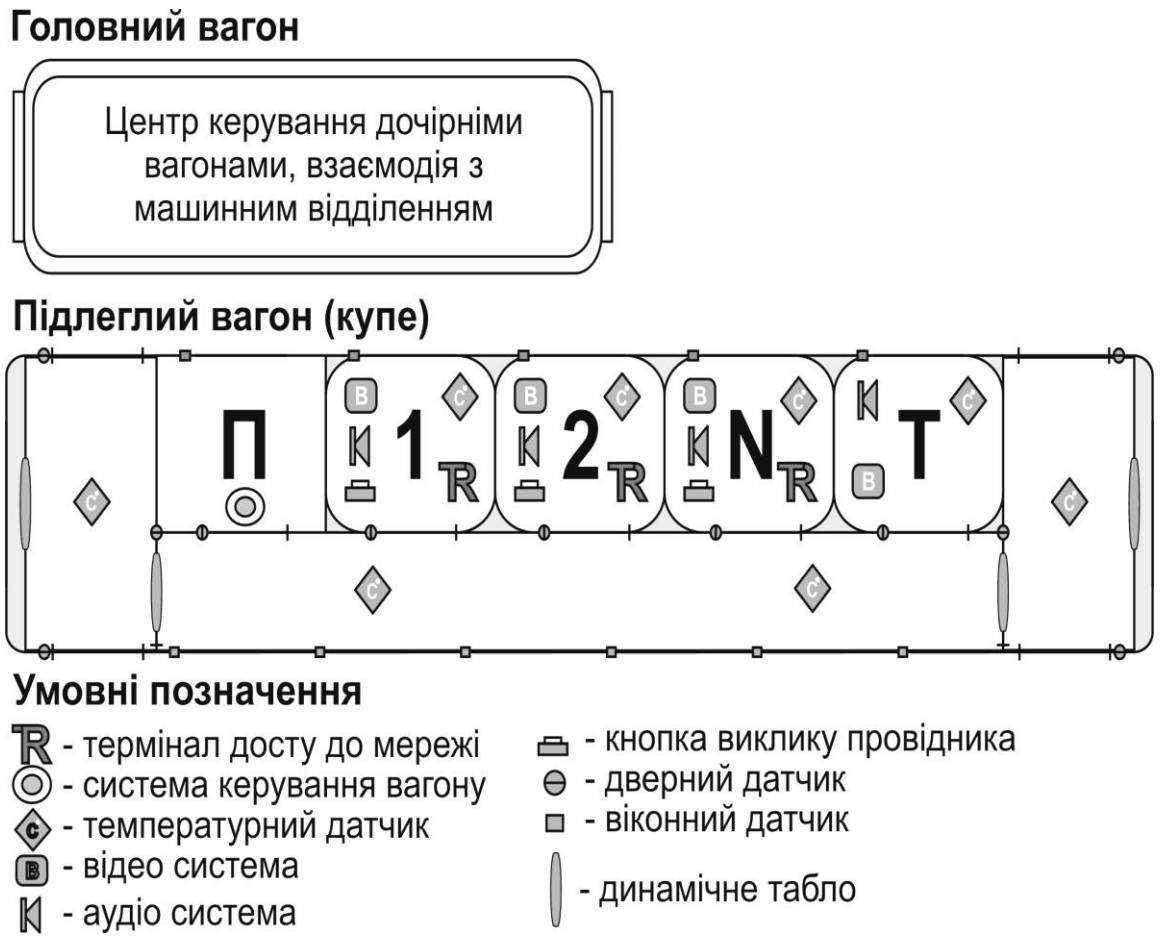


Рисунок 1 – Структурна схема системи

В свою чергу в купе провідника знаходиться центр керування (рисунок 2) який контролює поточні дії у вагоні та відсилає інформацію у центр керування. Розглянемо можливості системи керування у купе бортпровідника:
– перегляд показань температурного датчика;
– дублювання відеота аудіо сигналу;
– комутація з головним вагоном;
– перегляд положення дверних датчиків;
– перегляд положення віконних датчик;
– керувати консоллю та переглядати попередження з центру керування.

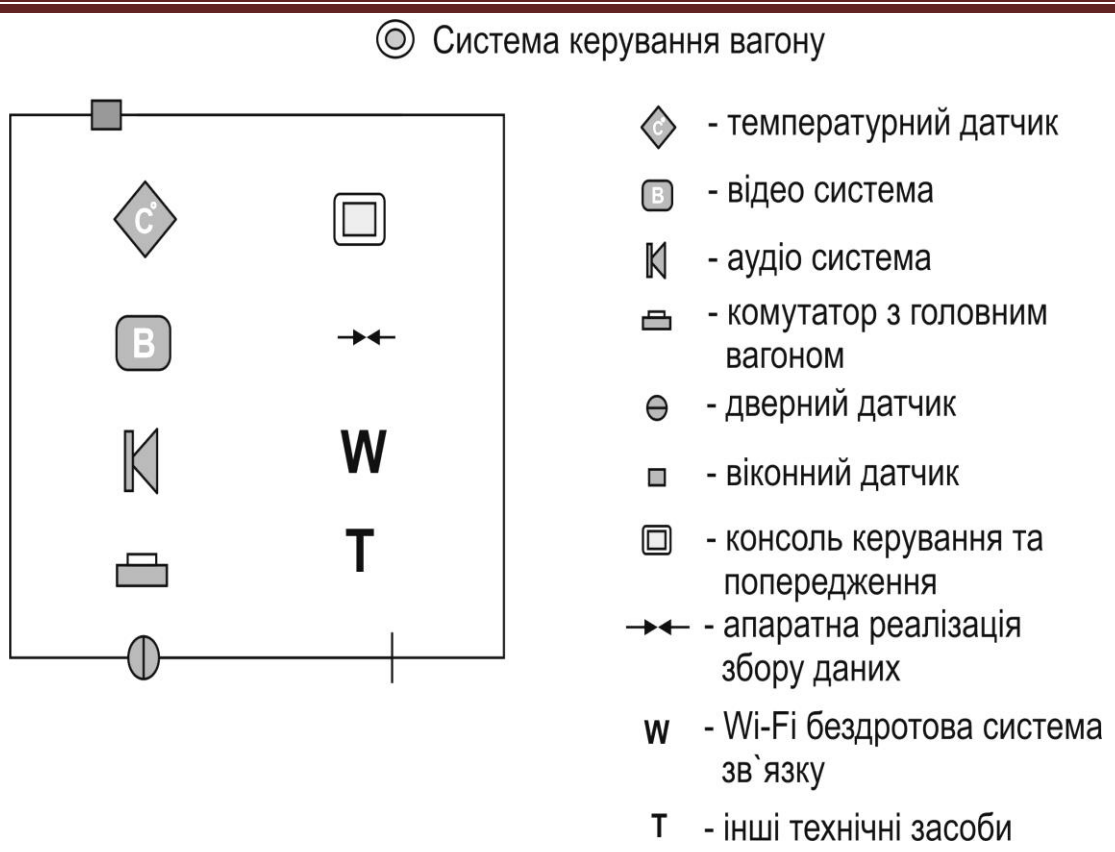


Рисунок 2 – Структурна схема системи керування

Також на структурній схемі системи керування відображено що крім системи керування у купе провідника знаходиться апаратна реалізація збору даних, бездротова система зв`язку (Wi-Fi) та реалізація інших технічних засобів.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів реалізації автоматизованої інформаційно-діагностичної системи поїзду. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем реалізації автоматизованої інформаційно-діагностичної системи поїзду. Досліджена система реалізації автоматизованої інформаційно-діагностичної системи поїзду.
На основі отриманих результатів досліджень створена програмна реалізація автоматизованої інформаційно-діагностичної системи поїзду. Розроблені алгоритми дозволяють успішно вирішувати завдання реалізації автоматизованої інформаційно-діагностичної системи поїзду. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 2(38). – С. 106-108.
2. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
3. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 2014. – № 2(15). – С.154-157.
4. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування,

автоматизація. – Кіровоград: Вид-во КНТУ, 2014. – Вип. 27. – С. 245-251.
5. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2014. – № 4(40). – С. 85-88.
6. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 1(126). – С. 75-79.
7. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 2015. – Вип. 1(42). – С.39-41.
8. Коваленко А.С. Експертна система технічного діагностування інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 2015. – № 1(41). – С. 106-111.
9. Коваленко А.С. Удосконалення методу технічного обслуговування об’єктів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко, О.П. Доренський // Системи озброєння і військова техніка. – Х.: ХУПС, 2016. – № 2(46). – С. 109-114.
10. Коваленко А.С. Метод визначення оптимального комплексу робіт з відновлення працездатності інтегрованої системи технічної діагностики в умовах ресурсних обмежень / А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 2016. – Вип. 3(140). – С. 69-72.

УДК 004

В. Прокопов, магістр гр. КІ-20М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ КЛАСТЕРИЗАЦІЇ ТА АНАЛІЗУ ДАНИХ З ВЕБ-РЕСУРСІВ

У статті представлено результати розробки програмного забезпечення, яке призначено для застосування алгоритмів машинного навчання у сфері інформаційної безпеки. Метою розробки є дослідження та програмна реалізація моделей алгоритмів машинного навчання для виявлення кібератак. Об’єктом дослідження є процес аналізу даних з веб-ресурсів у системах кібербезпеки. Предметом дослідження є методи та алгоритми аналізу даних з веб-ресурсів, засновані на лінійних моделях та ансамблевих рішеннях. Методи дослідження базуються на методах розробки програмного забезпечення, функціональній парадигмі програмування, теорії ймовірності та теорії статистики. Результат роботи – програмна реалізація алгоритмів машинного навчання для виявлення кібератак. В процесі роботи над програмною моделлю виконано аналіз існуючих програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення та наведені інструкції по роботі з програмними засобами.
комп’ютерна інженерія, аналіз та обробка даних, кібербезпека

Постановка проблеми. Стрімке розвинення інформаційних технологій, впровадження досягнень науково-технічного прогресу у сучасний побут та масштабна цифровізація багатьох сфер життя, дозволили розглядати сучасний світ у формі формалізованих сукупностей представлень інформації, що піддаються інтерпретації, – даних, що дало можливість, використовуючи математичні алгоритми та статистичні методи, досліджувати їх закономірності, взаємозв’язки, процеси та створювати прогнози. Зважаючи на широке розповсюдження машинного навчання, цілком природно, що цю технологію почали впроваджувати у сфери інформаційної так і комп’ютерної безпеки. Забезпечення комп'ютерної безпеки має всі підстави розглядатися, як одна із найбільш важливих проблем сучасного суспільства. Так як сучасне суспільство стає все більш залежними від комп'ютерів у роботі, проведенні дозвілля, розвагах, в звичайному житті, в рівних пропорціях зростає і значимість наявності вразливостей і лазівок в комп'ютерних системах, що привертають

зовсім недоречну увагу кола вкрай недоброзичливих особистостей, які сподіваються такими способами отримати гроші або просто заподіяти збитків. Отже, вкрай важливо захищати веб-ресурси від інформаційних атак, а також розпізнавати такі атаки для їх своєчасного усунення, якщо методи превентивного захисту не спрацювали.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1, 3] було виявлено певні прогалини системи кібербезпеки кластеризації та аналізу даних з веб-ресурсів. При вивченні джерел [4, 5] було проаналізовано методи побудови системи кібербезпеки кластеризації та аналізу даних, та виявлено потенційні шляхи реалізації. Аналіз публікацій [6, 7] підтвердив актуальність проблеми у контексті розробки системи кібербезпеки кластеризації та аналізу даних з веб-ресурсів.

Мета й завдання дослідження. Метою даної роботи є дослідження та програмна реалізація моделей алгоритмів машинного навчання для виявлення кібератак.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих реалізацій систем виявлення кібератак.

– Дослідження алгоритмів машинного навчання в контексті застосування для виявлення кібератак.

– Розробка та реалізація системи кібербезпеки кластеризації та аналізу даних з веб-ресурсів.

Об'єктом дослідження є процес аналізу даних з веб-ресурсів у системах кібрберзпеки.

Предметом дослідження є методи та алгоритми аналізу даних з веб-ресурсів, засновані на лінійних моделях та ансамблевих рішеннях.

Методи дослідження базуються на методах розробки програмного забезпечення, функціональній парадигмі програмування, теорії ймовірності та теорії статистики.

Основний матеріал. Розглянемо спочатку основні терміни області дослідження. *Машинне навчання* – створення алгоритмів та організація процесів, які здатні до навчання на основі дослідження великих обсягів даних, з тим, щоб на їх основі передбачати майбутні результати. *Кібербезпека* – методологія захисту комп'ютерних систем і мереж від розкриття інформації, крадіжки або пошкодження їх апаратного забезпечення, програмного забезпечення або електронних даних, а також від порушення або неправильного спрямування послуг. *Аналіз даних* – це процес перевірки, очищення, перетворення та моделювання даних з метою виявлення корисної інформації, надання висновків та підтримки прийняття рішень.

Загалом побудова моделі алгоритму машинного навчання, як правило, може поділятися на наступні декілька етапів: збирання даних, попередня обробка, аналіз, тестування і т.д. Для тренування моделі для виявлення кібератак було обрано набір даних (датасет) CSE-CIC-IDS2017. Даний набір даних був підготовлений за результатами аналізу мережевого трафіку в ізольованому середовищі, в якому моделювалися дії низки звичайних користувачів, а також шкідливі дії порушників. Набір даних CICIDS2017 містить найсучасніші поширені атаки, що відповідають вигляду справжніх даних реального світу (PCAP) [8].

Загальні кількість атрибутів, які описують кожний окремий зразок даних, становить близько вісімдесяти. Така велика кількість характеризуючих ознак, хоча і послугує для якнайкраще якіснішого відділення зразків між собою та класів, може виявитися надлишковою, оскільки не кожна ознака може слугувати для виявлення унікальності, що буде виявляти відмінність одного класу від іншого; деякі ознаки взагалі можуть не нести ніякої корисної інформації, яка б описувала дані. Беручи до уваги велику кількість зразків даних та розмір ознакового простору буде доцільним провести відбір ознак. Тобто буде доречно провести процедуру створення такої підмножини ознак, яка буде, при значно меншій порівняно з попередньою кількістю змінних, зведе до мінімуму втрату вагомої для набору даних інформації. Зниження ознакового простору набору даних дозволить отримати

низку переваг: підвищення ступеню інтерпретації моделі; збільшення швидкості навчання; зниження можливості приймання рішень моделлю з урахуванням «шумів».

Сам набір даних в загальній сукупності містить у собі понад два мільйони чотириста тисяч зразків даних, кожен з яких розмічений як сутність, що належить до певного класу, який описує належність до нормального трафіку (benign) чи шкідливого (наприклад, PortScan, DDoS, Bot, і т.д.). Всього в датасеті виділяється близько п’ятнадцяти різних класів, та слід зазначити, що кількість зразків в кожному із них розподілена вкрай нерівномірно, та ті сильно відрізняється від класу до класу. Наприклад, кількість зразків у класі heartbleed складає усього одинадцять, тоді як клас goldeneye налічує близько десяти тисяч зразків. Якщо взяти усю сукупність даних то частка класу benign складає близько вісімдесяти чотирьох відсотків, а решта шістнадцять відсотків припадає на усі інші класи атак. Тож, беручи до уваги ці фактори, аби уникнути проблеми із збалансованістю даних необхідним є проведення наступних дій: об'єднання усіх класів атак в один єдиний (це також зводить проблему класифікації з мультикласової до бінарної); забезпечення міжкласового балансу. Однією із методик вирішення проблеми дизбалансованості між класами є методика субдискретизації. Сутність даного методу полягає у вибірці елементів із домінуючих класів із метою скорочення їх кількості. Стратегії субдискретизації можуть бути простими, як, наприклад, випадковий вибір групи елементів, але при цьому можливі втрати інформації у певних наборах даних. У таких випадках стратегія вибірки має передбачати в першу чергу видалення елементів, які дуже схожі на інші елементи, що залишаються в наборі даних. Для відкидання надлишкових даних було застосовано техніку субдискретизації мажоритарного (домінуючого) класу на основі центроїдів кластерів. Ця техніка полягає у створені за допомогою алгоритму кластеризації (у даному випадку метод k-середніх) кластеру домінуючого класу та у подальшому відкиданню зразків, керуючись відстанню від центроїда до положення зразку у просторі, розрахованою за евклідовою метрикою.

Важливе місце у аналізі та досліджені даних відводиться їх попередній обробці. Етап попередньої обробки даних у даному випадку включає в себе перевірку кожного значення атрибуту, заповнення відсутніх значень, кодування даних у формат зрозумілий для моделі. Так, зокрема, необхідно провести дослідження ознак і замінити значення Infinity на значення -1, замість значення inf поставити 0, теж саме із значеннями типу NaN [9]. Наостанок проводиться відбір усіх атрибутів не числового типу (категоріальні, строкові, змішані і т.д.) та провести їх перетворення.

Для вирішення завдання з відбору ознак ефективною є стратегія відбору на основі моделі випадкового лісу. Модель, що застосовується для відбору ознак, вимагає обчислення певного показника важливості для всіх ознак, щоб характеристики можна було ранжувати за цією метрикою. Одним із типових напрямків використання випадкових лісів може бути визначення оцінки важливості ознак в задачах регресії і класифікації. З початку для надання оцінки важливості ознак у тренувальному наборі проводиться тренування випадкового лісу на цьому наборі. Впродовж процесу побудови моделі для кожного елементу тренувального набору записується так звана помилка невідібраних елементів. Потім така помилка усереднюється у всьому випадковому лісі для кожної із сутності. Отримавши оцінку важливості ознак, розмірність даних було знижено із вісімдесяти до двадцяти одного виміру ознакового простору.

Висновки. У статті наведено результати дослідження та розробки системи кібербезпеки кластеризації та аналізу даних з веб-ресурсів Після проведення етапу попередньої обробки даних, зміни значень даних, заповнення пропущених місць, формування ознак, видалення ознак, форматування значень атрибутів наступає етап розділення набору даних на дві різні підмножини: тренувальний та тестовий набори. Для тренування моделі були вибрані наступні алгоритми машинного навчання: наївний баєсів класифікатор, k-найближчих сусідів, дерева рішень, метод опорних векторів (SVM) з використанням гауссівського ядра, адаптивний бустинг, дерева рішень з прискоренням (бустинг градієнта). Разом з тренуванням одразу виконувалася перехресна перевірка (з

контролем) за семи блоками, для отримання більш точної оцінки узагальнюючої здатності моделі. Ефективність моделей оцінювалися за показниками їх правильності, точності, повноти та f1-мірою. Найбільш ефективні результати показали градієнтний бустинг (97,9%) та адаптивний бустинг (97,8%).

Список літератури

1. Ambareen Siraj Applications of Machine Learning in Cyber Security. 2014.
2. Matt Lewis Rise of the machines: Machine Learning & its cyber security applications. 2017
3. Robin Sommer, Vern Paxson Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. 2010
4. Dhruba Kumar Bhattacharyya Network Anomaly Detection: A Machine Learning Perspective. 2013. pp. 366
5. Peter Flach Machine Learning: The Art and Science of Algorithms that Make Sense of Data. 2012. pp. 409
6. Andriy BurkovThe Hundred-Page Machine Learning Book. 2019. pp 160.
7. Чио К., Фримэн Д. Машинное обучение и безопасность / пер. с анг. А. В. Снастина. – М.: ДМК Пресс, 2020. – 388 с.: ил.
8. Intrusion Detection Evaluation Dataset (CIC-IDS2017).
9. Kahraman Kostas, Anomaly Detection in Networks Using Machine Learning. 2018
10. Жерон, Орельен. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow: концепции, инструменты и техники для создания интеллектуальных систем. Пер. с англ. - СпБ.: ООО "Альфа-книга': 2018. - 688 с.: ил. - Парал. тит. англ.

УДК 004

А. Пономаренко, магістр гр. КН-20МЗ
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ГЕНЕРАЦІЇ ТА ПРОХОДЖЕННЯ ЛАБІРИНТІВ ДЛЯ РОЗРОБКИ ВІДЕОІГОР

У статті представлено результати розробки програмного забезпечення, яке призначено для реалізації алгоритмів генерації та пошуку руху в області лабіринту у системі ігрового рушія на платформі Windows. Метою розробки є дослідження та програмна реалізація алгоритмів створення, генерації, розробки схеми візуального вигляду ігрового рівня - лабіринту та їх оптимізація. Об'єктом дослідження є процес реалізації алгоритмів для генерації візуальних рівнів (таких як Ейлера, A*, хвильовий) в системи Windows та їх оптимізація для роботи на ПК. Результат роботи – програмна реалізація алгоритму Ейлера для генерації лабіринтів, в інших джерелах може називатися "deep-first-search" або "spanning tree", в системі ігрового рушія на платформі Windows. В процесі роботи над програмною моделлю виконано аналіз існуючих програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення. Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

комп'ютерна науки, система ігрового рушія, алгоритми генерації лабіринтів, алгоритми пошуку виходу з лабіринтів

Постановка проблеми. Ігрова індустрія постійно розробляє нові додатки для пришвидшення процесу розробки ігор. Значна кількість ігор, пригодницьких жанрів і аркади використовують лабіринти. Також дуже часто спостерігаються в інших жанрах: екшен, логічні ігри, іноді в симуляторах. Важливими при розробці ігор є дві задачі: розробка самого лабіринту як віртуального середовища гри та знаходження шляху крізь лабіринт для різних персонажів у грі, що управляються комп'ютером. Тож, дослідження програмного забезпечення системи генерації та проходження лабіринтів для розробки відеоігор, є актуальною задачею, яка потребує вирішення.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у системах генерації та проходження лабіринтів для розробки відеоігор.

Мета й завдання дослідження. Метою даної роботи є дослідження та розробка методів, алгоритмів та програмного забезпечення системи генерації та проходження лабіринтів для розробки відеоігор. А також збір теоретичних відомостей про сучасні інструментальні засоби для побудови ігор, вирішення задач для створення тесових проектів ігор-прототипів, генерації різних лабіринтів та можливість знаходження кінцевої точки у лабіринті.

Об'єктом дослідження є процеси генерації лабіринтів та пошуку руху у них.

Предметом дослідження є методи генерації лабіринтів та пошуку шляху у них за допомогою компонентів та інтерфейсів системи ігрового рушія Unity та їх оптимізація для роботи на ПК.

Методи дослідження базуються на теорії об'єктно-орієнтованого програмування, теорії ймовірності та теорії штучного інтелекту.

Виклад основного матеріалу. Було проведено дослідження алгоритмів генерації лабіринтів, найбільш поширені у застосуванні наведені нижче.

Алгоритм Ейлера. Дозволяє розробляти лабіринти, які мають лише один шлях між двома точками. Він дуже швидкий і використовує пам'ять ефективніше ніж інші алгоритми, такі як Kruskal та Prim. Він потребує пам'яті пропорційна числу рядків. Це дозволяє створювати лабіринти великих розмірів, при мінімальних розмірах пам'яті. Лабіринти класифікуються за семи різними класифікаціями: текстура, гіпервимірність, розмірність, топологія, фокус, теселяція. маршрутизація. При створені лабіринту можна взяти по одному предмету з кожного класу в різних комбінаціях. Наприклад, Гіперлабіринт включає в себе об'єкт що розв'язується, він складається з ліній, де підчас згинання та переміщення шлях утворює поверхню. Гіперлабіринт використовують лише в середовищі 3D або більшого розміру. Де умовою входу до гіперлабіринту є лінія. Він може бути великих розмірів, збільшує розмірність розв'язаного об'єкту рішенням, якого є площина, де підчас його переміщення шлях за ним утворюється тверде тіло в такому випадку Гіперлабіринт другого порядку може існувати в середовищі 4D або вище.

В класі Теселяції використовують геометрію окремих комірок з яких складають лабіринти. Теселяція буває таких типів:

1. Ортогональна. Виглядає як прямокутна сітка, де клітина має проходи і перетинаються під прямим кутом;
2. Дельта. Будується на основі трикутників, що з'єднуються між собою і можуть мати до трьох з'єднаних проходів;
3. Сигма. Лабіринт складається із шестикутників, з'єднаних між собою, де кожна клітина може мати до 6 каналів підключення до неї.
4. Зета. Розміщення на прямокутній сітці, в якій діагональні проходи під кутом 45 градусів між клітинками дозволенні на додаток до горизонтальних і вертикальних.
5. Іпсілон. Це лабіринти які складаються з взаємозв'язаних квадратів і восьмикутників, де кожна клітинка може мати 4 або 8 можливих проходів пов'язаних з нею.

Клас текстури є тонким і описує стилі проходження в будь-якій маршрутизації, в будь-якій геометрії. Текстура включає в себе: зміщення, біг, Elite, симетричний лабіринт, однорідність. Коефіцієнт "елітароності" вказує на розмір лабіринту і на довжину рішення. Зазвичай Елітарний лабіринт має коротке рішення він може бути набагато складнішим, ніж неелітарний.

Binary Space Partitioning. Розділення області в бінарному типі. Він також дозволяє обходити перетинання клітинок/кімнат у стадії розміщення на області генерації лабіринту. Ділячи поле частинами, порівняно з листями дерева, де розташовує згенеровану кімнату. Алгоритм використовує максимально різні конфігурації кімнат.

Клітинний автомат для генерації простору кімнат/лабіринтів. Суть запропонованого

алгоритму полягає в реалізації всього двох кроків: спочатку все поле заповнюється випадковим чином стінами – тобто для кожної клітини випадковим чином визначається, чи буде вона вільною або непрохідною – а потім кілька разів відбувається оновлення стану карти відповідно до умов, схожих на умови народження / смерті в «Життя».

Також було проведено дослідження алгоритмів пошуку виходу з лабіринтів.

Алгоритм «однієї руки» Найпоширеніший метод для проходження лабіринту є правило на основі алгоритму "однієї руки": рухаючись по лабіринту, треба весь час використовувати праву чи ліву рук його стіни. Він використовувався ще за часів древніх греків. Для проходження лабіринту потребує багато часу, але результат буде позитивним.

1) Роботи алгоритму почнеться з знаходженням першої стінки, в доль якої він буде рухатись. Для цього йому лиш потрібно рухатись вперед, поки не потрапить до перешкоди.

2) Після попадання до першої перешкоди алгоритм починає діяти за правилом “правої руки”.

4) Якщо проходу не знайдено по праву сторону стіни він повертає ліворуч. У разі потрапляння в глухий кут, ще раз повертає ліворуч, таким чином на 180 градусів, і йде в зворотному напрямку.

Якщо ж лабіринт містить окремі стінки, то, застосовуючи правило "однієї руки", не завжди підходить. Лабіринти з окремими стінками і з замкнутими маршрутами називаються багато зв’язними. При цьому багатопланові лабіринти можуть бути розділені на дві групи: без «петлі» навколо цілей (замкнутий маршрут не проходить навколо цілей) і з замкнутої «петлі» навколо мети.

Хвильовий алгоритм на основі пошуку та побудови шляху між двома точками в лабіринті. Він поділяється на 2 етапи:

1) З стартової точки в чотирьох напрямках хвиля починає свій рух в середину лабіринту. Збоку здається наче великий фронт рух великою кількості варіантів пошуку руху. Перші елементи фронту супроводжується вторинним потоком вони і являються джерелом переходів по області. Процес триває до останнього кінцевого положення елементу на області дослідження.

2) Розробка траєкторії рух по площині, їх побудова починається з стартового елементу закінчуючи кінцевим.

Позитивний момент алгоритму в тому, що шлях буде знайдений в лабіринті різної складності, при наявності виходу. Недолік, значне використання об’єму пам’яті.

Алгоритм Дейкстри базується на пошуку всіх варіантів найкоротшого шляху за допомогою заданої вершини графа. При достатній кількості необхідної інформації є можливість дослідити максимально вигідний шлях, послідовність руху обходячи перешкоди. До недоліків відносять неможливість наявності в графі дуги негативної маси. Даний алгоритм поетапно перебирає всі вершини графа і призначає їм комірки, які є відомим мінімальним відстанню від вершини джерела до конкретної вершини.

Наведемо деякі приклади псевдокоду алгоритмів пошуку шляху у лабіринті.

Псевдокод 1. Метод найпростішого рекурсивного алгоритму, в якому зв’язність в двомірному масиві визначається за 4 напрямками:

```
public int [, ,] lab = new int [100, 100, 3]; // лабіринт: [i,j,0] - осередки лабіринту, [i,j,1] - для хвильового методу - довжина хвилі, для однорукого методу - шлях персонажа
public int [,] path = new int [10000, 2]; // Зворотний шлях хвильового методу
public int countpath = 0; // кількість кроків у шляху хвильового методу
public int xcells; // осередків по горизонталі
public int ycells; // осередків по вертикалі
public int xstart; // координати стартової позиції
public int ystart; // координати стартової позиції
public int xstop; // координати кінцевої позиції
public int ystop; // координати кінцевої позиції
public int tx; // поточне становище при однорукому методі
```

```
public int ty; // поточне становище при однорукому методі
public int way; // Напрямок руху при однорукому методі
public int len; // поточна довжина шляху при однорукому методі
public int vert_rating=50; // ймовірність % створення вертикальної стінки в алгоритмі Ейлера
```

Псевдокод 2. // Хвильовий алгоритм

```
// Використовується в процесі пошуку виходу з лабіринту
public void Volna()
{
int i, j;
// Елементи масиву lab [i, j, 1] містять значення довжини хвилі лабіринту
// ініціалізуємо їх значеннями -1
for (i = 0; i < xcells; i++)
{
for (j = 0; j < ycells; j++)
{
lab [i, j, 1] = -1;
}
}
lab[xstart - 1, ystart - 1, 1] = 0; // на вході лабіринт довжина хвилі =0
int lastwave = -1; // Номер поточної хвилі
int cou = 1; // кількість осередків, які накрила попередня хвиля
bool found = false; // хвиля дістала до виходу?
while (!found && (cou > 0)) // поки хвиля не дійшла до виходу і поки попередня хвиля накрила хоч скільки-небудь осередків
{
cou = 0; // кількість осередків, які накрила хвиля
lastwave++; // Номер поточної хвилі
for (i = 0; i < xcells; i++)
{
for (j = 0; j < ycells; j++)
{
if (lab[i, j, 1] == lastwave) // обробимо лише комірки, які накрило попередньою хвилею
```

На рис. 1 зображена структурна схема розроблюваної системи. Розроблена система складається з головного меню та кнопок Генерація рівня, Опції та Вихід.

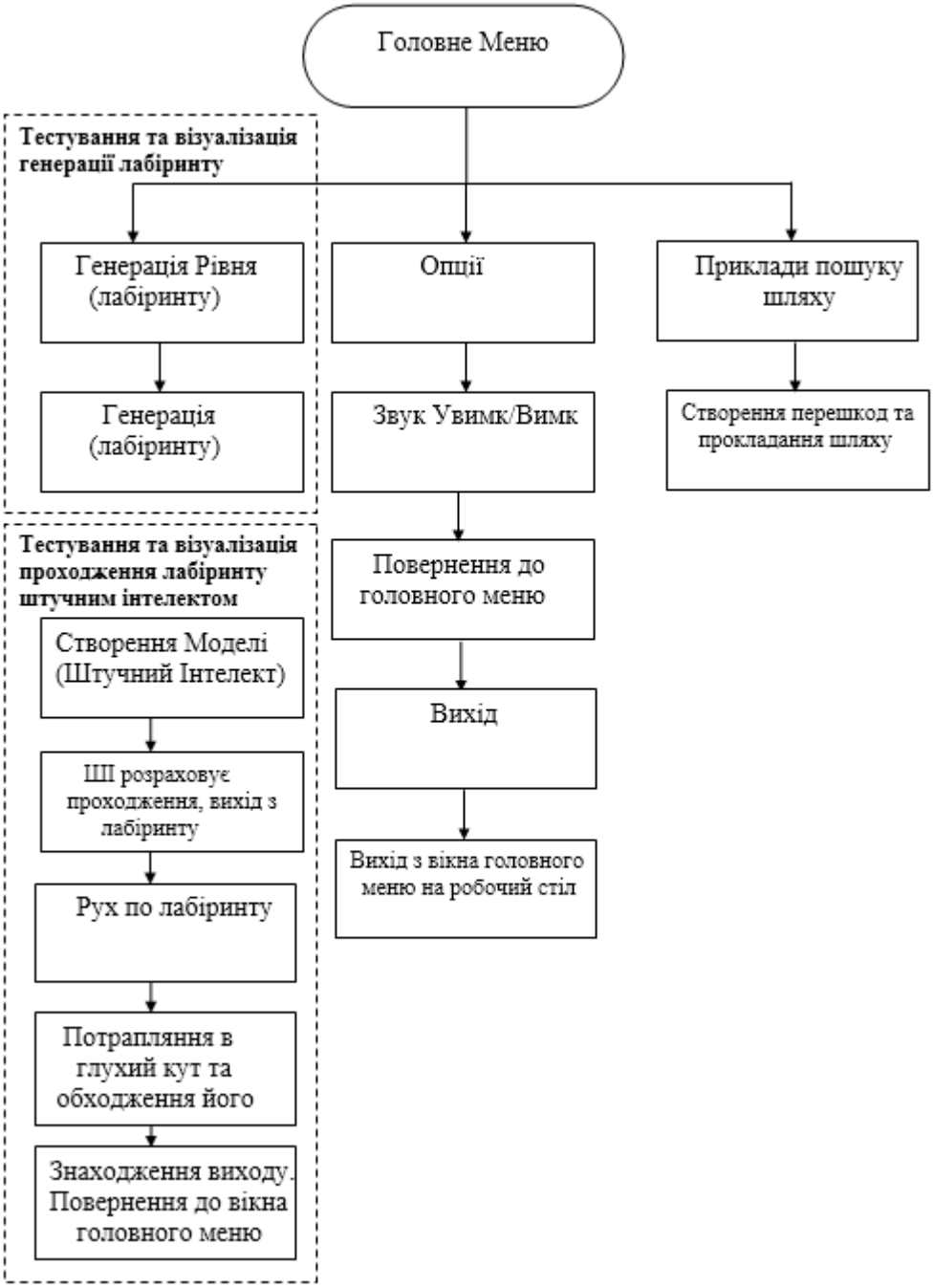


Рис.1. Структурна схема системи

З рис. 1 видно, що після запуску програми спочатку відбувається вивід основного вікна програми. Потім користувач обирає одну з наступних дій:

1. Запуск програми.
2. Налаштування.
3. Генерація лабіринту.
4. Перехід до налаштувань.
5. Рух по лабіринту.
6. Пошук кінцевої точки Алгоритм A*.
7. Приклади пошуку шляхів.
8. Створення власних перешкод.
9. Рух до виходу.
10. Звук увимк/вимк.

11. Повернення до головного вікна.
12. Вихід.

На рис. 2-3 наведено приклади сгенерованих у розробленому програмному забезпеченні лабіринтів та процесу пошуку шляху у них.

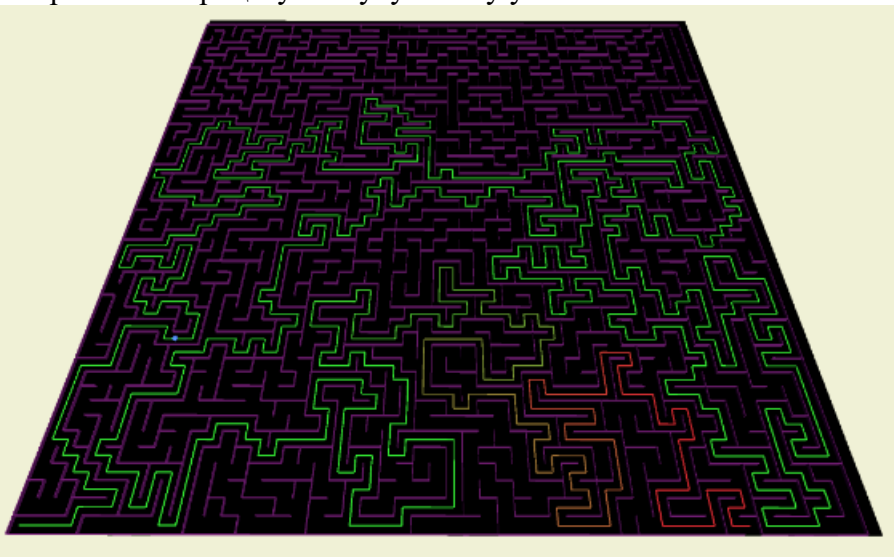


Рис. 2. Вікно сцени генерації лабіринту та пошуку виходу

Рис. 3. Вікно прикладу роботи алгоритму пошуку шляхів

Висновки. У статті наводяться результати розробки програмного забезпечення системи генерації та проходження лабіринтів для розробки відеоігор. Програма реалізована на мові високого рівня C#. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10. У роботі удосконалено методи генерації та проходження лабіринтів на основі штучного інтелекту для застосування у комп'ютерних іграх. Практична цінність отриманих результатів полягає у тому, що розроблене програмне забезпечення дозволяє генерувати зовнішнє середовище у комп'ютерних іграх та керувати рухом ігрових об'єктів для пересування по ньому. Розроблені алгоритми можна використовувати в ігровому 3D та 2D рушії для створення основи різних ігор.

Список літератури

1. Хокинг Дж. Unity в дії. Глава 11 Об'єднання фрагментів в готову гру 267с.
2. Хокинг Дж. Unity в дії. Глава 12 Розгортання ігор на пристроях гравців 298с.
3. Лазарев А.И. Генерация лабиринта алгоритмом эллера в UNITY // Вестник Науки и Творчества. 2017. №8 (20). URL: https://cyberleninka.ru/article/n/generatsiya-labirinta-algoritmom-ellera-v-unity
4. Володченко В.С., Ланцова Д.С., Миронова Т.А. Способы генерации лабиринтов в индустрии компьютерных игр // Вопросы науки и образования. 2019. №31 (81). URL: https://cyberleninka.ru/article/n/sposoby-generatsii-labirintov-v-industrii-kompyuternyh-igr
5. Султанова А.Б. Сравнительный анализ алгоритмов поиска оптимального пути // Бюллетень науки и практики. 2020. №12. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-algoritmov-poiska-optimalnogo-

puti
6. 1. Вирт Н. Алгоритмы и структуры данных. [Текст] / Н. Вирт. М.: Невский Диалект, 2010.
7. 2. Голицына О.Л. Основы алгоритмизации и программирования: учеб. пособие. [Текст] / О.Л. Голицына, И.И. Попов. 3–е изд., перераб. и доп. М.: ФОРУМ, 2015.
8. Burchardt H., Salomon R. Implementation of path planning using genetic algorithms on mobile robots // 2006 IEEE International Conference on Evolutionary Computation. IEEE, 2006. P. 1831-1836. https://doi.org/10.1109/CEC.2006.1688529
9. Niederberger C., Radovic D., Gross M. Generic path planning for real-time applications // Proceedings Computer Graphics International, 2004. IEEE, 2004. P. 299-306. https://doi.org/10.1109/CGI.2004.1309225
10. Грачев В.И., Потапов А.А., Потапов В.А. Фрактальные лабиринты // РЭНСИТ. 2011. №2. URL: https://cyberleninka.ru/article/n/fraktalnye-labirinty.

УДК 004

О. Майданик, магістр гр. КІ-20М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ШИФРУВАННЯ ТРАФІКУ ЧЕРЕЗ АНАЛОГОВИЙ ТРАКТ

У статті представлено результати розробки програмного забезпечення системи шифрування трафіку через аналоговий тракт на основі математичного більярду Сіная. Метою даної роботи є дослідження та програмна реалізація шифрованого трафіку через аналоговий тракт. Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань: огляд існуючих реалізацій трафіку через аналоговий тракт, дослідження методів реалізації трафіку через аналоговий тракт, програмна реалізація шифрованого трафіку через аналоговий тракт. Об'єктом дослідження є процес реалізації алгоритму шифрованого трафіку на основі математичного більярду Сіная. Предметом дослідження є методи реалізації шифрованого трафіку. Методи дослідження базуються на методах розробки програмного забезпечення, методах математичних обчислень, макетування пристрою. Програмне забезпечення розроблено в середовищі STM32CubeIDE 1.1.0 та може використовуватися на мікроконтролерах сімейства STM32.
комп'ютерна інженерія, комп'ютерні системи, шифрування даних, аналоговий тракт, захист інформації

Постановка проблеми. Важливим елементом систем шифрування даних є модуль генерації випадкових чисел для ключів шифрування. Стійкість до атак цього модуля є найважливішим показником безпеки тієї чи іншої системи шифрування. В даний час існує велика кількість методів генерації послідовностей з різним ступенем випадковості. Однак на практиці більшість цих генераторів виробляють послідовності, властивості яких не відповідають вимогам, що ставляться до генерації ключів у криптографії. Часто в числах, які згенеровані за допомогою таких генераторів псевдовипадкових чисел (ГПВЧ) простежуються очевидні закономірності. Також, дуже часто генератори ГПВЧ є найбільш слабким місцем у системах шифрування. Справа в тому, що ГПВЧ використовують різні складні функції для обчислення псевдовипадкових чисел, і послідовності, отримані в результаті роботи таких генераторів, часто є передбачувані та відтворювані, отже не придатні для використання в криптографічних програмах [1].

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні шифрування трафіку через аналоговий тракт.

Мета й завдання дослідження. Метою даної роботи є дослідження та програмна реалізація шифрованого трафіку через аналоговий тракт.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих реалізацій трафіку через аналоговий тракт.

– Дослідження методів реалізації трафіку через аналоговий тракт.

– Програмна реалізація шифрованого трафіку через аналоговий тракт.

Об'єктом дослідження є процес реалізації алгоритму шифрованого трафіку на основі математичного більярду Сіная.

Предметом дослідження є методи реалізації шифрованого трафіку.

Методи дослідження базуються на методах розробки програмного забезпечення, методах математичних обчислень, макетування пристрою.

Виклад основного матеріалу. У даній роботі для вдосконалення процесу шифрування трафіку через аналоговий тракт було вирішено підвищити стійкість модуля генерації ключів шифрування за допомогою використання математичного більярду Сіная у якості ГПВЧ.

У 1976 році відомий математик Сінай Ю.Г. довів, що поведінка більярдної кулі у динамічному більярді, яка визначається детермінованим рівнянням, та поведінка більярдної кулі, яка керується процесом Маркова першого порядку, нерозрізнимі. Оскільки марківський процес першого порядку є ймовірнісним процесом, який залежить тільки від попереднього зіткнення з перепоною, то він є як недетермінованим, так і непередбачуваним.

Запропоновані алгоритми моделювання більярду Сіная мають форму квадрата з колом по центру. Така фігура з окремим тілом в центрі є складною для обчислень та не дає досить великої ентропії. Наведені приклади та алгоритми реалізації гарно ведуть себе при використанні потужних обчислювальних ресурсів. Їх застосування більше підходить до використання на ПК, що обмежує поширення системи для використання на мікроконтролерах [2]. Модель стандартної форми поля прямокутника з внутрішнім колом зображеного на рисунку 1.

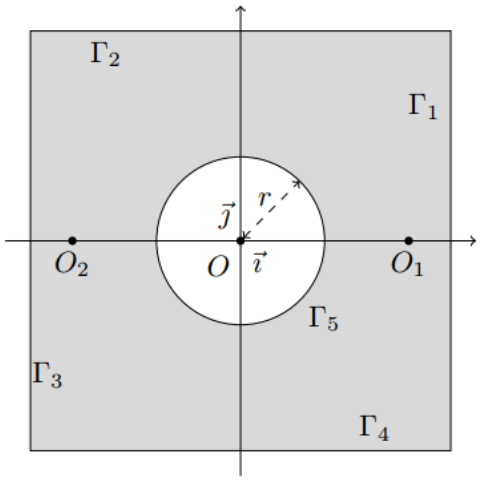


Рис. 1. Більярд Сіная з прямокутним полем та внутрішнім колом

Кращим варіантом для побудови ГПВЧ на основі більярда є форма з опуклими сторонами без додаткового тіла всередині поля, що спрощує алгоритм розрахунку. На рисунку 2 відображено розроблену у даній роботі модель генератора псевдовипадкових чисел на основі більярда Сіная з опуклими сторонами без додаткового тіла всередині.

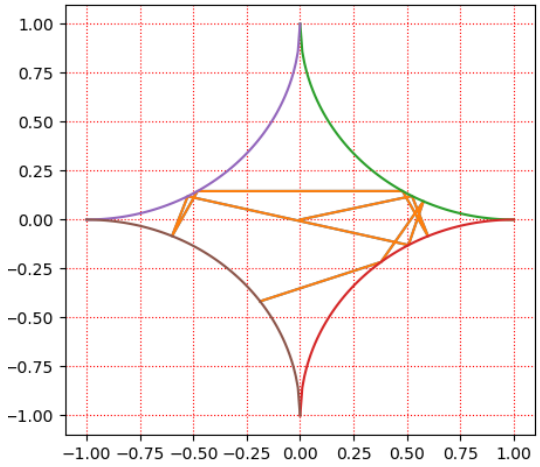


Рис. 2. Модель генератора псевдовипадкових чисел на основі більярда Сіная з опуклими сторонами без додаткового тіла всередині

Системи динамічного більярду виявили добре розвинену хаотичну поведінку. Незважаючи на хороші характеристики, ці системи ще не застосовуються у криптографії. Головною причиною є складність вираження рівняння руху частинок в явній формі [3].

Програмне моделювання руху кулі у більярді Сіная базується на твердженнях, що рух кулі здійснюється без втрати швидкості (тертя відсутнє) та кут падіння дорівнює куту відбиття. Таким чином приймаємо, що рух кулі має швидкості по координатах V_x=cos($\acute{\alpha}$), V_y=sin($\acute{\alpha}$). Звідси V_{x2}+V_{y2}=1. Приймаємо для побудови алгоритму руху кулі наступні вхідні параметри: напрямок руху кулі –V={V_x,V_y} та початкове положення кулі P={P_x, P_y}.

Математична точка рухається по більярду Сіная з постійною швидкістю v. Коли вона досягає кордону, зазнає пружного зіткнення з дзеркальним відображенням відповідно до закону відбиття, кут падіння дорівнює куту відображення відносно $\vec{n}$ нормального вектору в межі зіткнення кордону. Між двома зіткненнями частинка йде прямим шляхом [4].

Генератор заснований на системі хаотичного більярду, тому створюються послідовності, які успадковують хаос і непередбачуваність більярду. Ряд додаткових ітерацій витягується безпосередньо з пароля дозволяє генератору отримати вигоду у вигляді максимуму хаосу, який пропонує більярд.

Кути ініціалізації беруться, використовуючи покажчик, який вказує на різні позиції до тих пір, поки є його загальне покриття.

Математичні точки починають свій рух від центру поля в бік початкового кута, який задається на початку розрахунків. Далі частинка в точці перетину відбивається по закону кутів та рухається до іншої точки перетину. Саме в цих точках перетину її є число, яке генерується як випадкове.

При невеликій різниці початкового кута для різних математичних точок (напр., у проведених у даній роботі експериментах бралася різниця в 0,3 градуси) виникає дуже велика розбіжність у траєкторіях їх руху. Така велика розбіжність пояснюється високою хаотичністю математичного більярду Сіная.

Чутливість до невеликої зміни початкових параметрів є однією з основних властивостей ГПВЧ. Іншими словами, мала різниця в системі повинна викликати велику зміну псевдовипадкових послідовностей. Ця властивість робить генератор високо захищеним від статистичних та диференціальних атак, тому послідовність не може бути зламаною, навіть якщо між ними є невелика різниця початкових параметрів. Генератор заснований на математичному більярді Сіная володіє даною властивістю, а отже є захищеним від статистичних та диференціальних атак.

Перевага даного алгоритму в тому, що його можна використовувати на будь-якій платформі. Тобто можливе використання в портативних пристроях на основі

мікроконтролера. На сьогоднішній день вже існують мікроконтролери з вбудованими блоками криптографії. Вони коштують набагато більше відносно контролерів загального призначення, а також є вже добре вивченими зловмисниками.

На основі даної інформації можна зробити висновок, що дослідження та реалізація алгоритму математичного більярду є актуальною, тому як не потребує значних обчислювальних ресурсів для реалізації та окремих апаратних спеціалізованих блоків. Реалізація алгоритму полягатиме в створенні зв'язку точка-точка (Point to Point). Для цього потрібно одночасно генерувати ряд чисел на обидвох пристроях. Для синхронізації пристроїв можна застосувати годинник реального часу. На рис. 3 зображено фото макетних плат створених для дослідження роботи розробленого алгоритму.

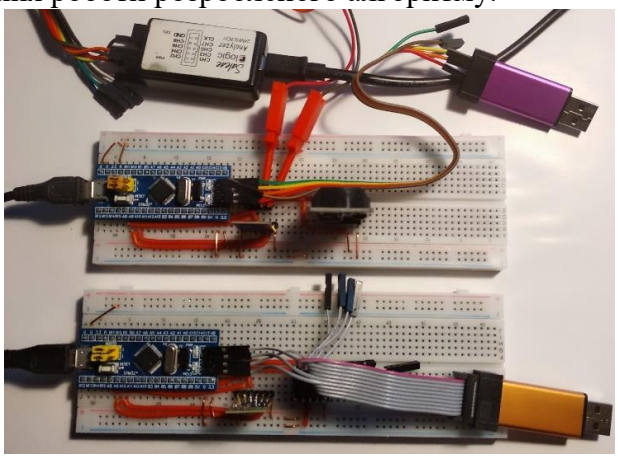


Рис. 3. Фото макетних плат для дослідження роботи алгоритму

Але, якщо потрібна шифрована передача даних на основі старих аналогових комунікацій, можливий варіант передачі даних через модуль, який сприймає аналоговий сигнал відцифровує його через аналогово-цифровий перетворювач (АЦП) шифрує та перетворює в аналоговий сигнал через цифро-аналоговий перетворювач (ЦАП). Функціональна схема модуля з аналоговим вводом та виводом зображена на рис. 4.

Рис. 4. Функціональна схема модуля з аналоговим вводом та виводом

Отже система на основі шифрованої передачі даних може мати будь-який вигляд.

Висновки. В даній роботі було підготовлено програму шифрованої передачі даних та реалізована її апаратна реалізація. З програмної сторони було створено керуючу програму для мікроконтролера, яка повинна налагодити радіообмін даними через радіо модулі загального призначення. Було створено макети, які передбачають обмін даними точка-точка з зв’язком через радіо модулі. Радіо модулі загального призначення на сьогоднішній день наявні в великому асортименті та коштують не дорого. Тому вартість побудованих пристроїв не велика. Але головна перевага – це безпечна шифрована передача даних різними каналами зв’язку. Також можлива адаптація до старих аналогових систем. Впровадження у інші системи можливе у вигляді як заздалегідь запрограмованого мікроконтролера так і у вигляді модуля. У випадку з заздалегідь запрограмованим мікроконтролером користувач просто монтує мікросхему у свою систему. Якщо ж потрібна аналогова передача на вже існуючих системах можливо використання окремого модуля з аналоговим входом та аналоговим виходом адаптованими по стандарту використовуваного обладнання. При

необхідності цифрової передачі можливе використання окремого модуля з мікроконтролером та радіомодулем. Як показали проведені дослідження, використання хаотичного більярда Сіная дуже перспективне в системах передачі даних.

Список літератури

1. Атака на ГПВЧ [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/Атака_на_ГПВЧ.
2. Собінов О.Г. Простий генератор псевдовипадкової послідовності // Інформаційні технології та комп'ютерна інженерія: зб. тез доп. наук.-практ. конф., м. Кіровоград, 4 груд. 2014 р. – Кіровоград: КНТУ, 2014. – С. 184.
3. Ганапольский Е.М. О природе квантового хаоса в рассеивающей бильярдной К-системе // Доповіді Національної академії наук України. - 2012. - № 3. - С. 85-91.
4. Sinai Y.G. Dynamical systems with elastic reflections // Russian Mathematical Surveys. – 1970. - vol. 25, no. 2, pp. 137-189.
5. Гальперин Г.А., Земляков А.Н. Математические бильярды. Бильярдные задачи и смежные вопросыматематики и механики – М.:Наука, 1990. – 288 с.
6. Новости электроники №10 (156), 2016 г. Информационно технический журнал. Учредитель – ООО «КОМПЭЛ».
7. Новости электроники №6 (44), 2012 г. Информационно технический журнал. Учредитель – ООО «КОМПЭЛ».
8. Шифрування даних: криптозахист STM32 [Електронний ресурс]. Режим доступу: https://www.compel.ru/lib/78828.
9. Синай Я. Г. Теория фазовых переходов: строгие результаты – М.: Наука, 1980.
10. STM32. Програмування STM32F103. Option bytes [Електронний ресурс]. Режим доступу: https://blog.avislab.com/stm32-ob/

УДК 004

С. Кірєєв, магістр гр. КІ-20М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ АУДИТУ МЕРЕЖІ ТЕПЛОПОСТАЧАННЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ІОТ

У статті представлено результати розробки програмного забезпечення, яке призначено для реалізації системи аудиту мережі теплопостачання з використанням технології IoT. Метою роботи є створення програмного забезпечення системи аудиту мережі теплопостачання з використанням технології IoT для того, щоб аудитор або власник цієї системи міг бачити якість роботи його системи на кожному з об'єктів, де встановлено обладнання системи теплопостачання. Об'єктом дослідження є процес аудиту мережі теплопостачання. Предметом дослідження є методи аудиту мережі теплопостачання з використанням технології IoT. Результат роботи – програмна реалізація алгоритмів аудиту мережі теплопостачання з використанням технології IoT. Система легко інтегрується в сучасні платформи і взаємодіє з усіма необхідними компонентами. Програма реалізована на мові високого рівня C# з використанням середовищ розробки Microsoft Visual Studio та Unity і призначена для виконання під управлінням багатозадачної операційної системи Windows 10.
комп'ютерна інженерія, комп'ютерні системи, технологія IoT, енергоаудит, мережі теплопостачання

Постановка проблеми. В наш час системи аудиту для різних галузей людської діяльності активно розвиваються, тому що для якісного управління будь чим необхідно проводити спостереження за об'єктом управління. Навіть при автоматичному управлінні системою, потрібні перевірки роботи та її результатів. Для цього існують програми аудиту. За допомогою них аудитор може перевірити ефективність роботи підприємства чи якої небудь системи. Аудит дозволяє своєчасно виявляти помилки в роботі системи та виправити їх. Закономірно, що аудит також потрібно використовувати в системах, які регулюють

подачу теплової енергії у будівлі. Такі програми здатні дати аудитору потрібну кількість інформації для оцінки ефективності роботи тієї чи іншої системи теплопостачання.

Системи аудиту теплопостачання все частіше використовують IoT-технології, адже саме вони дозволяють поєднати фізичні пристрої за допомогою мережі та отримувати дані з різних об’єктів, на яких встановлені системи регулювання подачі теплової енергії. IoT – це концепція мережі фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між зовнішнім середовищем і комп’ютерними системами за допомогою використання стандартних протоколів зв’язку.

Основною концепцією IoT є можливість підключення всіляких пристроїв, які людина може використовувати в повсякденному житті, наприклад, таких як холодильник, кондиціонер, пральна машинка, автомобіль, велосипед і навіть кросівки. Всі ці об'єкти (речі) повинні бути оснащені вбудованими сенсорами, обмінюватися інформацією між собою і виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої технології є системи типу «Розумний будинок». Така система аналізує дані навколишнього середовища і в залежності від показників регулює температуру в приміщенні. Наприклад, зимою регулюється інтенсивність опалення, а літом використовуються механізми відкривання і закривання вікон, завдяки чому провітрюються кімнати, і все це відбувається автоматично без втручання людини.

Програми аудиту різних систем з використанням системи IoT переважно потрібні на підприємствах та в організаціях, де одній людині треба обслуговувати десятки, або навіть сотні пристроїв, що розташовані в різних кабінетах і на різних поверхах будівлі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні аудиту мережі теплопостачання з використанням технології IoT.

Мета й завдання дослідження. Метою роботи є створення програмного забезпечення системи аудиту мережі теплопостачання з використанням технології IoT для того, щоб аудитор або власник цієї системи міг бачити якість роботи його системи на кожному з об’єктів де встановлено обладнання системи теплопостачання.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем аудиту мережі теплопостачання.

– Розробка системи аудиту мережі теплопостачання з використанням технології IoT.

– Випробовування розробленої системи аудиту мережі теплопостачання з використанням технології IoT.

Об’єктом дослідження є процес аудиту мережі теплопостачання.

Предметом дослідження є методи аудиту мережі теплопостачання з використанням технології IoT.

Методи дослідження базуються на методах об’єктно-орієнтованого програмування, теорії інформації та кодування, методах роботи з комп’ютерними системами та мережами, технології Інтернету речей.

Виклад основного матеріалу. У даній роботі було розроблено програмне забезпечення призначене для аудиту та контролю систем мережі теплопостачання, що встановлюються в житлових будівлях. Таким чином, можна здійснювати швидкий доступ до будь-якого з об’єктів, де встановлене відповідне обладнання. У розробленому програмному забезпеченні можна відразу побачити, на якому з об’єктів сталася поломка, адже навіть те, що один з датчиків перестане працювати або буде показувати неправдиву інформацію може означати, що робота на об’єкті порушена.

На рис. 1 показана структурна схема розробленого програмного забезпечення, а саме основні модулі програми:

а) обладнання на об’єкті;

б) головний сервер;

в) програмне забезпечення.

У першому блоці показано функціонування обладнання на об’єкті.

Розглянемо функції та елементи обладнання, які потрібні для отримання показників системі теплопостачання:

– Обладнання для отримання показників представлене датчиками, які прикріплюються хомутами до труб теплопостачання будівлі. Також для зменшення похибки датчиків, вони ізолюються за допомогою скловолокна. Також використовується датчик об’єму води, задача якого отримувати показник кількості води, яка пройшла через будівлю за певний період часу.

– Обладнанням для збору показників з датчиків є універсальний контролер, який збирає інформацію з всіх датчиків, встановлених на об’єкті. Для кожного контролера задається своя окрема IP-адреса. Його наступною дією є генерування HTML-сторінки, до якої розроблене програмне забезпечення може отримати доступ.

– Генерація HTML сторінки для можливості перегляду даних через мережу. Також кожному показнику надається свій тег для того, щоб його можна було відрізнити.

У другому блоці структурної схеми знаходиться сервер, який виконує роль шлюзу, через який можна отримати доступ до показників, що збираються в контролері.

У третьому блоці структурної схеми описується програмне забезпечення та його взаємодія з обладнанням, що знаходиться на об’єкті:

а) Підключення до HTML-сторінки через головний сервер.

Для цього використовується IP-адреса сторінки а саме внутрішня адреса, що записана на сервері.

б) Пошук даних за тегами.

До кожного елемента в програмі, що показує значення показника температури або об’єму води в мережі теплопостачання будівлі, прив’язаний тег, що відповідає за конкретний показник. Це дозволяє отримати потрібне значення в програмі та чітко бачити до чого воно відноситься.

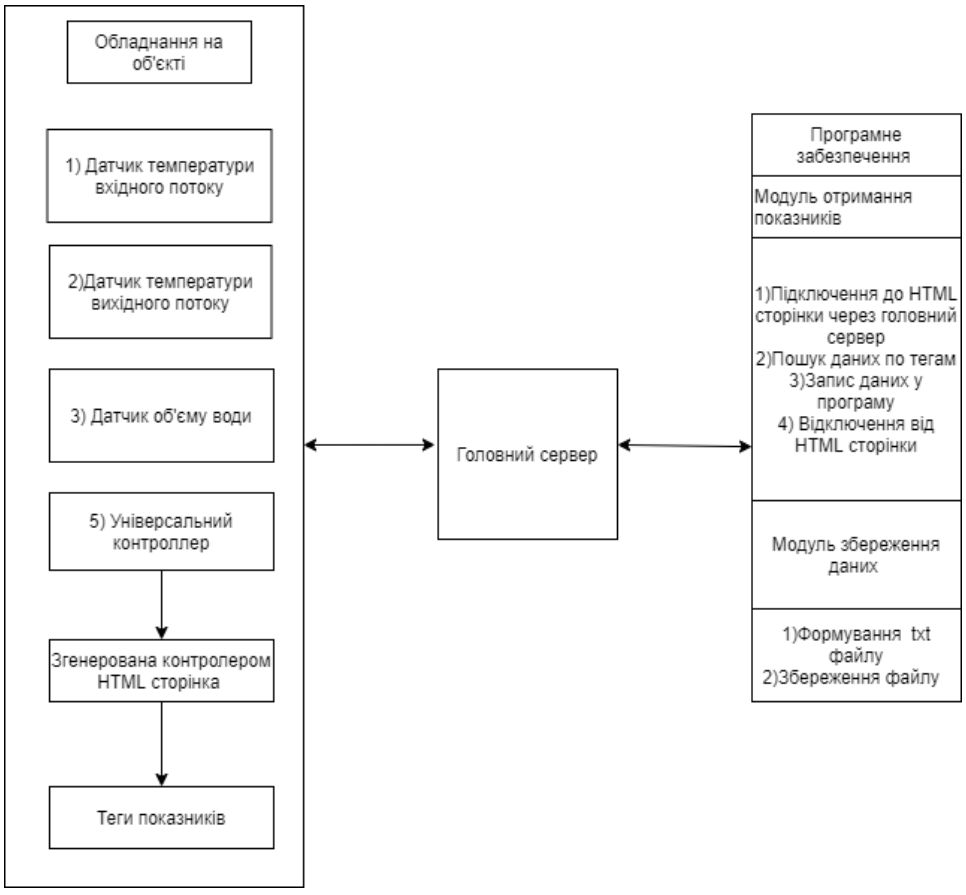


Рис. 1 – Структурна схема розроблюваної системи

Розроблене програмне забезпечення служить універсальним інструментом в руках програміста або системного адміністратора. При повному або частковому встановленні ліцензійного програмного забезпечення на одній або декількох клієнтських машинах, що обслуговуються, при певних ситуаціях, таких як: збій операційної системи; крах апаратної частини комп'ютера; оновлення версії ліцензійного програмного забезпечення або необдумані дії користувача. В такому разі дані, що були отримані, не будуть втрачені адже вони будуть продубльовані в пам’яті самого контролера.

Програма дозволяє своєчасно виявляти несправності на об’єктах. Розроблене програмне забезпечення буде корисне всім аудиторам різних організацій, в управлінні яких є велика кількість об’єктів, а також може допомогти аудиторам, що мають перевіряти якість роботи системи.

До особливостей розробленого програмного забезпечення можна віднести можливість перегляду кількості води, що пройшла за певний проміжок часу.

Збір інформації про систему повністю автоматизований. Користувачу залишиться тільки виконувати необхідні дії в заданій послідовності.

Перерахуємо можливості розробленого програмного забезпечення:

1. Забезпечує швидкий доступ до різних об’єктів;
2. Використовується для створення записів про зміну температур та інших показників;
3. Можливість швидкого запуску, тому що не потребує інсталяції;
4. Не вимоглива до конфігурації комп'ютера;
5. Простота в роботі (обігу);
6. Високий рівень захисту від перехоплень пакетів з даними;
7. Автоматична функція перевірки підключення до сервера;
8. Стабільна робота у всіх версіях MS Windows;
9. Простота і наочність роботи в програмі.

Розроблене в ході роботи програмне забезпечення можна використовувати при налаштуванні програмного середовища будь-яких ПК під управлінням ОС Windows. Така система може бути корисною в багатьох сферах використання сучасних комп’ютерних систем. Розроблене програмне забезпечення дозволяє швидко та ефективно провести аудит системи теплопостачання та порівняти отримані результати з попередніми.

Використані в ході роботи над проектом алгоритми та методи програмування, а також програмний код з коментарями і пояснювальна записка будуть корисні починаючим програмістам та проектувальникам комп’ютерних систем на базі технології IoT.

Висновки. У статті наводяться результати розробки програмного забезпечення системи аудиту мережі теплопостачання з використанням технології IOT, що призначене для перевірки стану систем мереж теплопостачання. Рішення даного завдання полягало у вирішенні наступних задач: був проведений огляд існуючих систем аудиту мереж теплопостачання, розроблено систему аудиту мережі теплопостачання з використанням технології IoT, проведено випробовування розробленої системи аудиту мережі теплопостачання з використанням технології IoT. Програма реалізована на мові високого рівня C# з використанням середовищ розробки Microsoft Visual Studio та Unity. Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10. Для підвищення рівня безпеки розробленого програмного забезпечення запропоновано застосовувати два рівні захисту програми, верхній рівень – вікно введення пароля на вхід в програмне забезпечення, другий рівень – обов’язкова наявність сертифікатів та приватних ключів для доступу на об’єкти. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення та масштабування.

Список літератури

1. Корчемний М. О. Енергозбереження в агропромисловому комплексі / М. О. Корчемний, В. М. Федорейко,

В. А. Щербань. – Тернопіль : Підручники і посібники, 2001. – 984 с.
2. Научно-методические принципы энергосбережения и энергоаудита: научное и учебно-методическое пособие: В 3-х томах. Том: Научно-методические принципы энергоаудита и энергоменеджмента / Т.Е. Троицкий-Марков, О.Н. Будадин, С.А. Михайлов, А.И. Потапов. М.: Наука, 2005. 537 с.
3. Щелоков Я.М. Энергетический анализ хозяйственной деятельности: учебно-методическое издание / Я.М. Щелоков. Екатеринбург: РУО АИН им. А.М. Прохорова, 2009. 388 с.
4. Анисимова Т.Ю. Особенности построения энергетического менеджмента на промышленных предприятиях / Т.Ю. Анисимова // Известия ВУЗов. Проблемы энергетики. 2007. № 3−4. С. 94−99.
5. Данилов Н.И. Основы энергосбережения: учеб. – 2-е изд., доп. и перераб. / Н.И. Данилов, Я.М. Щелоков; под общ. ред. Н.И. Данилова. Екатеринбург: Изд. дом «Автограф», 2010. 528 с.
6. Павенчик В.В. Основы энергосбережения: практикум / В.В. Павенчик, А.Н. Ковалев, М.В. Самойлов. Минск: БГЭУ. 2007. 195 с.
7. Интернет вещей / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков, М. Ю. Самсонов; под ред. А. В. Рослякова. Самара: ПГУТИ, ООО «Издательство Ас Гард», 2014. 340 с.
8. Щербинина М.Ю., Стефанова Н.А. Концепция интернет вещей // КЭ. 2016. №11. URL: https://cyberleninka.ru/article/n/kontseptsiya-internet-veschey
9. Куприяновский В.П., Шнепс-Шнеппе М.А., Намиот Д.Е., Селезнев С.П., Синягов С.А., Куприяновская Ю.В. Веб Вещей и Интернет Вещей в цифровой экономике // International Journal of Open Information Technologies. 2017. №5. URL: https://cyberleninka.ru/article/n/veb-veschey-i-internet-veschey-v-tsifrovoy-ekonomike
10. Куприяновский В.П., Намиот Д.Е., Дрожжинов В.И., Куприяновская Ю.В., Иванов М.О. Интернет Вещей на промышленных предприятиях // International Journal of Open Information Technologies. 2016. №12. URL: https://cyberleninka.ru/article/n/internet-veschey-na-promyshlennyh-predpriyatiyah

УДК 621.43.06

О. Гальченко, магістр, група АТ-20М
Центральноукраїнський національний технічний університет

АНАЛІЗ ТЕХНОЛОГІЙ ТА МАТЕРІАЛІВ ВИГОТОВЛЕННЯ БЛОКІВ ЦИЛІНДРІВ АВТОМОБІЛЬНИХ ДВЗ

В роботі розглянуто основні технології виготовлення сучасних блоків циліндрів автомобільних двигунів. Виявлено перспективні технології та матеріали виготовлення блоків, виконано порівняльний аналіз різних матеріалів та технологічних схем виготовлення блоків. Встановлено, що на сьогоднішній день значна частина блоків циліндрів виконуються за схемою «алюмінієвий блок – залита чавуна гільза». Для багатьох двигунів з такими блоками виробником не передбачено виконання капітального ремонту. Відновлення такого блоку можливо шляхом постановки сухих гільз, однак необхідно вивчити зміну теплопередачі, що виникає при такій технології ремонту.
блок циліндрів, автомобільний двигун, ремонт

Постановка проблеми. Останнім часом на автомобілях малої вантажопідйомності зарубіжного виробництва все частіше встановлюються двигуни внутрішнього згоряння (ДВЗ), блоки циліндрів яких виготовлені з алюмінієвих сплавів. Для одних моделей двигунів виробниками передбачена можливість відновлення зношених поверхонь циліндрів, для інших немає. Ремонт блоків циліндрів дозволяє не тільки відновлювати працездатність ДВС, а й використовувати їх залишковий ресурс. В результаті забезпечується економія матеріальних, енергетичних і трудових витрат.

Технологія відновлення блоків циліндрів з алюмінієвих сплавів постановкою ремонтних чавунних гільз все частіше застосовується в ремонтній практиці, але її широке поширення стримується відсутністю обґрунтованих рекомендацій щодо вибору значень технологічних параметрів з'єднання «гільза-блок циліндрів».

Для надання рекомендацій з технології ремонту алюмінієвих блоків циліндрів необхідно детально вивчити технологічні особливості їх виготовлення.

Аналіз останніх досліджень та публікацій. Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-7].

Мета і завдання досліджень. *Метою роботи* – пошук шляхів відновлення алюмінієвих блоків циліндрів з залитими чавунними гільзами постановкою ремонтних сухих гільз.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити існуючі технології підвищення ефективності припрацювання деталей автомобільних двигунів;

2. дослідити існуючі припрацювальні склади, виявити їх переваги та недоліки.

Об'єкт дослідження – блоки циліндрів автомобільних малолітражних двигунів, виготовлені з алюмінієвих сплавів.

Предмет дослідження – технологічні методи ремонту блоків циліндрів із залитими чавунними гільзами.

Методи досліджень базуються на теоретичному аналізі технологій та матеріалів виготовлення алюмінієвих блоків циліндрів та особливостей їх ремонту.

Блок циліндрів двигуна внутрішнього згоряння (блок) являє собою литу конструкцію складної конфігурації, всередині і зовні якої в заданому положенні розташовуються деталі і складальні одиниці двигуна. Блок сприймає навантаження від обертових і поступально рухомих деталей.

Блоки циліндрів виготовляють з сірого, ковкого або модифікованого чавуну, алюмінієвих сплавів [1-3] методами вільного лиття, лиття під низьким тиском (0,2-0,5 бар), лиття під високим тиском (700-1000 бар), пресування. В даний час все більшого поширення набувають бензинові і дизельні двигуни внутрішнього згоряння (ДВЗ), блоки яких виготовлені з алюмінієвих сплавів [2, 3].

Широке застосування алюмінієвих сплавів для виготовлення блоків циліндрів обумовлено їх значно меншою питомою вагою і більш високою теплопровідністю в порівнянні з чавуном [4, 5; 6]. Завдяки цьому досягається зниження маси двигуна на 40-50% і його більш швидке і рівномірне прогрівання при запуску. Висока теплопровідність матеріалу блоку дозволяє значно знизити обсяг охолоджуючої рідини в системі охолодження (глибина сорочки охолодження блоків сучасних ДВЗ становить 0,3-0,5 довжини циліндра) і розвантажити найбільш теплонавантажені зони блоку [3]. Хороші ливарні властивості, оброблюваність і корозійна стійкість алюмінієвих сплавів також є причинами їх широкого застосування для виготовлення блоків циліндрів.

Поряд з перевагами алюмінієві сплави мають і суттєві недоліки: великий коефіцієнт лінійного розширення, порівняно низькі зносостійкість і механічна міцність, що вимагає застосування ряду конструкторсько-технологічних рішень для забезпечення необхідної жорсткості конструкції і зносостійкості робочих поверхонь.

Блоки циліндрів можуть мати рядне, V-подібне, V-подібно-рядне (VR) і оппозитне розташування циліндрів. При цьому кількість циліндрів більшості автомобільних ДВЗ становить від чотирьох до шести. При рядном розташуванні циліндрів блоки мають найбільш просту конструкцію, проте робочий об'єм таких двигунів лімітований, що пов'язано з певними обмеженнями по довжині блоку і кількості циліндрів. У сучасному автомобільному двигунобудуванні спостерігаються тенденції зменшення діаметра і збільшення кількості циліндрів. Так, все більшого поширення в сучасній техніці знаходять V-подібні і VR конструкції блоків циліндрів. У VR конструкції блоку (розробник фірма Volkswagen) циліндри розташовані під кутом 15° в шаховому порядку. При цьому блок циліндрів має одну площину прилягання до головки блоку циліндрів (ГБЦ), а двигун, відповідно, одну загальну головку блоку циліндрів. В результаті подібні багатоциліндрові конструкції мають порівняно невеликі габаритні розміри.

По конфігурації поверхні прилягання блоку до головки блоку циліндрів (ГБЦ) і конструкції циліндрів, блоки циліндрів сучасних ДВЗ істотно відрізняються один від одного. Розглянемо принципові відмінності конструкцій блоків, їх переваги та недоліки.

Спочатку блоки циліндрів з алюмінієвих сплавів виготовляли з верхньою з'єднувальною плитою, по аналогії з чавунними блоками. Пізніше, з розвитком технологій з'явилася конфігурація блоку без верхньої з'єднувальною плити, що істотно спростило технологію виготовлення блоків [9; 10]. В даний час обидві ці конфігурації (з верхньої з'єднувальною плитою і без неї) мають широке поширення, причому кожна з них має свої переваги і недоліки.

В блоках з верхньою з'єднувальною плитою краще здійснюється ущільнення ГБЦ. У блоків без верхньої з'єднувальною плити циліндри не пов'язані із зовнішніми стінками блоку і можуть розташовуватися окремо один від одного або бути разом відлиті. В цьому випадку краще відбувається охолодження верхньої, найбільш теплонавантаженої частини циліндра. При такій конфігурації блоку складніше здійснюється ущільнення ГБЦ і циліндри більш схильні до температурних деформацій.

По конструкції циліндрів можна виділити наступні конфігурації.

Блок з «мокрими» чавунними гільзами циліндрів. Подібна конструкція почала застосовуватися ще в 30-х роках 20 століття [9; 10] і знаходить своє застосування по теперішній час: ЗМЗ-402 і модифікації, Peugeot, Renault, Citroen, Fiat і інші.

Перевагою такої конструкції є збереження позитивних властивостей блоків з алюмінієвих сплавів (менша маса, кращі теплопровідні властивості) і чавунних гільз циліндрів (класичні пари тертя: «поршень-циліндр» і «поршневе кільце-циліндр», традиційна технологія обробки гільз циліндрів).

Блоки з верхньої з'єднувальною плитою мають велику жорсткість верхньої частини, менш схильні до температурних деформацій циліндрів.

Блок циліндрів може виготовлятися з чавуну марок СЧ 24, СЧ-25 СЧ-30, СЧ-35 або алюмінієвого сплаву АЛ-4, АЛ-7, АЛ-9.

Існують наступні технологічні схеми виготовлення блоків

1. Чавунний або алюмінієвий блок і гільза виготовляються як окремі деталі, гільза запресовується у блок при складанні двигуна
2. Чавунний блок виготовляється разом з гільзою як одна монолітна деталь.
3. Блок з алюмінієвого або магнієвого сплаву, виготовлений заливанням чавунної гільзи.
4. Блок з алюмінієвого сплаву з гільзою відлитою разом з блоком (низький вміст кремнію) з тонким захисним покриттям з хрому або нікелю (нікосіл).
5. Монолітний блок з алюмінієвого сплаву з високим вмістом кремнію (технологія алюсіл);
6. Блок з низько кремнієвого алюмінієвого сплаву, виготовлений заливанням алюмінієвої висококремнієвої гільзи (технологія локасіл).

Якщо гільза виготовляється окремо від блоку та встановлюється при складанні блока, то такі гільзи циліндрів виготовляють з чавунів МСЧ-28, СЧ-21 та інш. Твердість таких цих чавунів залежить знаходиться в межах НВ від 170 до 255 до загартування і HRC 39-47 після загартування.

Заготовки для гільз отримують відцентровим відливанням в чавунні форми, а також в нерухомі земляні або оболонкові форми.

Основний недолік чавунних блоків циліндрів - це їх велика питома вага. Щоб поліпшити динаміку автомобіля світові виробники шукають шляхи зменшення ваги за рахунок його складових, в тому числі і двигуна. Сьогодні у багатьох сучасних автомобілях застосовується алюмінієвий блок циліндрів двигуна. Алюміній, крім своєї невеликої ваги, має ряд інших переваг перед чавуном.

Алюмінієві блоки циліндрів витримують температурний режим до + 150-200 °С. Теплопровідність алюмінієвих сплавів в три рази вище чавунних, це сприяє більш

ефективній роботі системи охолодження двигуна. Дуже важливо підібрати алюмінієвий сплав для блоку циліндрів. Він повинен відповідати багатьом технічним вимогам, серед них:

- низька вартість;
- відмінні ливарні властивості;
- гарна обробка різанням.
- несприйнятливість до підвищених температур.

Вибирати алюмінієвий ливарний сплав необхідно на етапі проектування блоку циліндрів.

Висновки. На теперішній час використовуються різні конструктивні та технологічні варіанти виготовлення блоків циліндрів двигунів. Найбільш поширеною технологією є відливання алюмінієвого блоку з одночасним заливанням чавунної гільзи. Для таких блоків деякі виробники не передбачають виконання капітального ремонту. В умовах нашої країни існує необхідність в розробці технології ремонту даних блоків шляхом постановки сухої ремонтної гільзи.

При відновленні блоків циліндрів з алюмінієвих сплавів постановкою ремонтних чавунних гільз вноситься суттєва зміна в конструкцію циліндрів, змінюється їх теплова провідність і жорсткість. До сих пір недослідженим залишається питання про те, якою мірою дана технологія впливає на експлуатаційно-технологічні характеристики відновлених блоків циліндрів.

Список літератури

1. Крутилин А. Н., Курбатов М. И., Курбатова М. И. Условия работы и основные требования, предъявляемые к материалу гильз блока цилиндров //Литьё и металлургия. – 2005. – №. 2-1 (34).
2. Schäfe A. Ремонт алюминиевых блоков цилиндров : справочник. Германия, 2006. 100 с.
3. Rohatgi P. Cast aluminum-matrix composites for automotive applications //Jom. – 1991. – Т. 43. – №. 4. – С. 10-15.
4. Новиков, А.Н. Технологические основы восстановления и упрочнения деталей сельскохозяйственной техники из алюминиевых сплавов электрохимическими способами [Текст] / А.Н. Новиков. – Орёл: ОрёлГАУ, 2001. - 233 с.
5. Кавтарадзе Р.З. Локальный теплообмен в поршневых двигателях: Учеб. пособие для вузов. – 2 изд. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2007. – 472 с.
6. Дударева Н.Ю., Мусин Н.Х. и др. Исследование износостойкости алюминиевых гильз цилиндров с модифицированной рабочей поверхностью // XIII КОРОЛЁВСКИЕ ЧТЕНИЯ Международная молодёжная научная конференция, сборник трудов. Том. 1 / СГАУ имени ак. С.П. Королёва (национальный исследовательский университет). – Самара, 2015. – с.224-225.
7. Завороткин Е.А. Особенности конструкций алюминиевых блоков цилиндров современных ДВС // Известия Санкт-Петербургского государственного аграрного университета №19. - СПб.: СПбГАУ, 2010. -С. 317-322.
8. Антипов А.И., Завороткин Е.А. Исследование дефектов цилиндров алюминиевых блоков цилиндров современных ДВС // Труды всероссийского научно-исследовательского технологического института ремонта и эксплуатации машинно-тракторного парка (ГНУ ГОСНИТИ) №107. -М.: ГНУ ГОСНИТИ, 2011. - С. 65-68.

УДК 621.791.927.5

Д. Герасимчук, магістр гр. МЗ-20М
Центральноукраїнський національний технічний університет

ОГЛЯД МЕТОДІВ ВІДНОВЛЕННЯ РОЗПОДІЛЬНИХ ВАЛІВ АВТОТРАКТОРНИХ ДВИГУНІВ

В роботі виконано аналіз умов роботи розподільних валів автотракторних двигунів, виявлено основні дефекти, причини їх виникнення та вплив на експлуатаційні показники роботи. Встановлено, що для відновлення профілю кулачків розподільних валів застосовуються способи електродугового наплавлення в захисному середовищі CO2, вібродугового наплавлення та методи напилювання. Проаналізовано переваги та недоліки існуючих методів відновлення.

Проведений аналіз способів відновлення розподільних валів, а також умов роботи пари кулачок-штовхач, дає можливість стверджувати, що в даний час немає універсального способу відновлення, який міг би одночасно поєднати в собі високу продуктивність, економічність, а також можливість забезпечити високу зносостійкість кулачка і сполученого з ним штовхача. Тому, залишається актуальною проблема удосконалення існуючих та пошук нових методів відновлення робочих поверхонь розподільних валів.
розподільний вал, відновлення деталей, плазмове напилювання

Постановка проблеми. Проведений аналіз показав, що 85-90% деталей машин виходить з ладу внаслідок зношування, при цьому 75% вибраковують деталей є ремонтопридатності. Витрати на запасні частини досягають 60% від собівартості ремонту машин. Відновлені деталі в 1,5-2,5 рази дешевше нових деталей, а по ресурсу, як правило, не поступаються їм.

Однією з найбільш відповідальних деталей двигуна автомобіля є розподільний вал. Дана деталь працює при високих навантаженнях та в умовах граничного мащення. Відновлення розподільних валів – складний та дорогий процес. Отже, розробка ефективних технологій відновлення валів є актуальною проблемою ремонтного виробництва.

Аналіз останніх досліджень та публікацій. Вивченню питань відновлення кулачків розподільних валів присвячено багато науково-дослідних робіт відомих вчених: В.А. Наливкіна, К.А. Ачкасова, Ш.Ш. Джанілідзе, В. Поляченко, В.Н. Бугаєва. С.С. Некрасова, В. Плешакова, І.Є. Ульмана. В.С. Дорофєєва, В.П. Силуянова, і ін.

Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-7].

Мета і завдання досліджень. *Метою роботи* є дослідження процесів зношування розподільних валів автотракторних двигунів та аналіз ефективності існуючих технологічних методів відновлення.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити причини зношування розподільних валів;
2. виконати аналіз ефективності існуючих методів відновлення.

Об'єкт дослідження – процеси відновлення розподільних валів автотракторних двигунів.

Предмет дослідження – закономірності зміни фізико-механічних властивостей розподільних валів автотракторних двигунів в процесі експлуатації.

Методи досліджень базуються на теоретичному аналізі причин виходу з ладу розподільних валів.

Розподільчий вал є важливою частиною механізму газорозподілу двигуна внутрішнього згоряння (ДВЗ) і призначений для передачі руху від колінчастого вала двигуна до клапанів.

Надійна і економічна робота системи газорозподілу двигуна внутрішнього згоряння багато в чому залежить від ресурсу розподільного вала, що визначається в першу чергу зносостійкість найбільш навантажених його робочих поверхонь - кулачків. Механізм взаємодії штовхача з кулачком розподільного валу досить складний, найбільший вплив на зношування цієї пари роблять наступні фактори [4]: зовнішній механічний вплив, що характеризується швидкістю відносного переміщення і навантаженням; температура тертя і температурний градієнт; фізико-механічні властивості сполучених пар і навколишнього проміжного середовища (модуль пружності, коефіцієнт об'ємного розширення, макро- і мікротвердість, межа плинності, термообробка і т.д.); макро- і геометрія поверхні тертя; вид тертя; тривалість і шлях тертя; властивості мастильного матеріалу. Дія цих чинників призводить до зносу кулачковою пари, і, як наслідок, до зниження ефективності роботи двигуна внутрішнього згоряння.

Розподільчий вал відноситься до нежорстких деталей. Однією з головних проблем, що виникають при виготовленні та ремонті розподільних валів, є те. що цей вал викривляється не лише в процесі обробки, але і після її завершення, тобто вал. що відповідав усім вимогам і минулий технологічний контроль, через певний інтервал часу деформується. Оскільки вал в двигуні встановлюється на опори, подібне викривлення валу призводить до збільшення вібрацій, навантажень на опори, їх швидкого зносу і, як наслідок, до зниження якості роботи двигуна.

Розподільчий вал виготовляють штампуванням з вуглецевих або легованих сталей. Поверхні опорних шийок і кулачків вала піддані загартуванню струмами високої частоти на глибину від 2 до 5 мм до твердості HRC 54-63. Ширина загартованої зони циліндричної частини кулачка не менше 17 мм і розташована симетрично щодо країв кулачка.

Необхідна твердість: опорних шийок - 55 ... 63 HRC, кулачків - не менше 55 HRC.

В процесі експлуатації на розподільний вал з конструктивно закладеної малою жорсткістю впливають сили тертя, вібрація, знакозмінні навантаження, середовище та ін., Внаслідок чого виникають дефекти вала: знос кулачків, опорних шийок і збільшення прогину. Знос кулачків розподільного вала по висоті викликає більш пізню відкривання і більш раннє закривання клапанів, що призводить, наприклад, до зменшення тривалості відкритого стану впускних клапанів, до погіршення наповнення циліндрів і зниження потужності двигуна. Знос опорних шийок призводить до появи стукотів в механізмі приводу клапанів і може привести до падіння тиску масла в системі змащення з усіма витікаючими наслідками [1].

Основною причиною деформацій є перерозподіл технологічних залишкових напруг і спадкових напруг заготовки при видаленні припусків і напруг від температурно-силового впливу обробного інструменту, причому, як правило, напруги перерозподіляються нерівномірно.

При ремонті деталей газорозподільного механізму двигуна внутрішнього згоряння певну складність являє відновлення розподільного вала.

Існуючі в даний час способи відновлення розподільних валів не знаходять широке застосування в силу невідповідності техніко-економічним критеріям сучасного машинобудування. Тому, актуальним завданням є пошук нових способів і технологій відновлення, що дозволяють підвищити ефективність ремонту, а саме знизити трудомісткість і собівартість, підвищити експлуатаційний ресурс відновленого вала, забезпечити екологічну чистоту процесу відновлення [1,2].

Головною вимогою до способів відновлення є їх універсальність, а саме поєднання в собі високої продуктивності, економічності і екологічності, а також забезпечення високої зносостійкості не тільки кулачка, а й сполученого з ним штовхача [2].

При ремонті гранично зношених валів поряд із забезпеченням зносостійкості кулачків стоїть складне завдання відновлення їх первісного профілю. В ремонті розподільних валів набули поширення два способи відновлення кулачків: його вершини і всього профілю.

Відомий спосіб відновлення зношених вершин кулачків, що містить операції наплавлення сталевими електродами, термічної обробки для зняття напружень, правки, зміцнюючої термообробки азотування, додаткової правки і шліфування. Валики наплавляють на вершину кулачка з урахуванням величини зносу. Недоліком технології є висока

трудомісткість і енергоємність внаслідок наявності двох операцій термообробки. Крім цього, технологія призначена тільки для розподільних валів, що мають знос вершин всіх кулачків [5].

До способів відновлення вершин кулачків в формує оснащенні можна віднести спосіб наплавлення порошковим дротом [6], спосіб електроконтактного приварювання порошків [7] і спосіб індукційного наплавлення [8]. Сутність цих способів полягає в тому, що безпосередньо на зношену або попередньо прошліфувати вершину кулачка наносять шар металу, при одночасному використанні формує вершину оснастки. Як наплавлювальних сплавів, при електроконтактного приварювання і індукційної наплавленні використовують порошки на основі заліза і нікелю. Загальним недоліком для цих способів є підвищена трудомісткість робіт і низька стійкість формує вершину оснастки.

При відновленні всього профілю кулачків розподільних валів застосовуються способи електродугового наплавлення в захисному середовищі CO_2, вібродугового наплавлення і ін. Способи електродугового наплавлення не знаходять широкого поширення з наступних причин: великі припуски на механічну обробку, наявність дефектів в наплавлених поверхнях, труднощі повторного відновлення раніше наплавлених цим способом поверхонь [9]. Вібродугове наплавлення в свою чергу не забезпечує рівномірної твердості по всій наплавленій поверхні, тому для вирівнювання і підвищення твердості на кулачках проводять їх термічну обробку за допомогою струмів високої частоти. Недоліком технології є також велика товщина наплавленого шару, що становить 2 мм [10].

Напилювання валів виконують самофлюсуючими порошками. Поверхня кулачка перед напилюванням проходить спеціальну підготовку. Після напилювання кулачків з метою підвищення зчеплення основного і напиленого матеріалів виконують оплавлення покриття полум'ям пальника або струмами високої частоти. При плазмовому напилюванні оплавлення кулачків і інших поверхонь роблять в печі. Недоліком цих технологій є необхідність ретельної підготовки напилюваних поверхонь, а також наявність додаткової операції оплавлення, що збільшує трудомісткість технологічного процесу. Крім цього нераціональні втрати порошку досягають 30% [13].

Менша кількість операцій містить технологія детонаційного напилювання кулачків. Вона забезпечує зчеплення основного і напилюваного матеріалу в межах 50 - 170 МПа, значно більшу густину покриття. ніж при газополуменевому і плазмовому напилюванні [14]. Однак високочастотний шум, що виникає при детонаційному, як і при плазмовому напилюванні вимагає створення спеціальних боксів з шумопоглинаючими стінами.

Найбільш широкого поширення набула технологія відновлення кулачків газопламеневого наплавленням [15]. Процес складається з операцій підготовки поверхонь під наплавлення, наплавлення, редагування, шліфування.

Ця технологія може бути використана як при наплавленні всього профілю, так і при наплавленні вершини кулачка. До недоліків технології відносяться: відпускання незношених кулачків. розташованих поруч з наплавляються, а також велика радіальна деформація вала, що досягає 1.5 - 1,8 мм.

Провівши аналіз способів відновлення розподільних валів, їх переваг і недоліків, а також умов роботи пари кулачок - штовхач, можна стверджувати, що в даний час немає універсального способу відновлення, який міг би одночасно поєднати в собі високу продуктивність, економічність, а також можливість забезпечити високу зносостійкість кулачка і сполученого з ним штовхача.

Вимога забезпечення високої зносостійкості пари кулачок - штовхач набуває особливої актуальності у зв'язку з тим, що в даний час зростає енергонасиченість ДВЗ за рахунок підвищення частоти обертання колінчастого вала. При цьому на клапан, з метою гасіння інерційних сил, встановлюють більш потужні пружини, які при малих обертах розподільного вала ведуть до зростання контактних напружень в кулачку і штовхачі, що негативно позначається на їх зносостійкості.

У зв'язку з цим актуальним завданням є пошук нових універсальних технології відновлення розподільних валів транспортних двигунів, що дозволяють підвищити експлуатаційний ресурс відновленого вала.

Висновки. Аналіз способів відновлення розподільних валів, їх переваг і недоліків, а також умов роботи робочих поверхонь, показав, що в даний час немає універсального способу відновлення, який міг би одночасно поєднати в собі високу продуктивність, економічність, а також можливість забезпечити високу зносостійкість кулачка і сполученого з ним штовхача.

Існуючі в даний час способи відновлення розподільних валів не знаходять широке застосування в силу невідповідності техніко-економічним критеріям сучасного машинобудування. Тому, актуальним завданням є пошук нових способів і технологій відновлення, що дозволяють підвищити ефективність ремонту, а саме знизити трудомісткість і собівартість, підвищити експлуатаційний ресурс відновленого вала, забезпечити екологічну чистоту процесу відновлення.

Список літератури

1. Орлин, А.С. Двигатели внутреннего сгорания. Устройство и работа поршневых и комбинированных двигателей [Текст] / А.С. Орлин, М.Г. Круглов. - М.: Машиностроение, 1990. - 284 с.
2. Шиповалов, А. Н. Технология восстановления кулачков распределительных валов плазменной наплавкой [Текст]: автореф. дне. ... канд. техн, наук: 05.20.03 / А.Н. Шиповалов; [Российский государственный аграрный заочный ун-т]. — М., 2010. — 18 с.
3. Непомилуев, В.В. Методика проектирования технологических процессов обработки распределительных валов [Текст] / В.В. Непомилуев, Е.Е. Цедейко // Авиационно-космическая техника и технология. — 2003. — Т.40, №5. — С. 131—134.
4. Браун, Э.Д. Моделирование трения и изнашивания в машинах [Текст] / Э.Д. Браун, Ю.А. Евдокимов, А.В. Чигинадзе. - М.: Машиностроение, 1982. - 191 с.
5. А. с. 1371983 СССР, МКИ С 21 Д 9/30. Способ восстановления чугунных распределительных валов [Текст] / А.К. Тихонов, В.И. Копыл, Л.Я. Кузьменко, В.В. Чотов, А.Б. Чумиков (СССР). — № 3705976/22-02; заявл. 13.03.84; опубл. 07.02.88, Бюл. №5.-5 с.
6. Джанилидзе, Ш.Ш. Исследование и разработка технологии восстановления кулачков распределительных валов двигателей ЗМЗ - 53 [Текст] / Ш.Ш. Джанилидзе. Н.А. Дьяченко, З.Б. Ермакова // Техническое обслуживание и ремонт автомобилей: Сб. трудов. - М.: Транспорт, 1977.-С. 111-121.
7. Восстановление кулачков распределительных валов и толкателей клапанов индукционной наплавкой износостойкими порошками [Текст]: тез. докл. науч.-техн. конф, стран-членов СЭВ "Ремдеталь — 88", Пятигорск, окт., 1988. — М.: АгроНИИТЭИИТО, 1988. — Ч. 2. — С. 39-40.
8. Глинский, М.А. Методика проектирования технологических процессов нанесения плазменных покрытий на основе применения безразмерных ком-плексных критериев / М. А. Глинский, И. Н. Кравченко, Е. М. Бобряшов // Научно-технический журнал: Ремонт. Восстановление. Модернизация. – 2011. – № 5. – С. 32–34.
9. Глинский, М.А. Исследование напряженно-деформированного состоя-ния наплавленных покрытий деталей, восстановленных плазменными методами / М. А. Глинский, И. Н. Кравченко, В. Ю. Гладков // Научно-технический журнал: Ремонт. Восстановление. Модернизация. – 2011. – № 6. – С. 2–8.
10. Повышение износостойкости и ресурса рабочих органов почвообраба-тывающих машин / Ю. А. Кузнецов, И. Н. Кравченко, М. А. Глинский, В. В. Гончаренко // Научно-технический журнал: Ремонт. Восстановление. Модернизация. – 2017. – № 9. – С. 14–17.
11. Разработка технологии нанесения плазменных покрытий многофункци-онального назначения / И. Н. Кравченко, М. А. Глинский, Ю. А. Шамарин, Т. А. Чеха // Научный журнал: Вестник ФГОУ ВПО «Московский государ-ственный агроинженерный университет имени В.П. Горячкина». – 2017. – № 6 (82). – С. 63–71. DOI: 10.26897/1728-7936-2017-6-63-71.
12. Кудинов В.В. Плазменные покрытия. - М.: Наука, 1977. - 184 с.
13. Хасуй А. Техника напыления: Пер. С япон. / Под ред. С.Л.Масленникова. М.: Машиностроение, 1975. - 288 с.
14. Березин М.И. Низкотемпературная плазма и области ее применения / Обзоры по электронной технике: М., 1973. - Вып.24(167). - Сер. Технология, организация производства и оборудование. - 46с.
15. Газотермическое напыление покрытий. Сборник руководящих технических материалов. ИЭС им. Е.О.Патона. - Киев, 1990. - 176 с.

УДК 621.43.06

Р. Коваленко, магістр гр. АТ-20М
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ НАПРЯМКІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРИПРАЦЮВАННЯ АВТОМОБІЛЬНИХ ДВИГУНІВ

В роботі розглянуто основні напрямки підвищення ефективності припрацювання автомобільних двигунів. Виконано класифікацію основних способів підвищення ефективності припрацювання. Встановлено, що одним з ефективних напрямків підвищення ефективності є застосування припрацювальних складів та подача їх за допомогою повітря в зону найбільш інтенсивного тертя.

Виконано аналіз переваг та недоліків існуючих припрацювальних присадок. Надано рекомендації з застосування припрацювальних складів в автомобільних двигунах після виконання капітального ремонту.
припрацювання, автомобільний двигун, присадка

Постановка проблеми. Одним з факторів, що визначають довговічність двигунів, є стан поверхонь тертя основних їх деталей.

При формуванні поверхонь тертя необхідно забезпечувати отримання оптимальних триботехнічних характеристик поверхонь, що сполучаються, таких як низький коефіцієнт тертя, висока зносостійкість, оптимальні фізико-механічні властивості. Значною мірою вони визначаються якістю процесів припрацювання деталей капітально відремонтованих двигунів.

Останнім часом розроблені нові технологічні процеси фінішної обробки, які дозволяють знизити припрацювальний знос і підвищити антифрикційні властивості (підвищити мастило деталей, знизити коефіцієнт тертя і т.д.), а також зменшити час припрацювання пар тертя.

Однак, аналіз інформації, отриманої з друкованих та електронних джерел, дає можливість стверджувати, що не всі резерви інтенсифікації процесів припрацювання деталей двигунів вичерпані.

Аналіз останніх досліджень та публікацій. Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-7].

Мета і завдання досліджень. *Метою роботи* - дослідження шляхів підвищення ефективності процесів припрацювання циліндро-поршневої групи автомобільних двигунів застосуванням триботехнічних складів.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити існуючі технології підвищення ефективності припрацювання деталей автомобільних двигунів;

2. дослідити існуючі припрацювальні склади, виявити їх переваги та недоліки.

Об'єкт дослідження – технологія підвищення довговічності автотракторних двигунів застосуванням триботехнічних складів.

Предмет дослідження –закономірності вибору раціонального триботехнічного складу для зниження інтенсивності зношування деталей.

Методи досліджень базуються на теоретичному аналізі процесів та засобів припрацювання автомобільних двигунів.

Наукове і практичне значення в удосконаленні процесів припрацювання деталей двигуна мають роботи С.Г. Арабян, Н.П. Воїнова, І.С. Вороніцин, В.А. Владимирова, Л.М. Гаєнко, А.С. Гуревича, В.В. Долбіна, В.Г. Заренбін, І.М. Карасика, М.А. Карпенко, П.М. Керівник, Р.В. Кугеля, М.М. Маслова, Е.М. Мухіна і ін.

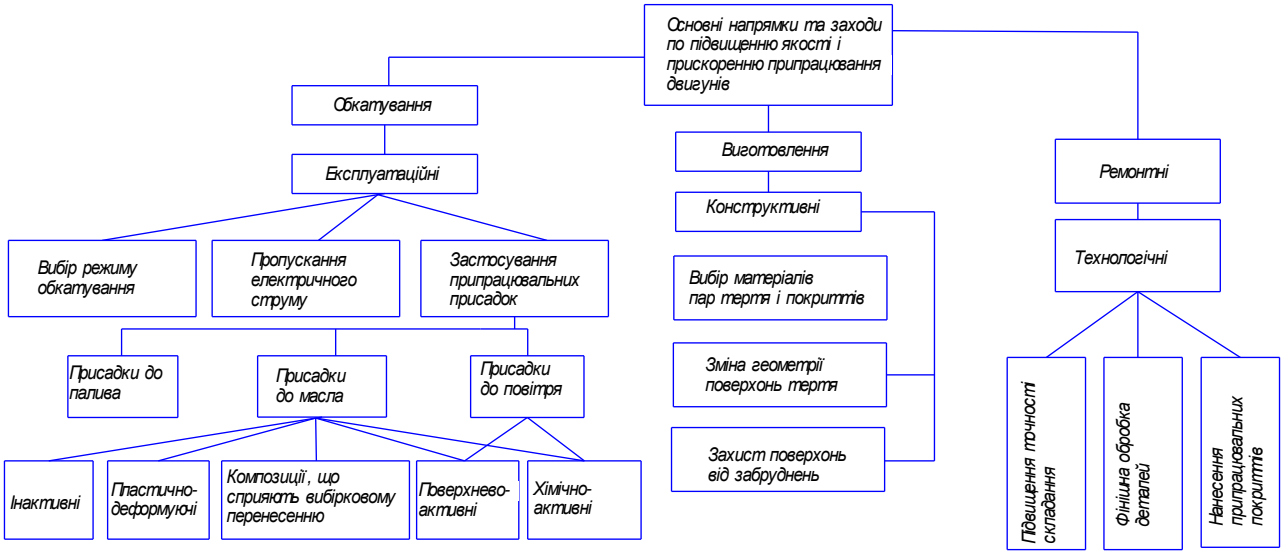


Рисунок 1 - Класифікація заходів по прискоренню припрацювання деталей двигуна

Згідно [27, 28], всі заходи щодо прискорення припрацювання деталей двигуна (рис. 2.3) можливо розділити:

конструктивні, здійснювані при виготовленні деталей;

технологічні, здійснювані при ремонті і відновленні деталей;

експлуатаційні, здійснювані при обкатці двигунів.

Прискорення і підвищення якості припрацювання деталей двигунів, домогтися конструктивними заходами, в умовах ремонтного виробництва дуже складно і не завжди економічно доцільно. Технологічні заходи вимагають матеріальних витрат, залучення кваліфікованих фахівців і дорогого устаткування.

Одним з найбільш перспективних напрямків оптимізації процесу припрацювання є експлуатаційні заходи, які забезпечують високу інтенсивність зношування, формування оптимальної мікрогеометрії поверхні деталей під час холодної обкатки з подальшим максимальним зниженням інтенсивності зношування при гарячої обкатці.

За способом фізико-хімічної дії припрацювальні присадки можна розділити на ряд груп: інактивні речовини (ІВ), поверхнево-активні речовини (ПАР), хімічно-активні речовини (ХАР), композиції, що сприяють виборчому переносу (КСВП).

За механізмом дії припрацювальні присадки діляться на наступні типи.

Присадки з використанням ПАР (ДФІ - 1; ОГМ - 1, 2, 3 та інші) сприяють інтенсифікації процесу припрацювання тертьових поверхонь деталей за рахунок ефекту адсорбційного зниження міцності матеріалів. Як ПАР найчастіше застосовують олеїнову, стеаринову і рицинову кислоти, ефіри органічних кислот, гліцерин та інші. Необхідно відзначити, що дія ПАР погіршується при високих температурах, що може викликати зниження протизадирних властивостей.

Інактивні присадки (Градис; АЛП - 1,2; Молікот - А; Ресурс; Ремол - 1; Деста - М; Гарант і ін.). Загальний недолік припрацювання деталей на маслах з інактивними присадками: характер поверхні під шаром присадки залишається колишнім, і при використанні в подальшому чистого масла мікронерівності розкриваються і зішліфовуються. Крім того, ці присадки нерозчинні в моторних маслах і випадають в осад при зберіганні і фільтрації.

Трібополімерізуючі присадки(ЕФ - 357; ЕФ - 262 і ін.). Застосовуються при холодному обкатуванні двигунів. Механізм дії цих присадок заснований на посиленні адгезійного взаємодії поверхонь тертя, що припрацьовуються. Особливість цих складів - висока припрацювальна ефективність при порівняно низькій температурі масла.

При гарячому обкатуванні адгезійний ефект полімерних плівок зникає, тоді як, тільки гаряче обкатування під навантаженням сприяє формуванню оптимальних фізико-механічних властивостей поверхонь тертя.

Хімічно - активні присадки (ОМ-2; ОКМ [69,70]; ДК-8) інтенсифікують хімічні процеси на поверхнях деталей, що труться, що призводить до утворення шарів з продуктів хімічної взаємодії з металом, які розділяють контактуючі поверхні, тим самим, перешкоджаючи схоплюванню і задирам.

Розглянуті хімічно активні присадки при всій їх ефективності мають такі недоліки: токсичність; хімічну активність присадок при збільшенні навантаження і температури, що призводить до підвищеного корозійно-механічному зношуванню деталей; складність приготування в умовах ремонтного виробництва.

Пластично деформуючі присадки (ОМД-8; VP-357 фірми «Optimal» Німеччина; EP Supplement фірми CRC Бельгія) містять цинкові, сурм'яні, свинцеві солі нафтенових і діалкілдітіофосфорних кислот, сполуки бору, сульфіду олова, алкілсвінец і комплексні сполуки молібдену.

Пластично деформуючі присадки можуть проявляти припрацювальні властивості тільки при обкатуванні під навантаженням, що не узгоджується з концепцією прискорення припрацювання в період холодної обкатки.

До присадок, що реалізують ефект виборчого перенесення-відноситься композиція КТЦМС, яка призначена для поліпшення антифрикційних, протизносних і протизадирних властивостей масел. При її використанні скорочується знос і час обкатування двигуна в 2 рази, шорсткість поверхні. Недолік на порядок зменшується композиції збільшується площа припрацювання і труднощі приготування в заводських умовах. Присадка характеризується загальнотоксичною дією.

Висновки. Термін служби двигуна і його міжремонтний ресурс залежить від якості припрацювання його деталей в період післяремонтного обкатки. Для досягнення повного припрацювання деталей двигуна потрібно 30...60 годин роботи. Прискорення припрацювання шляхом правильного вибору режимів обкатки двигунів, використанням нових технологій, застосуванням припрацювальних присадок дозволяє скоротити час обкатки двигуна.

В умовах ремонтних підприємств найбільш економічними і ефективними є експлуатаційні заходи щодо прискорення припрацювання деталей двигуна, які полягають в застосуванні комплексних присадок до масла і повітрю. Це дозволяє знизити припрацювальний знос і тим самим збільшити ресурс двигуна в цілому.

Аналіз застосовуваних присадок для припрацювання деталей двигунів після ремонту виявив найбільш перспективне використання комплексних присадок, що містять поверхнево-активні і хімічно активні речовини.

Список літератури

1. Носихин, П.И. Повышение качества и ускорение обкатки отремонтированных дизелей на основе современных достижений трибологии: Автореф. дис ... доктора техн. наук. -М., 1997. - 34 с.
2. Старосельский, А.А. Долговечность трущихся деталей машин / Под ред. А.Старосельский, Д.Н.Гаркунов. - М.: Машиностроение, 1967. - 395 с.
3. Школьников, В.М. Масла и составы против износа автомобилей /М.Школьников, Ю.Н.Шехтер и др. -М.: Химия, 1988. - 96 с.
4. Проников, А.С. Надежность машин. - М.: Машиностроение, 1979. - 591с.
5. Григорьев, М.А. Отечественный и зарубежный опыт повышения надежности и долговечности автомобильных двигателей / Под ред. М.А.Григорьев, В.А.Далецкий. - - М.: НИИавтопром, 1973. - 177 с.
6. Кацилграс, Г. А. Особенности сборки и приработки капитально отремонтированных двигателей / Г.А. Кацилграс. - М.: Росвузиздат, 1963. - 28 с.
7. Григорьев, М.А. Износ и долговечность автомобильных двигателей / М.А. Григорьев, Н.Н. Пономарев.- М.: Машиностроение, 1976. - 248 с.

УДК 621.431.3

А. Колодєєв, магістр гр. АІ(ТС)-20М
Центральноукраїнський національний технічний університет

ЗМІЦНЕННЯ РОБОЧИХ ОРГАНІВ ДИСКОВИХ БОРІН КОНТАКТНИМ НАВАРЮВАННЯМ

В роботі встановлено, що одним з ефективних методів зміцнення робочих органів сільськогосподарських машин є контактне наварювання покриттів. Даний метод характеризується високими фізико-механічними властивостями покриттів та забезпечує високі експлуатаційні характеристики. Процеси електроконтактного зміцнення мають наступні основні переваги: високу продуктивність і низьку енергоємність, мінімальну зону термічного впливу струму на деталь внаслідок малої тривалості імпульсу нагріву, відсутність необхідності у використанні захисної атмосфери через короткочасний термічний вплив на матеріал покриття і відсутність світлового випромінювання і газовиділення. Наносити покриття на дискові робочі органи методом контактного наварювання можливо з використанням контактних зварювальних машин з роликовими електродіми та спеціальним пристосуванням для орієнтуванням осі деталі під кутом.
контактне наварювання, зміцнення деталей, дискові робочі органи

Постановка проблеми. На теперішній час в промисловому і сільськогосподарському виробництві особливого значення набувають технології, що відповідають вимогам ресурсозбереження без збільшення матеріальних витрат на їх реалізацію. Це в повній мірі відноситься і до технологій відновлення і зміцнення дискових робочих органів сільськогосподарських машин, інтенсивна експлуатація яких призводить до затуплення лез в результаті їх зношування і корозії, що погіршує агротехнічні показники техніки, збільшує експлуатаційні витрати і веде до подорожчання сільськогосподарської продукції. Ефективним шляхом збільшення терміну служби таких деталей є підвищення їх зносостійкості методами зварювання, наплавлення або напилювання зносостійких покриттів, термообробки, дифузійного насичення, хіміко-термічної обробки і т. інш.

Одним з резервів зниження собівартості відновлення і зміцнення дискових робочих органів сільськогосподарських машин є використання в якості матеріалу для зміцнення композиційних порошкових матеріалів.

Ефективним способом відновлення і зміцнення дискових робочих органів з використання таких порошкових матеріалів є контактне наварювання (КНП), що дозволяє отримувати покриття з порошків зносостійких сплавів без їх розплавлення, тобто в твердій фазі. До теперішнього часу можливість використання контактного наварювання для зміцнення робочих органів дискових борін досліджена недостатньо.

Аналіз останніх досліджень та публікацій. Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-7].

Мета і завдання досліджень. Метою роботи є дослідження можливості підвищення зносостійкості робочих органів дискових борін контактним наварюванням.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити особливості технологічного процесу контактного наварювання порошковими матеріалами;

2. запропонувати технологічну схему контактного наварювання деталей типу «диск».

Об'єкт дослідження – технологічні процеси зміцнення дискових робочих органів.

Предмет дослідження – закономірності формування зміцнюючого покриття і якості його з'єднання з поверхнею деталі при контактному наварюванні порошкових матеріалів.

Методи досліджень базуються на теоретичному аналізі технологій та матеріалів зміцнення робочих органів сільськогосподарських машин.

Зношування дисків грунтообробних агрегатів - це процес руйнування їх грунторіжучої поверхні при терті внаслідок абразивних і фізико-механічних властивостей грунту, кінцевим результатом якого стають поступово змінені їх форма, розмір і стан робочої поверхні [1]. Зі зрозумілих причин, через вказані зміни якість виконання технологічного процесу лущення, дискування різко погіршується, знижуються показники техніко-економічної оцінки роботи грунтообробних машин.

Зі збільшенням напрацювання стан дисків, що зношуються, безперервно змінюється і досягає граничних значень відразу за кількома конструкційним параметрам, що впливає на функціональні і технологічні якості.

Для виготовлення дискових робочих органів грунтообробних технічних систем застосовуються такі конструкційні сталі: 40, 45, 40Х, 65Г, Л53, а також такі методи термічної обробки, як гартування і відпускання, що зміцнють грунторізальну поверхню дисків, твердість якої при цьому становить НВ 160-550 (не більше 39-56 HRC), а показник міцності не перевищує значень в 1400 МПа.

Практичні дослідження [2, 3] доводять, що при такій термообробці не виключається пряме руйнування грунторізальної поверхні диска шляхом мікродряпання і прорізання кварцовими частинками грунту. Інтенсивність зношування дискових робочих органів становить 0,3 мм/км, що говорить про фактичне напрацювання таких деталей в 1,5-3,0 рази менше у порівнянні із заявленою виробниками і нормативною документацією. Сучасними дослідженнями встановлено, що для ефективної обробки шару грунту на заданій глибині досить забезпечення міцності основного металу дискових робочих органів грунтообробних машин не менше 1500-1800 МПа [4].

Значення ударної в'язкості повинні бути в межах 0,8-1,25 МДж/м^2. Такі показники виключать деформацію дисків і їх поломку. При виробництві ґрунтообробної техніки важливо не тільки використовувати якісні матеріали, а й застосовувати відповідні технології термічної обробки (об'ємне гартування СВЧ та інш.). В результаті термообробки властивості сталей змінюються в досить широких межах, що дає можливість створювати більш міцні і надійні конструкції технічних систем.

Включення до складу сталей легуючих елементів значно змінює її властивості. Наприклад, невеликі добавки бору (В) значно підвищують прогартованість (глибину проникнення загартованої зони); при високому вмісті марганцю (Mn) сталі набувають велику твердість і опір зносу [5].

Дослідження, які проведені в роботах [5, 7, 8] доводять доцільність застосування контактного нагрівання для одержання покрить в режимі спікання і наварювання. В основі цієї технології покладено наукові принципи і технологічні прийоми порошкової металургії.

Контактне наварювання передбачає електронагрів металевого порошку, що засипається між деталлю і електродом, за рахунок теплової енергії, яка виділяється електричним струмом на активному опорі.

Енергія, необхідна для спікання порошку і наварювання його до поверхні деталі при електроконтактному наварюванні, виділяється електричним струмом у вигляді тепла безпосередньо в порошковому шарі в основному на контактах між частинками порошку, поверхнею деталі і електрода. Процес наварювання забезпечується сумісною дією на порошковий шар високої температури (0,9…0,95 температури плавлення порошку) і тиску (до 100 МПа), при цьому в кінетиці утворення металевого покриття приймають участь як бездифузійні явища схоплення, так і дифузійні процеси спікання і зварювання в твердій фазі.

Контактний спосіб дозволяє отримувати покриття з перемінними фізико-механічними властивостями по глибині шару [5]. Дослідженнями встановлено можливість одержання двох, трьох і більше послідовних зон по глибині покриття, виконаного із зносостійких порошків.

Процеси електроконтактного зміцнення мають наступні основні переваги: високу продуктивність і низьку енергоємкість, мінімальну зону термічного впливу струму на деталь внаслідок малої тривалості імпульсу нагріву, відсутність необхідності у використанні

захисної атмосфери через короткочасний термічний вплив на матеріал покриття і відсутність світлового випромінювання і газовиділення.

Процес електроконтактного нанесення покрить характеризується використанням електричного струму силою 1,5…30 кА, вторинною напругою 1...6 В. тиском до 100 МПа. Відмічається висока швидкість нагріву зони, що зміцнюється. По даним роботи [6], швидкість нагріву порошку методом електроопору при густині струму 0,9...1,2 кА/мм2 перевищує 50000 К/с.

Встановлено, що покриття, які наносяться методом електроконтактного наварювання володіють високими фізико-механічними властивостями (міцністю зчеплення 150...300 МПа, пористість не більше 10%). Слід відзначити, що при електроконтактному наварюванні наявність окисних плівок практично не знижує міцності з′єднання, так як плівка володіє високим електроопором і найбільш інтенсивно розігрівається імпульсом струму з подальшим видаленням з зони з′єднання. Так, по даним Кліменко Ю.В., при наплавленні шару на другий, сильно окислений шар, міцність з′єднання не нижча ніж при аналогічному наварюванні першого шару на очищену поверхню деталі. Зносостійкість покрить знаходиться на рівні сплавів одержаних електродуговим наплавленням високохромистого чавуну, істотно переважаючи термічно оброблені вуглецеві і низьколеговані сталі.

Основні технологічні варіанти контактного наварювання представлені на рис. 1.

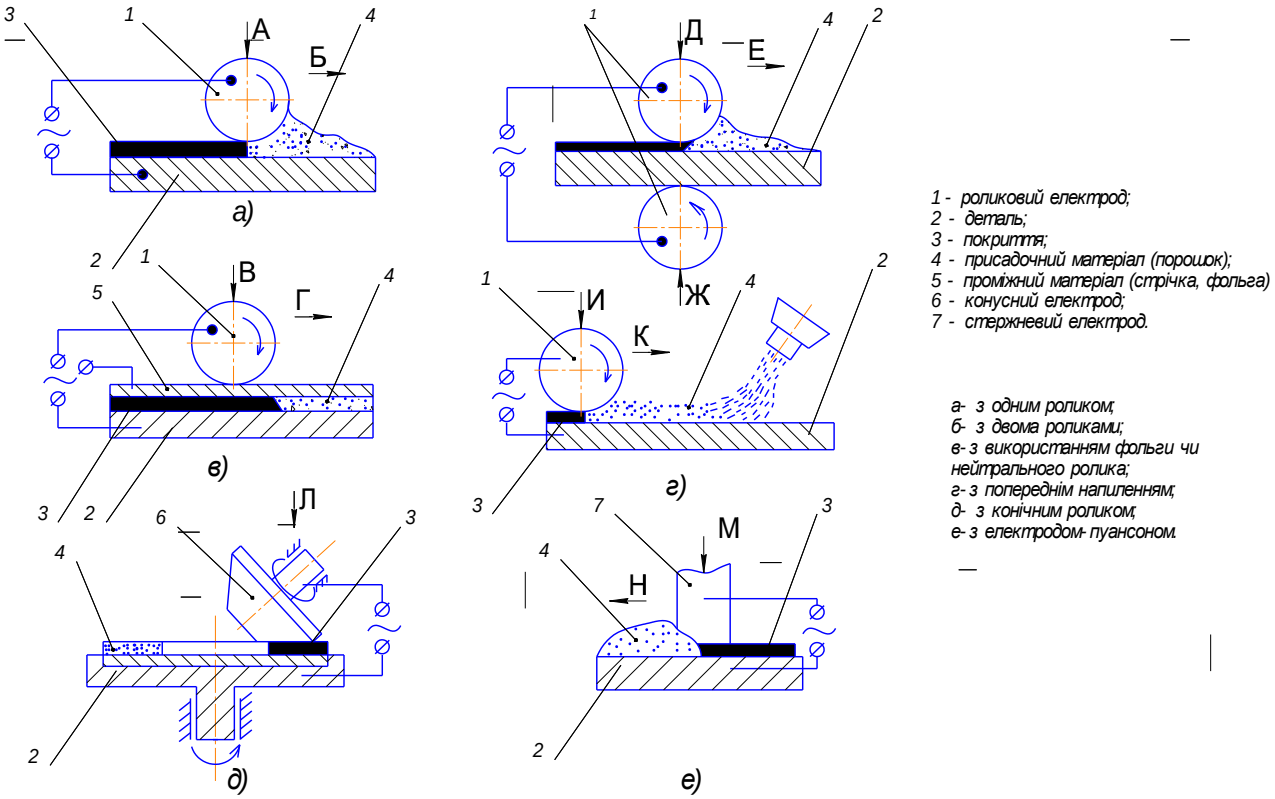
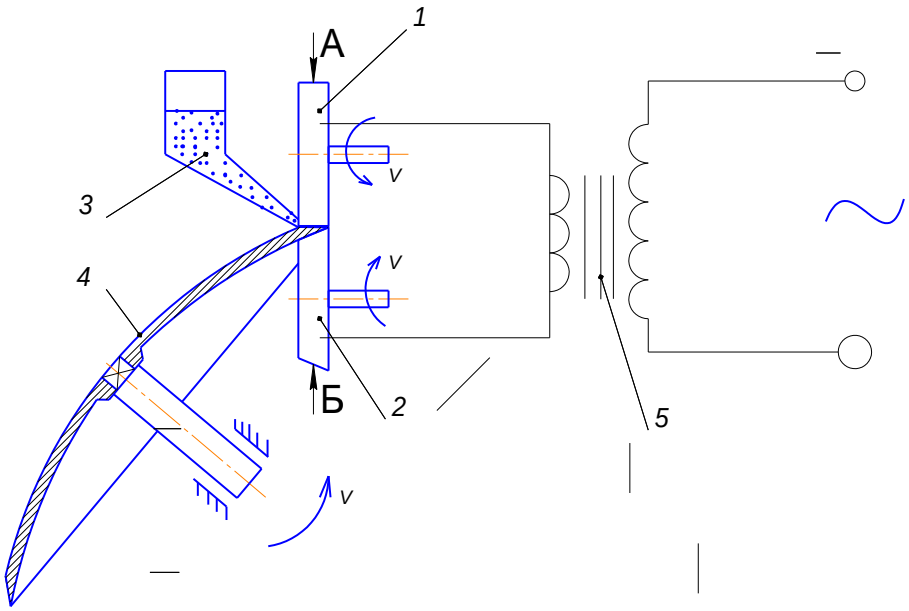


Рисунок 1 – Технологічні варіанти контактного наварювання порошкових матеріалів

Для контактного наварювання на поверхню диска борони найбільш доцільно використання варіанта *д* (рис. 1).

Схема наварювання порошку на диск борони буде мати вигляд (рис. 2).



1 - верхній електрод; 2 - нижній електрод; 3 - бункер з порошком; 4 - деталь (диск); 5 - трансформатор.

Рисунок 2 – Схема контактного наварювання на диски борони

Висновки.

Проведений аналіз показав, що контактне наварювання порошків являється одним з перспективних способів нанесення покрить на робочі органи сільськогосподарських машин. Відсутність рідкої фази в зоні зміцнення при нанесенні покрить значно розширює технологічні можливості процесу зміцнення.

Зміцнення робочих органів, що мають форму диска доцільно виконувати на роликових контактних машинах або модернізованих шовних машинах для контактного зварювання.

Для більш детального вивчення процесу, слід приділити увагу основним технологічним параметрам, якими є тиск і температура, а також фізико-механічним властивостям порошкової формовки і кінетиці утворення порошкового шару.

Список літератури

1. Сельскохозяйственная техника: Кат., т. 1 «ТЕХНИКА ДЛЯ РАСТЕНИЕВОДСТВА». — М.: ФГНУ «Росинформагротех», 2005. — 292 с. ISBN 5-7367-0547-8
2. Синеоков Г.Н., Панов И. М. Теория и расчет почвообрабатывающих машин. М., Машиностроение, 1977. с. 380.
3. Сабликов М.В. Сельскохозяйственные машины. Часть вторая. М., Колос, 1968. с. 247. 6. Канарев Ф.М. Ротационные почвообрабатывающие машины и орудия. М., Машиностроение, 1983. с. 94.
4. Стрельбицкий В.Ф. Дисковые почвообрабатывающие орудия. М., Машиностроение, 1978. с.178 8. Турбин Б.Г., Лурье А.Б., Григорьев С.М., и др. Сельскохозяйственные машины. Теория, конструкция и расчет. М., Л., Издательство машиностроительной литературы, 1963. с. 306
5. Красота, М.В. Технологія електроконтактного наварювання порошків з отриманням рівномірних властивостей по перерізу покриття: автореф. ... дис. канд. техн. наук / М.В. Красота. – Київ, 2002. – 20 с
6. Хасуи А., Моригаки О. Наплавка и напыление. – М.: Машиностроение, 1985 – 240 с.
7. Черновол М.И. Упрочнение и восстановление деталей машин композиционными покрытиями: Учеб. пособие. – К.: Вища школа., 1992, - 79 с.
8. Молодык Н.В., Зенкин А.С. Восстановление деталей машин: Справочник.- М.: Машиностроение., 1989, - 480 с.

УДК 62.192:621.43-233

О. Матвієнко, магістр гр. АТ-20М3
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ПРОЦЕСІВ ВТОМЛЕНОГО РУЙНУВАННЯ КОЛІНЧАСТИХ ВАЛІВ АВТОМОБІЛЬНИХ ДВИГУНІВ

В роботі встановлено, що одним основною причиною руйнування колінчастих валів є втомний злам. Розглянуто процеси виникнення та розвитку втомної тріщини на кожному етапі. Встановлено, що уникнути втомного руйнування можливо застосуванням конструктивних та технологічних заходів. З'ясовано, що на теперішній час немає єдиної думки про причини і механізм позитивного впливу того чи іншого методу на елементи колінчастих валів на їх втомну міцність.
втомлене руйнування, тріщини, колінчастий вал

Постановка проблеми. Аналіз наукових джерел інформації та досвід експлуатації автомобілів показали, що відмови двигунів відбуваються через провертання шатунних вкладишів та виникнення втомних тріщин на робочих поверхнях колінчастого вала. Масовість розвитку подібних дефектів свідчить про те, що недостатньо розкрита їх фізична сутність. У численних дослідженнях чітко не встановлено вплив конструктивних, технологічних, експлуатаційних факторів і режимів роботи двигуна на механізм розвитку відмов.

Більшість конструктивних елементів автомобілів працює в умовах циклічного навантаження, що створює сприятливі умови для розвитку втомних тріщин. Аналіз результатів руйнування валів в умовах експлуатації свідчить, що найбільша їхня кількість відбувається із зародженням втомної тріщини в з'єднаннях шийок різного діаметра. Основною причиною таких поломок є висока концентрація напруг у канавках.

Експлуатаційні дані свідчать про те, що 70-85% поломок колінчастих валів відбуваються по щоках і противаги від знакозмінних напружень вигину [6]. При цьому втомлена тріщина зароджується, як правило. У галтелях в місцях перекриття корінних і шатунних шийок, де виникає концентрація напружень, і вона проходить різні стадії розвитку. Так, в результаті дії зовнішніх сил вже на ранній стадії роботи в небезпечних ділянках окремі кристали піддаються різним пластичним деформаціям.

В наукових джерелах інформації недостатньо повно розглянуто процес втомного руйнування колінчастого вала, що обмежує його ресурс при форсуванні двигуна.

Аналіз останніх досліджень та публікацій. Закономірності зміни технічного стану колінчатих валів в процесі експлуатації двигунів досліджені такими вченими, як Ф.Н. Авдонькін, В.Н. Басков, А.А. Гафиятуллин, М.А. Григор'єв, І.Б. Гурвич, А.С. Денисов, В.А. Донецький, В.В. Єфремов, В.І. Казарцев, К.Т. Кошкін, Е.С. Кузнецов, А.Т. Кулаков, В.С. Лукинський, М.А. Масин, В.М. Михлин, І.А. Мішин, В.А. Наливкин, В.Н. Нікішин, Н.П. Світличний, А.Г. Степанов, А.М. Шейнін, В.А. Шадрічев і ін.

Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-8].

Мета і завдання досліджень. *Метою роботи* - дослідження процесів виникнення та розвитку втомлених тріщин колінчастих валів автомобільних двигунів.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити причини зниження втомленої міцності покритів;

2. дослідити напрямки підвищення втомленої міцності зносостійких покриттів.

Об'єкт дослідження – колінчасті вали дизельних двигунів вантажних автомобілів.

Предмет дослідження – закономірності виникнення та розвитку втомлених тріщин у колінчастих валах автомобільних ДВЗ.

Методи досліджень базуються на теоретичному аналізі причин зниження втомленої міцності колінчастих валів автомобільних ДВЗ.

Відповідно до сучасних уявлень втомна міцність твердих тіл не тільки визначається їх фізико-хімічної природою, а й залежить від дефекту структури, які існують в реальних тілах, наприклад, в колінчастих валах у вигляді мікро- і макротріщин, порожнин, включень різного походження, дислокацій і т.д. В процесі деформації твердого тіла навколо таких дефектів виникає висока концентрація напружень, яка є причиною появи нових дефектів або розвитку вихідних. У тілі колінчастого вала починається процес локального або повного руйнування.

Приклади руйнувань реальних конструкцій колінчастих валів за описаним вище механізмом показали, що існуючих класичних методів розрахунку по пружності і пластичного станів недостатньо, що в ці розрахунки необхідно вводити нові, істотно відмінні від старих, характеристики руйнування. Все це і додало проблеми крихкого руйнування колінчастих валів першорядне значення.

Експлуатаційні дані свідчать про те, що 70-85% поломок колінчастих валів відбуваються по щоках і противаги від знакозмінних напружень вигину [6]. При цьому втомлена тріщина зароджується, як правило. У галтелях в місцях перекриття корінних і шатунних шийок, де виникає концентрація напружень, і вона проходить різні стадії розвитку. Так, в результаті дії зовнішніх сил вже на ранній стадії роботи в небезпечних ділянках окремі кристали піддаються різним пластичним деформаціям.

Неоднорідність цього деформування обумовлена, головним чином, гистерезисом і незворотними втратами енергії при циклічному навантаженні. Пластичні деформації окремих кристалітів і їх груп викликають в подальшому перерозподіл напружень як від зовнішніх зусиль, так і від залишкових напружень [7]. Метал колінчастих валів складається з окремих безладно орієнтованих кристалів неправильної форми зерен. При повторних навантаженнях в окремих, найменш сприятливо орієнтованих зернах виникає зрушення - пластична деформація. Багаторазові повторні навантаження в протилежні сторони в несприятливо орієнтованих зернах по лініях ковзання поступово розвивають втомні мікротріщини - вони проходять через всі зерна, перетинають кордон і поширюються на сусідні зерна.

Поступово мікротріщини розростаються. Перетин неослабленим металу все зменшується, і при якомусь черговому навантаженні метал колінчастого вала раптово руйнується від втоми. Так як на початку обсяг пластично деформованого металу порівняно великий, то мікротріщин з'являється багато і вони мають хаотичну орієнтацію.

В процесі виробництва високонавантажених елементів колінчастих валів виникають початкові технологічні залишкові напруги [8]. Особливість останніх полягає в тому, що вони діють тільки в поверхневих шарах деталей глибиною 1-2 мм. Поверхневий шар, як правило, ослаблений через структурні і фазові перетворення, зміни за хімічним складом, через наявність мікроконцентраторів напружень. Ослаблення поверхневого шару може бути пов'язане з наявністю початкових технологічних залишкових напруг від механічної або термічної обробки.

Значне підвищення запасу втомної міцності при зовнішніх знакозмінних навантаженнях виходить в результаті поверхневого пластичного деформування (ППД) елементів колінчастого вала: щік, противаг, корінних і шатунних шийок, підшипників ковзання, болтів кріплення противаг.

Підвищення запасу втомної міцності пояснюється двома основними причинами: сприятливим впливом стискають початкових технологічних залишкових напруг і поліпшенням механічних властивостей поверхневого шару в результаті ППД.

Механізм втомного руйнування матеріалу елемента колінчастого вала полягає в наступному: при дії знакозмінних напружень в матеріалі виникає втомлена тріщина, яка поступово проникає вглиб конструкції. При змінних деформаціях краї втомленої тріщини зближуються, утворюючи притерту, гладку зону зламу. По мірі розвитку тріщини робоча площа перетину послаблюється, що веде до руйнування елемента колінчастого вала при динамічному навантаженні - ударі. Зона остаточного зламу має грубозернисту поверхню. Досліди показують, що втомні тріщини виникають тільки при знакозмінних динамічних напругах [8].

Металографічні дослідження зразків з матеріалу колінчастих валів показали, що причиною зародження втомних тріщин є поступове накопичення недосконалостей кристалічної решітки в результаті багаторазового повторення пластичної деформації металу. Неоднорідність реального металу веде до великого розкиду напружень не тільки в різних зернах, а й усередині одного зерна. Причому, втомлена тріщина починає розвиватися як по зернам, так і по їх кордонів. Так як на початку обсяг пластично деформованого матеріалу порівняно великий, то тріщин з'являється багато, і вони мають хаотичну орієнтацію. Надалі пластичні деформації зосереджуються, головним чином, в вершинах тріщин, розташованих перпендикулярно дії нормальних максимальних напружень, що визначає їх переважне, в порівнянні з іншими напрямками, розвиток. Поява магістральної тріщини призводить до зниження напруги в цій області, гальмування тріщин, які розвивалися в інших напрямках, що зазвичай характеризується періодом стабільного зростання пошкодження.

Основними з них є конструктивні й технологічні заходи.

Конструктивні заходи в основному зводяться до зменшення концентрації напруг у місцях, де звичайно виникають втомні тріщини, що ведуть до поломки деталей і елементів конструкцій. Для зменшення концентрації напруг застосовують:

а) скруглення кутів, використання в цих місцях стовщених накладок для елементів конструкцій;

б) вварювання пасків по контуру вирізів в елементах конструкцій;

в) збільшення закруглень у жолобниках (виточеннях) валів, осей і інших деталей;

г) фрезерування вхідного кута шпонкової канавки;

д) збільшення діаметра вала під насадженою на нього втулкою й ін.

Технологічні заходи в деталях машин спрямовані, в основному, на видалення корозії, яка знижує втомну міцність, у результаті глибокої механічної обробки поверхні деталей. Для цих цілей використовують:

а) шліфування поверхні спеціальною механічною обробкою (термічної, термохімічної);

б) застосування зміцнених покриттів поверхні деталей.

Таким чином, при виготовленні та відновленні колінчастих валів слід застосовувати технологічні операції, які спрямовані на зниження імовірності виникнення втомлених тріщин.

Висновки. Основною причиною руйнування колінчастих валів є втомний злам. Процес розвитку втомної тріщини відбувається поетапно. Уникнути втомного руйнування можливо застосування конструктивних та технологічних заходів. На теперішній час немає єдиної думки про причини і механізм позитивного впливу того чи іншого методу на елементи колінчастих валів на їх втомну міцність.

Список літератури

1. Стативкин Г.П. Усталостные поломки коленчатых валов дизелей и борьба с ними: Тр. ЦНИДИ, вып.60/ Г.П. Стативкин, В. А. Япчеленко. - Л., 1970. - С.37-43.
2. Серенсен С.В. Несущая способность и расчеты деталей машин на прочность. Справочное пособие / С.В. Серенсен, В.П. Кочаев, Р.М. Шнейдерович. -М: Машиностроение, 1975 - 488 с.
3. Косырев С.П. Исследование остаточных напряжений в высоконагруженных деталях форсированных дизелей / С.П. Косырев, А. В. Разуваев, Л.А. Сорокина, Р.М. Рафиков, Е.А.

Комиссаренко//Двигателестроение. - 2003. №3, С.21-24.
4. Марьина Н.Л. Механизм усталостного разрушения коленчатых валов форсированных дизелей - М: Тяжелое машиностроение, №7, 2011. С.22-24.
5. Косырев С.П. Концентрация остаточных напряжений в коленчатом вале форсированного дизеля в условиях поверхностного пластического деформирования / С.П. Косырев, И.О. Кудашева, Н.Л. Марьина// - М: Ремонт, восстановление, модернизация, №5, 2011. С.35-38.
6. Видинеев, А. А. Обеспечение качества коленчатого вала автомобильного двигателя / В. Н. Никишин, А. Т. Кулаков, А. С. Денисов, А. А. Видинеев // Вестник Сарат. гос. техн, ун-та. - 2006. - № 4 ; вып. 3. - С. 65-75 (0,64/0,12).
7. Видинеев, А. А. Обеспечение эксплуатационных свойств коленчатого вала двигателя КамАЗ-740 при ремонте и восстановлении / А. С. Денисов, А. Т. Кулаков, В. В. Погораздов, Б. Ф. Тугушев, Е. Ю. Горшенина, А. А. Видинеев // Вестник Сарат. гос. техн, ун-та. - 2009. - № 3 ; вып. 2. - С. 74-78 (0,32/0,05).

УДК 621.431.3

В. Усенко, магістр гр. АІ(ТС)-20М
Центральноукраїнський національний технічний університет

ВІДНОВЛЕННЯ ДЕТАЛЕЙ ТРАНСПОРТНИХ ЗАСОБІВ ТИПУ «ВАЛ» КОНТАКТНИМ НАВАРЮВАННЯМ ДИСКРЕТНИХ ПОКРИТТІВ

В роботі встановлено, що одним з ефективних методів відновлення деталей типу «вал» транспортних засобів є контактне наварювання покриттів. Внаслідок того, що більшість валів автомобільної та тракторної техніки працюють при знакозмінних навантаженнях, використання даного методу супроводжується втратою втомленої міцності деталей, що пов'язано з високою твердістю та ламкістю зносостійких покриттів. Ці покриття в процесі експлуатації під дією знакозмінних навантажень розтріскуються і деталь виходить з ладу. Зменшити імовірність розтріскування можливо досягти шляхом заміни суцільних покриттів на дискретні. Існує необхідність у вивченні функціональних властивостей покриттів, що отримуються контактним наварюванням порошкових матеріалів.
контактне наварювання, відновлення деталей, дискретні покриття

Постановка проблеми. Розробка новітніх технологій поверхневого зміцнення для деталей транспортних засобів, що працюють в умовах інтенсивного зношування є актуальною проблемою.

Для деталей транспортних засобів потрібні технології, що забезпечують високу продуктивність обробки в поєднанні з товщиною покриттів відповідної допустимому зносу.

З методів нанесення покриттів найбільш економічним і продуктивним є контактне наварювання. Однак, в даний час відсутні науково обґрунтовані рекомендації з розробки технологій контактної наварки твердих ламких покриттів. Одним з перспективних рішень в даному випадку є нанесення зміцнених шарів градієнтної (дискретної) будови.

Теплофізичні параметри контактного наварювання дозволяють формувати поверхневі зміцнені шари за рахунок нанесення матеріалів на поверхні деталі в твердій фазі.

У транспортних засобах, які використовуються найбільш інтенсивному зношуванню піддаються деталі типу «вал». Ця група деталей, як правило, працює при знакозмінних навантаженнях. При відновленні і зміцненні таких деталей твердими зносостійкими матеріалами найчастіше дані покриття розтріскуються і відшаровуються в процесі експлуатації.

Аналіз останніх досліджень та публікацій. Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-7].

Мета і завдання досліджень. *Метою роботи* - дослідження процесів формування дискретних покриттів, що забезпечують підвищення експлуатаційних властивостей поверхонь деталей при контактному наварюванні покриттів.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити причини зниження втомленої міцності покритів;

2. дослідити напрямки підвищення втомленої міцності зносостійких покриттів.

Об'єкт дослідження – процеси контактного наварювання дискретного зносостійкого покриття на вали транспортних засобів.

Предмет дослідження – закономірності зміни фізико-механічних властивостей зміцнених шарів дискретних покриттів на деталях транспортних засобів типу «вал», отриманих контактним наварюванням.

Методи досліджень базуються на теоретичному аналізі причин зниження втомленої міцності ламких зносостійких покриттів.

Контактне наварювання (КН) є одним з найбільш продуктивних і економічних способів нанесення покриттів.

При контактному наварюванні покриттів з порошкових матеріалів процес утворення покриття відбувається в результаті взаємного розплавлення і кристалізації деталі і матеріалу, що наварюється (дріт, стрічка).

На теперішній час наварювання покриттів з компактних матеріалів, що відрізняється високою продуктивністю і забезпечує стабільну якість з'єднань, застосовується в автомобільному, сільськогосподарському машинобудуванні та інших галузях при відновленні та зміцненні деталей.

Якість наварюванні покриттів з компактних матеріалів забезпечується виконанням повного технологічного циклу, що складається з окремих операцій: попе-реднього стискування зварювальних деталей електродами машини, нагріванням металу з утворенням литої зони, проковування навареного з'єднання після виключення зварювального струму і охолодження з'єднання після зварки.

Спосіб контактного наварювання, ефективно застосовується для відновлення більшості валів автомобільної, сільськогосподарської техніки, дорожніх машин, що працюють як на зношування, так і при динамічних і повторно-змінних навантаженнях. Виключення становлять важко навантажені колінчасті вали, особливо великі, тобто діаметром більш 120…150 мм, а також деталі із зносами робо-чих поверхонь більш 0,8-1 мм на сторону. Собівартість відновлення виробів за до-помогою КН не перевищує 20…40 відсотків нових при рівному ресурсі.

Застосування відомих методів відновлення і зміцнення, в тому числі і контактного наварювання, ускладнене у зв'язку з великою трудомісткістю і небезпекою виникнення несприятливого напруженого стану. Для цих цілей досить перспективне застосування покриттів дискретної структури.

Зменшити ймовірність руйнування тонких крихких покриттів можливо, шляхом нанесення їх у вигляді окремих елементів, тобто отриманням дискретних покриттів.

Досвід експлуатації та результати численних досліджень свідчать про те, що в більшості випадків функціональні властивості і ресурс різних видів машин і технологічного оснащення визначається інтенсивним зношуванням високонавантажених деталей вузлів тертя і поверхні робочих органів [1]. Разом з тим, традиційні методи зміцнення і нанесення покриттів, здатні поліпшити їх експлуатаційні характеристики, не задовольняють постійно зростаючим вимогам в умовах динамічних навантажень, високих температур, активного впливу корозійних середовищ і наявності абразивних потоків. Ефективним виходом з цієї ситуації є формування на поверхні виробів з конструкційних матеріалів зносостійких покриттів градієнтної (дискретної) будови, шаруватих, матрично-наповнених або скелетного типу [2].

Трибологія давно зіткнулася з явищем виборчого зношування матеріалів, викликаного структурною неоднорідністю. Такого роду явище спостерігається в бабітових підшипниках

ковзання, на сталевих деталях при їх зношуванні і поліруванні [3]. Суть його полягає в тому, що найбільш інтенсивному руйнуванню піддається менш міцна (найчастіше м'якша) структурна складова, в результаті чого спочатку рівна робоча поверхня стає хвилястою. При цьому ефект формозміни поверхні тертя більш яскраво виражений на матеріалах з крупнодисперсною структурою. Утворення такої експлуатаційної хвилястості при деяких умовах тертя має сприяти підвищенню службових властивостей сполучень. Відомо, наприклад, що в режимі недостатнього мащення на поверхні тертя штучним чином створюють своєрідні кишені, збільшуючи тим самим її маслоємність, що в свою чергу знижує знос і небезпеку виникнення задирань. Наявність таких кишень дозволяє значно обмежити присутність продуктів зношування в зоні тертя, підвищивши тим самим зносостійкість сполучення і стабільність його триботехнічних характеристик.

Для традиційних суцільних покриттів, як і для компактних матеріалів, у всіх випадках знос є результатом локального перенапруження одного або обох контактуючих тіл за рахунок нормального і дотичного навантаження. Дискретна структура покриття обмежує це локальне перенапруження.

В роботі [6] був запропонований метод розрахунку розміру дискретної ділянки покриття з урахуванням залишкових напружень, високий рівень яких значно впливає на характеристики міцності системи основа-покриття.

Авторами робіт [7] зазначалося, що зародження тріщин в покриттях дискретної структури починається при більш значних критичних деформаціях, ніж в покриттях регулярної структури. Про це говорять експериментальні дослідження і теоретичні розрахунки, виходячи з яких, слід, що покриття дискретної структури може витримати вищі навантаження в порівнянні з покриттями регулярної структури. Для оптимізації технології одержання покриттів дискретної будови застосовується також багатокритеріальний підхід [9], що дозволяє скоротити кількість випробувань і отримати регресивні залежності межі витривалості.

Про перспективність формування дискретної будови поверхні говорить той факт, що контактуючі пари не стикаються всією поверхнею. Вони контактують з дискретним, випадково розташованими майданчиками фактичного контакту [7]. Це обумовлено відхиленнями форми поверхні, хвилястістю і шорсткістю. При цьому досягнення повного контакту не доцільне, це підтверджується вивченням деформацій і контактних напружень, що труться [7]. Отже, більш прийнятним може бути цілеспрямоване формування рельєфу поверхні.

Висновки. Процес контактного наварювання дискретних покриттів вимагає системного аналізу всієї сукупності факторів (вхідних і вихідних параметрів, включаючи геометричні параметри дискретного покриття) на підставі комплексу досліджень структури, твердості, напруженого стану, зносостійкості і шорсткості поверхні. Такі систематизовані дані стосовно відновлення і зміцнення деталей транспортних засобів в даний час у вітчизняній і зарубіжній літературі відсутні. Рішення даного завдання є актуальним і дозволить значно розширити області застосування новітніх технологій відновлення і зміцнення матеріалів.

Список літератури

1. Кагаев В.П. Прочность и износостойкость деталей машин /П. Катаев, Ю. Н. Дроздов. - М.: Высшая школа, 1991. - 319 с.
2. Корниенко А. А. Износостойкие композиционные покрытия градиентного типа / А. А. Корниенко, Я. П. Замора, М. В. Лучка // Оборудование и технология термической обработки металлов и сплавов: 6-й междунар. конф. ОТТОМ-6.: тезисы докл. - Харьков, 2005. - ч. II. - С. 225-230.
3. Горячева И. Г. Изнашивание неоднородно упрочненных поверхностей / И. Г. Горячева, М. И. Добрычин // Трение и износ. - 1986. - № 6. - С. 985-992.
4. Красота, М.В. Технологія електроконтактного наварювання порошків з отриманням рівномірних властивостей по перерізу покриття: автореф. ... дис. канд. техн. наук / М.В. Красота. – Київ, 2002. – 20 с
5. Ляшенко Б. А. Упрочнение поверхности металлов покрытиями дискретной структуры с повышенной

адгезионной и когезионной стойкостью / Б. А. Ляшенко, Ю. А. Кузема, М. С. Дигамм. - Киев, 1984. - 57 с. - (Препринт / НАН Украины, Ин-т пробл. прочн.).
6. Ляшенко Б. А. Определение параметров дискретной структуры покрытий с учетом остаточных напряжений / Б. А. Ляшенко, Е. Б. Сорока, А. В. Рутковский, И. В. Липинская // Проблемы прочности. - 2002. - № 4. - 119-125.
7. Ляшенко Б. А. Исследование прочностных характеристик и фрет- тинг-коррозии дискретных покрытий / Б. А. Ляшенко, И. А. Долгов, Е. К. Соловых // Инженерия поверхности и реновация изделий: Материалы 8- й международной научно-технической конференции, 27-29 мая 2008 г., г. Ялта.-Киев: АТМ Украины, 2008- С. 151-153.

УДК 621.791.927.5

С. Чоповий, магістр гр. АІ(ТС)-20М
Центральноукраїнський національний технічний університет

АНАЛІЗ УМОВ РОБОТИ ТА ПРИЧИНИ ВИХОДУ З ЛАДУ КОРПУСНИХ ДЕТАЛЕЙ СІЛЬСЬКОГОСПОДАРСЬКОЇ ТЕХНІКИ

В роботі виконано аналіз умов роботи корпусних деталей сільськогосподарської техніки, виявлено основні дефекти, причини їх виникнення та вплив на експлуатаційні показники роботи. Аналіз дефектів корпусних деталей мобільних сільськогосподарських машин дав змогу отримати їх частоту зустрічання.

Встановлено, що основна частка дефектів доводиться на внутрішні гладкі циліндричні поверхні (отвори), тому актуальним питанням є необхідність забезпечення зносостійкості саме цих поверхонь. Інтенсивність зношування поверхонь найчастіше визначається структурою, фізико-механічними і геометричними характеристиками матеріалів деталей, умовами роботи деталі, конструктивними особливостями з'єднання.

корпусна деталь, відновлення деталей, дефект

Постановка проблеми. У конструкціях сільськогосподарських самохідних машин і механізмів різного призначення базисними деталями є корпуса різних агрегатів – двигунів, коробок передач, роздавальних коробок. Ці деталі визначають ресурс вказаних агрегатів, їх вихід з ладу приводить до простоїв техніки та економічних втрат.

Основними дефектами корпусних деталей є зношення отворів, які, в основному, слугують опорними поверхнями для валів агрегатів або інших деталей.

Отвори деталей, що виконують роль опор для вала, в процесі експлуатації зазнають нерівномірності розподілу контактного тиску і швидкості ковзання, багаторазові зміщення і проковзування поверхонь, мають циклічний характер прикладання навантажень, що призводить до додаткових пластичних деформацій і зміни геометрії профілю, заповнивши контактну і втомленому руйнуванню нерівностей останнього, а в деяких випадках - до виникнення мікрорізання.

Проведений аналіз зношуваності отворів корпусних деталей показав, що більшість з них виходить з ладу у зв'язку з низькими експлуатаційними властивостями робочої поверхні.

Огляд сучасних способів поверхневого зміцнення, аналіз їх переваг та недоліків дозволяє рекомендувати технологію електромеханічної обробки як один з ефективних способів підвищення довговічності опорних поверхонь отворів деталей.

У корпусних деталях сільськогосподарської техніки широко застосовуються гладкі внутрішні циліндричні поверхні. В процесі експлуатації машин, більше 85% втрачають свою працездатність не через поломки, а внаслідок зношування їх робочих поверхонь. Для підвищення їх довговічності необхідно формувати високі експлуатаційні властивості на робочих поверхнях. При цьому для зовнішніх поверхонь такі технології розроблені в

великому обсязі, а для внутрішніх зміцнюючих технологій, які забезпечують тривалу безвідмовну роботу з'єднань, досліджень недостатньо. Особливо проблематична зміцнююча обробка отворів деталей.

Аналіз останніх досліджень та публікацій. Великий внесок у розвиток технологій відновлення і зміцнення деталей сільськогосподарської техніки внесли: Б.М. Аскіназі, К.А. Ачкасов, Н. Батищев, В.П. Багмут, Ф.Х. Бурумкулов, М.Н. Єрохін, В.М. Кряжков, В. Курчаткин, П.П. Лезін, Е.А. Лисун, В.П. Лялякін, С.С Некрасов, В. Поляченко, Е.А. Глибин, В.В. Стрільців, І.Є. Ульман, В.П. Ципцин, П. Черноїванов, В.А. Шадрічев і інші вчені.

Проблематика, що вирішується в даній роботі була також досліджена в наукових працях [1-7].

Мета і завдання досліджень. *Метою роботи* є дослідження процесів зношування та причин виходу з ладу корпусних деталей сільськогосподарської техніки.

Для досягнення поставленої мети вирішувалися наступні задачі досліджень:

1. дослідити причини зношування корпусних деталей;

2. встановити основні дефекти, яких набувають корпусні деталі в процесі експлуатації машини.

Об'єкт дослідження – процеси зношування корпусних деталей сільськогосподарських машин.

Предмет дослідження – закономірності зміни фізико-механічних властивостей поверхонь корпусних деталей автотракторної техніки.

Методи досліджень базуються на теоретичному аналізі причин виходу з ладу корпусних деталей сільськогосподарської техніки.

Термін служби мобільних сільськогосподарських машин, механізмів і обладнання до капітального ремонту багато в чому залежить від зносостійкості їх корпусних деталей.

Як відомо, велика частина деталей цих машин (80...85%) виходить з ладу внаслідок їх інтенсивного зношування, при цьому більшість деталей ремонтованих машин вибраковується внаслідок незначного зносу робочих поверхонь, що становить не більше 1% початкової маси деталей [1, 2] . Через низьку довговічність деталей виникає економічно невиправданий високий рівень витрат матеріальних і трудових ресурсів.

Аналіз дефектів корпусних деталей мобільних сільськогосподарських машин дав змогу отримати частоту зустрічання вказаних дефектів. На рис. 1 представлено процентне співвідношення зносів корпусних деталей в залежності від виду поверхні деталей машин.

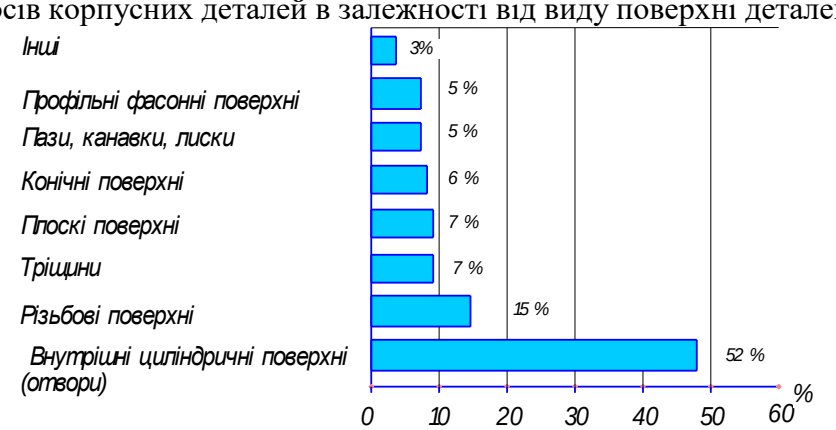


Рисунок 1 – Розподіл зносів поверхонь корпусних деталей мобільних сільськогосподарських машин

Як видно з діаграми, основна частка дефектів доводиться на внутрішні гладкі циліндричні поверхні (отвори), тому актуальним питанням є необхідність забезпечення зносостійкості саме цих поверхонь.

Необхідно враховувати, що інтенсивність зношування поверхонь найчастіше визначається структурою, фізико-механічними і геометричними характеристиками матеріалів деталей (твердість, шорсткість і т.д.), умовами роботи деталі (наявність мастила, температура, вплив абразиву, тиск, швидкість відносного переміщення деталей, що труться),

конструктивними особливостями з'єднання (шарнір, підшипник ковзання, напрямна; - наявність ущільнення, відкрите з'єднання).

З метою підвищення довговічності деталей слід прагнути до підвищення якості поверхонь деталей за рахунок використання зміцнюючих технологій.

Для підвищення довговічності і надійності деталей необхідні відомості про умови роботи, характер зношування поверхонь, матеріали деталей. Це важливо для призначення режимів поверхневого зміцнення. Переважаючими серед усього обсягу корпусних деталей є чавунні деталі.

У зв'язку з цим було проведено аналіз залізовуглецевих деталей за величинами гранично допустимого зносу. При цьому вибиралися деталі, вибракування яких проводилося в зв'язку із зносом внутрішнього діаметра.

Найбільшого поширення мають отвори корпусних деталей із сталей та чавуну. Це сталі 10, 20 і 25, якісні сталі 40, 45, 40Х та чавуни СЧ 18…СЧ24.

Розмірний аналіз деталей показав, що близько 40% отворів мають внутрішній діаметр в інтервалі 30…100 мм, більше 30% отворів мають внутрішній діаметр в межах 20 мм.

Особливий інтерес представляють дані про величину гранично допустимих зносів (рис. 2). Гранично допустимі зноси понад 70% всіх досліджених отворів корпусних деталей складають до 0,5 мм. Ця обставина робить правомірним застосування поверхневих методів зміцнення з метою підвищення довговічності значною номенклатури корпусних деталей з отворами.

Для оцінки величини зносів отворів деталей виникає необхідність встановлення розподілу їх зносів. З цією метою після мікрометражних досліджень значення односторонніх зносів отворів деталей зводилися до рядів розподілу, і проводилася статистична обробка [4]. Вимірюванню піддавалися такі деталі: Втулка кронштейна кулака трактора МТЗ - 80.1, втулка каретки підвіски трактора ДТ-75М, втулка балансира трактора Т-25 А, втулка нижня кронштейна кулака трактора МТЗ - 80.1, опорна отвір вала корпусу гідробака трактора Т-25А. Ці деталі багато в чому визначають працездатність вузлів в цілому. Номінальні розміри отворів вказані в технічних вимогах на капітальний ремонт. Вимірювання отворів проводилося за допомогою індикаторного нутроміру.

Рисунок 2-Розподіл за величиною зносів отворів корпусних деталей

Згідно [5-7] зносостійкість і довговічність з'єднань різко зростає з підвищенням твердості однієї або обох деталей, що труться. В цьому випадку для виготовлення деталей рекомендується застосовувати загартовані сталі та відбілені чавуни. Економічно невигідно добиватися підвищення твердості всієї деталі, іноді буває достатнім зміцнення робочої поверхні на глибину граничного зносу даної деталі.

Більшість деталей надходять на складання після термічної або хіміко-термічної обробок. Зміцнення отворів даними способами є тривалим багатоопераційним процесом, що включає в себе попередню механічну обробку, об'ємне загартування і подальшу лезову та/або абразивну чистові операції, так як при тривалому високотемпературному нагріванні деталі має місце викривлення робочих поверхонь.

Для більшості з'єднань в інструкціях по експлуатації техніки величини гранично допустимих зазорів, регламентовані допустимі зноси кожної з деталей, що труться, згідно з

якими в процесі дефектації приймається рішення про придатність деталі для подальшої експлуатації, про необхідність заміни її новою деталлю.

Залежно від конструктивних особливостей машин, їх призначення і виконуваних операцій характер взаємодії гладких циліндричних з'єднань може бути обумовлений нерівномірністю розподілу навантажень на робочі поверхні деталей.

Особливо несприятливо на роботу деталей з отворами, що слугують опорами для вала позначаються, нерівномірність розподілу контактного тиску і швидкості ковзання, багаторазові зміщення і проковзування поверхонь, що з'єднуються, одна відносно одної, циклічний характер прикладання навантаження, що призводить до додаткових пластичних деформацій і зміни геометрії профілю, а в деяких випадках - до виникнення мікрорізання. Все це викликає досить швидку втрату працездатності пари тертя в цілому.

В результаті зношування отвору з'єднання відбувається зміна його геометрії, збільшення зазору між деталями, порушується взаємне розташування деталей, зростають динамічні навантаження на деталі. Граничний знос деталей з'єднання впливає на технічні, економічні та екологічні показники роботи техніки. Також необхідно зауважити, що відновлення зношеного отвори є трудомісткий багатоопераційний процес. В основному деталі, що мають характерний знос отворів, замінюються на нові, що не вирішує наявної проблеми.

При виборі оптимального способу і режимів поверхневого зміцнення для кожної конкретної деталі рухомого з'єднання необхідно мати додаткові статистичні дані по зносу цих деталей: величину середніх зносів, процентне співвідношення деталей із зносом, менше і більше гранично допустимого, закон розподілу величин зносів, коефіцієнт варіації.

Висновки. В результатів досліджень встановлено, що основна частка дефектів доводиться на внутрішні гладкі циліндричні поверхні (отвори), тому актуальним питанням є необхідність забезпечення зносостійкості саме цих поверхонь. Особливо несприятливо на роботу корпусних деталей з отворами, мають нерівномірність розподілу контактного тиску і швидкості ковзання, багаторазові зміщення і проковзування поверхонь, що з'єднуються, одна відносно одної, циклічний характер прикладання навантаження, що призводить до додаткових пластичних деформацій і зміни геометрії профілю, а в деяких випадках - до виникнення мікрорізання. Все це викликає досить швидку втрату працездатності пари тертя в цілому.

Вибір оптимального способу і режимів поверхневого зміцнення для кожної конкретної корпусної деталі рухомого з'єднання слід виконувати з урахуванням статистичних данних по зносу цих деталей: величину середніх зносів, процентне співвідношення деталей із зносом, менше і більше гранично допустимого, закон розподілу величин зносів, коефіцієнт варіації

Список літератури

1. Гаркунов, Д.Н. Триботехника (износ и безызносность) Учебник. - 4-е изд., перераб. и доп. - М.: Изд-во МСХА, 2001. - 616 с.
2. Дорожкин, Н.Н. Методы получения износостойких покрытий из металлических порошков с наполнителями./ Н.Н. Дорожкин, В.К. Ярошевич, М.А. Белоцерковский, В.А. Верещагин - Мн.: Наука и техника, 1979. - 152 с.
3. Морозов, А.В. Характер эксплуатационного износа гладких цилиндрических подвижных соединений применяемых в сельскохозяйственной технике / А.В. Морозов, В.А. Фрилинг // Материалы III Международной научно-практической конференции «Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути решения». - Ульяновск: ГСХА, 2011, т. II. - С. 271-275.
4. Крагельский, И.В. Узлы трения машин: Справочник. / И.В. Крагельский, Н.М. Мухин М.: Машиностроение, 1984. - 280 с.
5. Фрилинг В.А. Влияние режимов избирательной электромеханической закалки поверхности отверстия на глубину упрочненного слоя / В.А. Фрилинг // Научно - технический вестник Поволжья - 2012,- №2. - с. 295 - 300.
6. Фрилинг В.А. Исследование влияния содержания углерода на микротвердость при избирательной электромеханической закалке трибонагруженного участка отверстия / Л.В. Федорова, А.В. Морозов, В.А. Фрилинг// Известия ТулГУ. - 2012,- Выпуск 3. - С.18 - 21.
7. Фрилинг В.А. Повышение износостойкости втулки балансира трактора МТЗ - 80.1 избирательной

электромеханической закалкой / Л.В. Федорова, А.В. Морозов, В.А. Фрилинг // Известия ТулГУ. - 2012,- Выпуск 9. - С. 18 - 21.
8. Фрилинг В.А. Повышение эффективности электромеханической закалки отверстий гладких цилиндрических подвижных сопряжений испытывающие одностороннюю радиальную нагрузку / Л.В. Федорова, А.В. Морозов, В.А. Фрилинг // Ремонт восстановление модернизация. - 2012. - №8. - С. 49 - 53.
9. Фрилинг В.А. Повышение износостойкости гладких цилиндрических подвижных сопряжений избирательной электромеханической закалкой отверстий / Л.В. Федорова, А.В. Морозов, В.А. Фрилинг // Вестник ФГОУ ВПО МГАУ. - 2012. - № 9. - с. 25 - 29.

УДК 651.012.12

В. Барабаш, канд. пед. наук, доцент
А. Бакала, магістр гр. ІС-20М (1,4)
Центральноукраїнський національний технічний університет

СИСТЕМА ХМАРНОЇ ТЕХНОЛОГІЇ ТА ЇЇ ВПРОВАДЖЕННЯ У ЖИТТЯ РІЗНИХ СФЕР

У статті досліджено ефективність впровадження хмарного зберігання (сховища) на підприємстві. А також її переваги та недоліки, що являють собою досить переконливі сторони того чи іншого збереження документації підприємства. Також висвітлено важливість вивчення питання, при впровадженні цієї системи збереження даних не тільки самого підприємства але і даних, що пов'язані із особливою та конфіденційною інформацією.
хмарна система, інформація, збереження, пам'ять, документообіг

Постановка проблеми. У функціонуванні підприємств, установ та інформаційних систем, існує потреба у кращому створенні, збереженні та передачі даних як документів, так і особистої інформації, що пов'язана з певною установою. Введення у діяльність ефективних та функціональних систем допомагає зміцнити не тільки саму структуру всередині установи, а й довести її до необхідної результативності у порівнянні з конкурентами. Система удосконалює працю з усіма етапами документа.

Аналіз останніх досліджень та публікацій. Невід'ємною частиною сучасного життя є технології, тобто сучасні технології. Разом з їх розвитком, зростаємо і ми. Важливого встигати за їх прогресом та удосконалювати своє життя у різних сферах роботи. Стосовно Хмарних технологій, розвитком цього питання займається Вишневецька Л.Є. [1], Вакалюк Т.А., Семеріков С.О. та інші.

Хмарні технології – це технологія, яка надає користувачам Інтернет доступу до комп'ютерних ресурсів і використання програмного забезпечення онлайн-сервіра., при цьому користувачеві не потрібно ніяких особливих знань про інфраструктуру «хмари» або навичок управління цією «хмарною» технологією. До переваг хмарних технологій слід віднести: відкритість освітнього середовища для користувачів; існує можливість використання відео і аудіо файлів прям з інтернету, без додаткового завантаження на комп'ютер; необмежений обсяг збереження даних; доступність з різних пристроїв і відсутня прив'язка до робочого місця; забезпечення захисту даних від втрат та інше [1].

Мета й завдання дослідження. Дослідження особливості введення хмарної технології та її специфіка виступає метою роботи. Завдання полягають у:

- Визначення особливості хмарної системи.
- Дослідити структури хмарного сховища та її види.
- Окреслити тенденції розвитку хмарних сервісів.

Об'єктом дослідження є система хмарної технології в різних сферах.
Предметом дослідження є функціонування та розвиток хмарної системи всередині установи.

Виклад основного матеріалу. Системи зовнішньої пам'яті значно розвивалися за свою історію. Дискети, DVD-диски, зовнішні жорсткі диски, USB-диски - всі ці технології швидко розвивалися і змінювалися разом з апаратною базою комп'ютерів.

Настав час оцифрування та віртуалізації. Це означає, що відбувається перехід від обладнання до функцій. Коли ми використовуємо сервіс каршеринга, це означає, що замість власного «апаратного» автомобіля ми фактично використовуємо його функцію «водіння».

Хмарне сховище – це віртуалізація вашої власної системи зберігання. Ваші дані зберігаються в хмарі на деяких пристроях, ви просто відправляєте дані в «хмару». Крім того, навіть інтерфейс системи хмарного сховища може бути дуже схожий на звичайний файловий менеджер на комп'ютері. Так працює хмарне сховище. Хмарна системи зберігання даних існує: внутрішня (приватна) чи зовнішня (публічна). Це забезпечує IT-інфраструктуру, яка дозволяє надійно та безпечно керувати серверами зберігання даних, яким потрібен постачальник хмарних послуг або просто «хмара» (приватна чи публічна).

Публічна хмара – це віртуалізована система зберігання даних, що надається зовнішнім постачальником. У його центрі обробки даних, дані багатьох клієнтів зберігаються в режимі кількох орендарів без перешкод. Ефективність витрат досягається за рахунок оптимального та централізованого використання ресурсів.

Приватна хмара: віртуалізоване сховище для всієї компанії. Він має спеціальний центр обробки даних (DPC), де зберігаються віртуалізовані дані інфраструктури та виконуються програми компанії. У цьому випадку більшість компаній беруть на себе роль постачальника хмарних послуг IT-послуг.

Приватні або публічні хмарні сервери працюють як одна група серверів у структурі хмарного сховища, а не як окремі системи. Для цієї мети пам'ять жорсткого диска віртуалізується за допомогою гіпервізорів та інших компонентів сервера. Гіпервізор більше не матиме фізичних серверів, процесорів і сховища даних, але матиме віртуальні сервери. Однак у них є приємна особливість: вони можуть адаптуватися до особливих вимог, можуть швидко мігрувати між фізичними серверами і навіть центрами обробки даних. Існує певна абстракція між реальним апаратом і функціями віртуального сховища, які називаються Virtual Machine Monitor (монітор віртуальної машини), також званий гіпервізором (гіпервізором). У будь-якому випадку віртуалізація пропонує гнучкість, легку масштабованість і легку зміну функціональних можливостей.

Структура хмарного сховища: для доступу до віртуальної пам'яті в хмарі зазвичай потрібне відповідне програмне забезпечення. Служби загальнодоступних хмар, як правило, включають не тільки веб-додаток, який можна використовувати через звичайний браузер, але й драйвери для доступу з різних пристроїв. З їх допомогою можна отримати доступ до хмари та отримати доступ до свого диска. До збережених там файлів можна отримати доступ через різні пристрої (комп'ютери, планшети, смартфони тощо), які підтримуються постачальником хмари.

Переваги хмарного сховища виступає багато причин для організації зберігання даних у зовнішній хмарі. Перш за все, це економія коштів на покупку та обслуговування власного серверного сховища. Існує загальна думка, що хмарні послуги так само дорогі або дорожчі, ніж локальне сховище. Щоб порівняти вартість обох варіантів, не варто робити розрахунки «з головою до голови», орієнтуючись лише на вартість «обладнання» та послуг хмарного провайдера. ТСО – це загальна цільова вартість від початку володіння до кінця володіння, а також загальна вартість власності. Експлуатаційні труднощі та аварії є переважною частиною «непрямих витрат». Однак при виборі місця для хмарного сховища вся відповідальність за основну інфраструктуру лягає на хмарного провайдера – це важливо враховувати при оцінці вартості його послуг.

Перевага хмарного сховища полягає в тому, що вихідні та резервні дані (які необхідно створити резервну копію) будуть розміщені в різних географічних місцях. Він захищає дані під час різних непередбачених ситуацій, які зазвичай трапляються в самий невідповідний момент: збій системи, пожежа, поломка обладнання.

Іншими перевагами хмарного сховища є: спритність – це можливість використовувати весь необхідний обсяг пам'яті. Якщо потрібно більше, постачальник робить його доступнішим - і плата збільшується. Якщо потрібно менше, постачальник робить його менш доступним, а плата зменшується. Під час пікового трафіку у системі завжди має бути максимальна потужність. У звичайному режимі ємність більше не використовується; вимірювання – за допомогою віртуалізації пам'яті можна вибрати необхідний обсяг пам'яті на основі контракту. Є можливість будь-коли збільшити або зменшити об'єм пам'яті, не купуючи, не встановлюючи або налаштовуючи обладнання; хмарне сховище доступне в будь-який час і з будь-якого пристрою (якщо є підключення до Інтернету). Таким чином, є можливість одержувати інформацію «на ходу», де і коли вона потрібна.

Недоліки хмарного сховища, перш за все вистурає залежність від підключення до Інтернету. У разі збою файли в хмарі не існують. Існуюча пропускна здатність залишається важливим фактором: навіть з найшвидшим сховищем доступ до даних буде повільним через низьку швидкість з'єднання. Особливо це стосується мобільних мереж, є й інші недоліки. Залежність від провайдера, якщо виникають проблеми з постачальником або якщо відбувається добровільна зміна умов договору, замовник може змінити постачальника, але це не миттєвий процес. Надсилання інформації через корпоративний брандмауер завжди є ризиком. Не всі постачальники пропонують послуги шифрування сховища. Хоча хороші постачальники завжди намагаються забезпечити найвищий рівень безпеки для своїх систем, інфраструктура провайдера є популярною мішенню для хакерських атак. Конфіденційність – ключове питання, яке потребує уточнення при укладанні контракту на хмарне сховище (яким чином захищені дані в інфраструктурі провайдера).

Вибираючи між приватною або загальнодоступною хмарою, завжди потрібно робити ретельний аналіз ТСО. Персональна хмара – термін, який багато обговорюється серед IT-спеціалістів: чи існує таке поняття – особиста хмара? Або це просто сховище інформації в системі компанії. Якщо для зберігання даних в корпоративній системі (локально) використовуються технології віртуалізації, то таке рішення по праву можна назвати персональною хмарою. Коли приватна хмара раптово закінчується, виникають проблеми: можливо перемістити деякі дані та програми у загальнодоступну хмару, щоб служити інструментом резервного копіювання та відновлення після аварій. Багато приватних хмарних компаній переносять деякі функції у загальнодоступну хмару, наприклад в ICloud корпоративна електронна пошта, послуги хмарного відеоспостереження тощо. Використовується хмара для збереження конфіденційності критично важливої для бізнесу інформації. .

Гібридне хмарне рішення поєднує переваги приватної та загальнодоступної хмари та може запропонувати такі переваги:

• вищий рівень управління;
• хороша «спеціалізація», тобто вміння налаштувати оптимальне рішення;
• економіка.

У багатьох випадках хмарне сховище може бути хорошою альтернативою традиційним рішенням локального зберігання.

Розвиток хмарних сервісів характеризується низкою характерних тенденцій. Перший – розширити хмарну пропозицію. Ми вже спостерігаємо зростання попиту клієнтів та пропозиції хмарних рішень від провайдерів – фінтех-компаній, інтеграторів та операторів зв'язку. Нові та існуючі гравці продовжують: вони оновлюють свої хмарні пропозиції, намагаються бути конкурентоспроможними та задовольняти потреби клієнтів, що ростуть.

По-друге, хмарна мережа. Зростаючий попит і пропозиція хмарних платформ і сервісів стимулюватиме розвиток мережевих сервісів між IT-системами різних компаній. Світовою тенденцією сьогодні є активне використання глобальних соціальних хмар, таких як Google Cloud, Microsoft Azure, Amazon Web Services. Транснаціональні корпорації все частіше передають свої дані в публічні хмари. У цьому контексті забезпечення

«підключення» та стійкості є головною метою дата-центру, щоб діяти як цифровий центр для клієнтів.

По-третє, протяжність хмар. Умови, за яких суспільство, зокрема економіка, вийшло з пандемії, підкреслили важливість технологічного прогресу в повсякденному житті. Відеоконференції та виставки, онлайн-лекції та семінари, універмаги та бібліотеки з відкритим кодом, телефонні дзвінки, покази фільмів – неповний перелік доступних послуг, які постійно розширюються. Ці послуги та функції вимагають збільшення потужності та обсягу хмарних обчислень, пропускної здатності мережі та надійності системи зберігання, що використовується для цих цілей.

Зрозуміло, що кожна наступна фаза ізоляції призведе до збільшення кількості видів транспорту.

Висновки. Отже, хмарні рішення мають велику кількість переваг: від ефективності витрат, до безпеки і гнучкості. Провайдери постійно оновлюють свої інструменти та роблять їх максимально технологічними і зручними. Клієнтам залишається тільки користуватись і насолоджуватись. Хмарами системами користуються також державні органи та останови, такі як: Prozorro, ДіЯ, EHealth, Нафтогаз України, Укрспірт, Міністерство Охорони Здоров'я, Дніпровська Державна Рада та інші, і з кожним місяцем цих підприємств стає все більше. Слід і приватним підприємствам, установам починати впроваджувати систему хмарного використання. Розвиток технології віртуалізації призвело до можливості створення віртуальної інфраструктури, гнучкого масштабування і нарощування систем, зниження витрат на організацію і супровід систем, доступності віртуальної інфраструктури через мережу Інтернет. Збільшення пропускної здатності мережі призвело до збільшення швидкості обміну даними, зниження вартості Інтернет трафіку, доступності хмарних технологій. Всі ці фактори призвели до підвищення конкурентоспроможності хмарних технологій в сфері інформаційних технологій.

Список літератури

1. Вишневецька л.є. Використання інформаційних технологій у професійній підготовці майбутніх фахівців.
2. Хмарні технології: [навч. посіб. / уклад. В. П. Вишневецька]. — К. : НПУ ім. М. П. Драгоманова, 2017. — 159 с.
3. Биков В. Ю. Теоретико-методологічні засади створення і розвитку сучасних засобів та е-технологій навчання / В. Ю. Биков // Розвиток педагогічної і психологічної наук в Україні 1992–2002 : зб. наук. праць до 10-річчя АПН України / Академія педагогічних наук України. – Частина 2. – Х. : ОВС, 2002. – С. 182–199.
4. Биков В. Ю. Хмарні технології, ІКТ-аутсорсинг і нові функції ІКТ підрозділів освітніх і наукових установ / В. Ю. Биков // Інформаційні технології в освіті. – №10. – 2011. – С. 8-23.
5. Вакалюк Т. А. Хмарний сервіс для створення документів з можливістю надання прав спільного доступу декільком користувачам / Т. А. Вакалюк // Психолого-педагогічні проблеми сільської школи : збірних наукових праць Уманського державного педагогічного університету імені Павла Тичини / [ред. кол. : Побірченко Н. С. (гол. ред.) та інші]. – Умань : ФОП Жовтий О. О., 2014. – Випуск 48. – С. 65–70.
6. Семеріков С.О. Хмарні технології навчання: витоки / О. М. Маркова, С. О. Семеріков, А. М. Стрюк // Інформаційні технології і засоби навчання. – 2015. – №2 (46). – С. 29-44. – Режим доступу до журн. : http://journal.iitta.gov.ua/index.php/itlt/article/view/1234/916#.VfFO4NLtmko.
7. Интеграция— основа облака [Электронный ресурс] / Л. Черняк // Открытые системы. СУБД (16 сентября 2011). – 2011. – №07. – Режим доступа к издательству : http://www.osp.ru/os/2011/07/13010473/.

УДК 556

А. Годорожа, магістр гр. ЕО-20МЗ
Центральноукраїнський національний технічний університет

УПРАВЛІННЯ ВОДНИМИ РЕСУРСАМИ В МЕЖАХ БАСЕЙНУ РІЧКИ ПІВДЕННИЙ БУГ НА ТЕРИТОРІЇ КІРОВОГРАДСЬКОЇ ОБЛАСТІ

У статті розглянуто сутність управління водними ресурсами за басейновим методом, якісний стан поверхневих вод в басейні річки Південний Буг на території Кіровоградської області. Мета – дослідити вплив впровадження принципу басейнового управління одними ресурсами, антропогенного навантаження на якість води масивів поверхневих вод в басейні річки Південний Буг на території Кіровоградської області.

Об'єкт дослідження – екологічний стан річок в басейні річки Південний Буг на території Кіровоградської області. Предмет дослідження - якість води масивів поверхневих вод в басейні річки Південний Буг на території Кіровоградської області. Методи дослідження: метод термінологічного аналізу, статистичний метод, структурний аналіз, абстрактно-логічний метод, балансовий метод, узагальнення, порівняльний метод. Результат роботи - розробка природоохоронних заходів з покращення екологічного стану поверхневих водних ресурсів з ренатуралізації річок області, з метою покращення якості поверхневих вод.

річковий басейн, водні ресурси, якість води, екологічний стан, басейновий принцип управління водними ресурсами

Постановка проблеми. Екологічні основи управління водними ресурсами України – важлива складова проблеми забезпечення вирішення водогосподарсько-екологічних проблем. Україна є однією з країн Європи, які найменш забезпечені власними водними ресурсами, і є одним із регіонів зі значним антропогенним навантаженням на водні джерела та нестачею у достатній кількості прісної води.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [9 - 17] було виявлено певні прогалини щодо дієвих механізмів досягнення гарного стану вод та покращення екологісчного стану річок.

Мета роботи – дослідити вплив впровадження принципу басейнового управління одними ресурсами, антропогенного навантаження на якість води масивів поверхневих вод в басейні річки Південний Буг на території Кіровоградської області.

Для реалізації зазначеної мети вирішені такі завдання: обґрунтувати необхідність басейнового принципу управління водними ресурсами; вивчити питання екологічного стану річок басейну р. Південний Буг; дослідити якості поверхневих вод.

Об’єктом дослідження є екологічний стан річок в басейні річки Південний Буг на території Кіровоградської області.

Предметом дослідження є якість води масивів поверхневих вод в басейні річки Південний Буг на території Кіровоградської області

Методи дослідження: метод термінологічного аналізу, статистичний метод, структурний аналіз, абстрактно-логічний метод, балансовий метод, узагальнення, порівняльний метод.

Водні ресурси України складаються зі стоку річок та прісних підземних вод. Ресурси місцевого річкового стоку, тобто стоку, що формується у річковій мережі на території країні, у середній за водністю рік становлять 52,4 млрд. м3, а в дуже маловодний рік 95 %-ої забезпеченості – 29,7 млрд. м3. [9].

Доступні для широкого використання водні ресурси формуються, в основному, в басейнах Дніпра, Дністра, Сіверського Дінця, Південного та Західного Бугу, а також малих

річок Приазов'я та Причорномор'я. Відповідно до ст. 1 Водного кодексу України, басейновий принцип управління – це комплексне (інтегроване) управління водними ресурсами в межах району річкового басейну. [8].

Наразі використання річкових екосистем продовжує мати екстенсивний та часто руйнівний для них характер, що проявляється у несвідомому, часто неправомірному, освоєнні річкової долини. До таких дій належать вирубка лісів, надмірне розорювання земель, несвідома господарська діяльність, будівництво житлових чи промислових об'єктів поблизу річок, що мають прямий вплив на забруднення річки та руйнування її русла. Така діяльність має ще більш негативні наслідки під впливом зміни клімату. Басейни малих річок практично позбавлені природних біофільтрів, оскільки їх водозбори або розорані майже до урізу води, або нищівно експлуатуються іншими способами, що забезпечує майже безперешкодне потрапляння поверхневого стоку безпосередньо до русла. [15].

Заходи, спрямовані на відновлення річок до їх початкового (природного) стану або до еталонного стану, можуть бути також спрямовані на досягнення окремих задач, таких як: підтримка біорізноманіття, покращення умов для рекреації, управління ризиками, пов'язаними із повенями, розвитку ландшафту, або виконання декількох задач водночас.

Річка Південний Буг належить до числа великих річок басейну Чорного моря і є однією із найбільших. Її басейн, площею 63 700 км2, повністю розташований у межах України, межує з басейнами Дністра (на заході) та Дніпра (на півночі та сході). Довжина річки – 806 км.

Басейн Південного Бугу розміщений на території семи областей України, найбільші частини площі припадають на Вінницьку (25,7%), Кіровоградську (24,2%), Миколаївську (23,2%) і Черкаську (13,2%). Невеликі частини річкового басейну розташовані у межах Одеської, Хмельницької та Київської областей.

У Кіровоградській області басейн р. Південний Буг знаходиться у межах лісостепової та степової зони Придніпровської височини та являє собою підвищену хвилясту рівнину, розчленовану густою мережею річкових долин, ярів та балок.

Багато річок басейну р. Південний Буг беруть свій початок на Кіровоградщині, зокрема це такі середні річки як Інгул, Велика Вись, Чорний Ташлик, Висунь. Майже вся річка Синюха (середня) протікає Кіровоградською областю.

У зв'язку із недостатньою водністю регіону, річки та балки значно зарегульовані.

Основним фактором формування в області поверхневого стоку є опади, які розподіляються зонально та зменшуються на південь. Внаслідок цього прослідковується чітка відповідність характеристик річкового стоку.

На формування стоку та якість води значно впливає господарська діяльність. В посушливий рік сформовані місцеві водні ресурси практично регулюються створеними ставками і водосховищами. Значна розораність водозборів річок, особливо в степовій південній частині області, викликає підвищену мутність води до 500г/м3, що спричиняє замулення річок і водойм. Однією з причин забруднення поверхневих вод є скиди підприємствами забруднених вод.

Вода Південного Бугу вирізняється також доволі високою насиченістю розчиненим киснем. Чинником, що сприяє покращенню кисневого режиму, є наявність порожистих ділянок, де відбувається перемішування води.

Характерною особливістю басейну Південного Бугу, що виділяє його з поміж інших великих річок, є велика зарегульованість. Всього в басейні річки на території області налічується 46 водосховищ та 2148 ставків. Сумарний об'єм штучних водойм становить близько 264,98 млн.м^3**.**

Значення показників вмісту забруднюючих речовин характеризують поверхневі води як такі, що забруднені органічними речовинами. Їх вміст зростає в липні – серпні, в період підвищення температури, збільшення випаровування та малої водності річок. У всіх створах спостерігаються високі значення показників БПКп. Скидання стічних вод у річки та водойми

без належної очистки, внаслідок неефективної роботи очисних споруд та їх відсутності, сприяє забрудненню водних об'єктів.

В цілому, якість води на питних водозаборах області, за фізико-хімічними показниками, задовільна. Винятком є пункти моніторингу з підвищеною мінералізацією. Проте, вміст біогенних елементів групи азоту та фосфору, завжди знаходяться в межах оптимальних значень. Розчинений у воді кисень, має властивість змінюватися протягом року, в залежності від пори року. Влітку концентрація кисню значно менша ніж взимку. Така сама тенденція і з показниками органічного забруднення води ХСК та БСК.

Одним із важливих факторів поліпшення якості води є опади, але враховуючи останні роки (відсутність опадів) маємо картину, що вказує на поступове погіршення показників сольового складу води.

Вода річок Інгулець, Сухоклія та Чорного Ташлика має високу природну мінералізацію. Протягом останні п'яти років спостерігається чітка тенденція підвищення показників, які формують сольовий склад води. Враховуючи те, що в Кіровоградській області практично відсутні підприємства, які скидають високо мінералізовані стічні води, основною причиною зростання цих показників є природній фактор, а саме висока температура повітря у весняні і літні місяці та відсутність достатньої кількості опадів протягом року.

Однією з головних причин незадовільної якості води водних об'єктів є забруднення біогенними елементами (сполуками азоту та фосфору). Наявність підвищеної кількості поживних елементів є рушійною силою євтрофікації вод, яка проявляється у неконтрольованому підвищенні біомаси фіто- і зоопланктону, вищих водних рослин та порушенні природної рівноваги біологічної продуктивності. Наступне за цим розкладання відмерлих решток значної маси гідробіонтів спричинює активне споживання кисню на їх окиснення і подальше накопичення патогенної мікрофлори та специфічних токсинів. Внаслідок цього погіршуються органолептичні показники води та санітарно-гігієнічний стан водного об'єкта, створюються умови для виникнення задухи, а вода у цілому стає непридатною для питного і господарського користування. Загалом процес євторофікації протікає у річках в період літніх місяців. Перевищення норм по показниках біогенних елементів сполук фосфору та азоту не спостерігається, але в період літніх місяців збільшується їх кількість.

Розчинений у воді кисень протягом багатьох років знаходиться в межах оптимальних значень. Так у зимові місяці значення розчиненого кисню значно вище ніж влітку.

Слід звернути увагу на зростання показника органічного забруднення води ХСК. Ще п'ять років назад, цей показник мав менші значення ніж зараз. Хімічне споживання кисню - це кількість кисню, необхідна для хімічного окиснення неорганічних і органічних речовин. Різке зростання ХСК води свідчить про забруднення водойми. Величина ХСК є важливою гігієнічною характеристикою води, яка дозволяє судити про забрудненість води окисленими речовинами, але не дає інформації про склад забруднення.

Висновки. Отже заходи з відновлення річок мають довгостроковий характер та мають на меті: Рекомендовано, аби питання відновлення річок у масштабах всього водозбору розглядали як частину комплексного стратегічного плану, наприклад, як складову Плану управління відповідним річковим басейном. Такий підхід забезпечить вирішення проблем річкової системи як єдиного цілого. Зосередження уваги на окремих заходах, не беручи до уваги стан речей на водозборі в цілому, може призвести до згубних наслідків в інших місцях річкового басейну. Заходи з відновлення можна поділити на ті, що стосуються безпосередньо самої річки та її заплави, та на заходи щодо покращення екологічного стану на водозборі.

Список літератури

1. Якість води та управління водними ресурсами: короткий опис Директив ЄС та графіку їх реалізації. Проект ЄС «Додаткова підтримка Міністерства екології та природних ресурсів України у впровадженні

Секторальної бюджетної підтримки» – Режим доступу: http://buvrtysa.gov.ua/newsite/download/Water_brochure.pdf.
2. Методика екологічної оцінки якості поверхневих вод за відповідними категоріями. – К.: «Символ-Т», 1998. – 28 с..
3. Методика встановлення і використання екологічних нормативів якості поверхневих вод суші та естуаріїв України. – К., 2001. – 48 с.
4. Досвід використання «Методики екологічної оцінки якості поверхневих вод за відповідними категоріями» (пояснення, застереження, приклади) / А.В. Яцик, В.М. Жукінський, А.П. Чернявська, І.С. Єзловецька. – К.: «Оріяни», 2006. – 60 с.
5. Методика картографування екологічного стану поверхневих вод України за якістю води. – К.: «Символ-Т», 1998. – 48 с.
6. Методичне керівництво по розрахунку антропогенного навантаження і класифікації екологічного стану малих річок України НТД 33-4759129-03-04-92. – К.: Мінприроди України, Держводгосп України, 1992 – 40 с.
7. Методика екологічної оцінки якості поверхневих вод за відповідними категоріями. – К.: «Символ-Т», 1998. – 28 с.
8. Стратегія розвитку Кіровоградської області на 2021-2027 роки, Звіт з оцінки результативності реалізації Стратегії розвитку Кіровоградської області на період до 2020 року за січень-вересень 2020 року, доступ: http://economika.kr-admin.gov.ua/index.php?action=invest
9. Хільчевський В.К. Гідрографічне та водогосподарське районування території України, затверджене у 2016 р. – реалізація положень ВРД ЄС / В.К. Хільчевський, В.В. Гребінь // Гідрологія, гідрохімія і гідроекологія. – 2017. – Т. 1. – С. 8–20. – Режим доступу: http://nbuv.gov.ua/UJRN/glghge_2017_1_3
10. Чернявська А.П. Екологічна оцінка та встановлення екологічних нормативів якості води стосовно Десни в межах України // Гідрологія, гідрохімія і гідроекологія. – 2001. – Т. 2. – С. 702–712.
11. Нежиховский Р.А. Наводнения на реках и озерах. – Л.: Гидрометеоиздат, 1988. – 184 с.
12. Яцик А.В. Екологічна ситуація в Україні і шляхи її поліпшення, К.: «Оріяни», 2003 – 96 с.
13. Наукові засади раціонального використання водних ресурсів України за басейновим принципом: монографія / За редакцією В.А. Сташука; [В.А. Сташук, В.Б. Мокін, В.В. Гребінь, О.В. Чунарьов]. – Херсон: Грінь Д.С., 2014. – 320 с.
14. Воронов Ю.В., Яковлев С.В. Водоотведение и очистка сточных вод. – М.: Изд-во Ассоциации строительных вузов, 2006. – 704 с.
15. Дьомін М.М. Сучасні проблеми екосистеми малих річок / М.М.Дьомін, О.О.Михайлик // Містобудування та територіальне планування: наук.-техн. збірник. – К.:КНУБА, 2018. – Вип.68. – С.140-14
16. Руденко Л.Е., Яцик А.В., Денисова О.І., Серебрякова Т.М., Чернявська А.П. та ін. Екологічна оцінка сучасного стану поверхневих вод України // Укр. геогр. журн. – 1996. –№ 4. – С. 3–13.
17. Дубняк С.С., Дубняк С.А. Оцінка стану і проблеми законодавчого регулювання водоохоронних зон водних об’єктів України // «Гідрологія, гідрохімія і гідроекологія»: Наук. збірник. – К.: ВГЛ «Обрії», 2005. – Том 7. – С. 25–39.

УДК 651.012.12

О. Коломієць, канд. пед. наук, доцент
О. Гордієнко, магістр гр. ІС-20М (1,4)
Центральноукраїнський національний технічний університет

ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ЗАКЛАДАХ ОСВІТИ

У статті досліджено основні підходи до використання електронного документообігу в закладах освіти. Також висвітлено електронний документообіг в його постійній видозміні, створення та реєстрація електронних документів на основі використання комп'ютерних мереж. Акцентується на основних функціях системи електронного документообігу та перевагах його використання.
електронний документообіг, електронний документ, сфера освіти, заклад освіти

Постановка проблеми. Надзвичайно швидкі темпи розвитку комунікаційних та інформаційних технологій вимагають належних змін від основоположних соціальних

інститутів суспільства в цілому та державного управління зокрема, адже державне управління має встигати за змінами, відповідати сучасному ритму життя [1].

В умовах розбудови сучасної України як демократичної та правової держави реформи визнані найкращим методом прогресивного розвитку суспільства, де одним із головних пріоритетів є розвиток інформаційного суспільства зі стрімким поширенням новітніх інформаційних технологій, а також інтенсифікацією інформаційних зв'язків. Потрібно побудувати інноваційну, високотехнологічну модель суспільства, у якому будь-який громадянин має змогу нагромаджувати і створювати знання та інформацію, мати до них вільний доступ, обмінюватися та користуватися ними, аби дати можливість кожній людині повною мірою реалізувати особистий потенціал для поліпшення якості рівня життя та забезпечення суспільного розвитку. Стрімке збільшення масштабів інформації, яка використовується в різних сферах управлінської діяльності, зокрема: освітній, медичній, правовій, її складність та швидке оновлення, обумовлює необхідність застосовування інтегрованих систем документообігу, які в сучасних умовах стали не просто засобами оптимізації внутрішніх процесів підприємств чи установ, а й основою стрімкого розвитку новітніх інформаційних технологій. Отже, одним із актуальних завдань в Україні є розвиток інфраструктури електронного документообігу

Аналіз останніх досліджень та публікацій. Проблеми впровадження електронного документообігу в освітній сфері на сучасному етапі є предметом уваги багатьох науковців (Л. Л. Прокопенко, Т. М. Тарасенко, М. Н. Бобильова, Ю. Г. Вітін, В. І. Тихонов, М. Н. Цивін, М. В. Ларін, О. В. Матвієнко, І. Ф. Юшин, А. В. Якіменко та ін.). У спеціальних дослідженнях розглядаються, зокрема, такі питання: збереження електронних документів на підприємствах; нормативно- методологічне регулювання, впровадження електронного документообігу; використання закордонного досвіду впровадження електронного документообігу на вітчизняних підприємствах. Однак низка важливих питань щодо впровадження та використання електронного документообігу в галузі освіти потребує додаткового дослідження.

Мета й завдання дослідження. Метою дослідження є аналіз особливостей впровадження електронного документообігу в закладах освіти.

Для досягнення поставленої мети визначено такі завдання:

– дослідити основні концептуальні основи електронного документообігу;

– визначити основні функції систем, якими забезпечується електронний документообіг;

– визначити роль та специфіку використання електронного документообігу в закладах освіти.

Об'єктом дослідження є електронний документообіг.

Предметом дослідження електронний документообіг в закладах освіти, його основні функції та переваги використання.

Виклад основного матеріалу. Електронний документообіг являє собою сукупність процесів зберігання, передавання, відправлення, створення, оброблення, одержання, застосування та ліквідації електронних документів, які циркулюють на підприємстві чи організації, на основі використання комп'ютерних мереж. Під управлінням електронним документообігом слід розуміти організацію «руху документів» між підрозділами організації або підприємства, між окремими користувачами чи групами користувачів. При цьому «рух документів» означає не їхнє фізичне переміщення, а передачу прав на їх застосування із повідомленням до конкретних користувачів та контролем за їхнім здійсненням. Також документообіг тлумачать як створення інформаційної бази документів на різних носіях для застосування управлінським апаратом у процесі виконання функцій.

Впровадження електронного документообігу в Україні регламентується низкою законів та підзаконних актів, які створюють базу нормативно-правового регулювання електронного документообігу. Це, зокрема, Закони України: «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг», «Про захист

інформації в інформаційно-телекомунікаційних системах», «Про Національну програму інформатизації», «Про обов'язковий примірник документів», «Про Національну систему конфіденційного зв'язку». Таким чином, електронний документообіг є законодавчо підкріпленим та доволі поширеним у державних установах та на підприємствах України процесом.

Відповідно до Закону України «Про електронні документи та електронний документообіг» встановлено, що електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа, зокрема електронного підпису [1]. Електронний документообіг у сфері освіти – це високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи різноманітних освітніх рівнів.

В Україні за підтримки проєкту USAID «Альянс сприяння прозорому управлінню освітою в Україні – UTEMA» впроваджується електронний документообіг у Міністерстві освіти і науки України. У проєкті визначена стратегія поетапного переходу до системи електронного документообігу та управління – спершу в межах міністерства, а згодом в інших закладах освітньої галузі. Базою систем електронного документоозігу у сфері освіти взято систему електронного документообігу Адміністрації Президента України, яку безкоштовно пристосують під вимоги Міністерства освіти і науки України.

Система електронного документообігу Адміністрації Президента України дозволяє паралельно працювати над одним документом та уникати його дублювання, що суттєво збільшує оперативність виконання роботи. Тобто державний службовець може віднайти документ за темою, номером або контекстом, встановити відповідального за його розроблення, а також побачити статистику затримки у роботі з документом співробітниками. Подібний контроль реалізації документа на всіх стадіях робить підготовку документів більш керованою та прогнозованою.

Уведення системи електронного документообігу передбачає опрацьовування документів, яке буде існувати та здійснюватися в електронному вигляді, майже без паперів, коли вхідна та вихідна кореспонденція зберігається в єдиній системі, а документ підписується індивідуальним електронним цифровим підписом. Це означатиме, що головним робочим інструментом співробітника є його робочий комп'ютер, а матеріальне переміщення документів «на підпис» зведеться до мінімуму. Електронний документообіг покликаний удосконалити якість управління в освітній сфері.

Головні завдання електронного документообігу:

- зменшення затрат часу на пошук інформації;
- гарантія збереження документа;
- скорочення термінів затвердження та погодження документів;
- підтримка повного життєвого циклу інформації;
- перехід на безпаперовий метод діяльності;
- створення єдиного інформаційного простору для зберігання і роботи з усіма видами документів у Міністерстві освіти та науки Україні (подолання інформаційного безладу);
- підвищення контролю виконавської дисципліни та прозорості руху документів.

Головним завданням Міністерства освіти та науки України є створення найкращої системи забезпечення електронного документообігу в закладах освіти (ЗО). Суттєвими проблемами цієї ситуації є, по-перше, велика кількість різних видів документів (як зовнішніх, так і внутрішніх) у ЗО, що істотно ускладнює роботу системи, а по-друге, надзвичайно швидкий розвиток інформаційних технологій, які, зі свого боку, призводять до втрати актуальності минулих досліджень зі стрімким розвитком технічного прогресу.

ЗО потрібно досліджувати як велику організацію, яка є незмінною багатопрофільною територіально розподіленою структурою, що має всі необхідні адміністративні системи життєзабезпечення і діє на принципах децентралізованого управління. Саме тому можна засвідчити, що інформаційна система ЗО має бути корпоративною системою управління, яка

б забезпечувала інтеграцію всіх головних ділових процесів організації і перепроваджувала їх у площину комп'ютерних технологій, мала можливість об'єднатися з іншими системами, а також складалася із підсистем, що вдосконалювали б її діяльність. Для автоматизації електронного документообігу ЗО необхідно попередньо дуже добре вивчити технологію виконання головних процедур, які є змістом документообігу та діловодства загалом.

Відомо, що з 2016 р. в Україні запроваджено революційні зміни у сфері державних закупівель: усі торги з використанням державних коштів здійснюються на єдиному вебпорталі державних закупівель Prozorro, і це, безумовно, також впливає на розвиток електронного документообігу в закладах освіти [3].

Електронний документообіг у ЗО забезпечуватиме:

– одноразову реєстрацію документа в системі;

– можливість паралельного виконання різних операцій з метою зменшення часу руху документів, а також збільшення оперативності їх виконання;

– безперервність руху документа;

– функціонування єдиної бази документальної інформації для централізованого зберігання документів;

– унеможливлення дублювання документів (зберігання в системі копій);

– ефективно організовану систему пошуку документа в базі;

розвинену систему звітності за статусами, атрибутами і датами документів, що дозволяє контролювати поетапний рух документів [2].

Необхідно зазначити, що застосування електронного документообігу в ЗО не є важким процесом, адже не вимагає від користувачів знань мов програмування або якихось нюансів використання інформаційних технологій. Проте є ряд труднощів, яких зазнає ЗО під час уведення систем електронного документообігу в дію. Для роботи системи документообігу ЗО варто сформувати передумови, необхідні для переходу до системи організації електронного документообігу:

– розуміння керівництвом необхідності надавати більше уваги

обробці документів. Погоджувати, стверджувати, шукати й, зрештою, аналізувати документи зручно, коли маєш усі їх в електронному вигляді;

– розвиток систем автоматизації бізнес-процесів, який забезпечить появу на ринку комплексних платформ управління бізнес-процесами та документами;

– поліпшення ситуації із забезпеченням безпечного доступу територіальних підрозділів до інформаційних систем центрального апарату організації;

– розвиток інтеграційних технологій;

– поширення технологій електронного цифрового підпису.

Основними проблемами систем електронного документообігу в ЗО, на нашу думку, є такі:

– бази даних не мають гнучкої і функціональної структури, інформація часто зберігається у спеціалізованих базах даних, а не на електронних носіях в архівах, тобто захист мінімальний, крім того, при зберіганні електронного документа можливе його псування чи видозміна, тому потрібна розробка такої бази даних, яка б мала власний захист (найчастіше надають перевагу системам MSSQL);

– система не має (особливо в підрозділах бухгалтерії, відділах кадрів) розмежованого доступу до інформації для відповідних користувачів за рахунок використання різних засобів захисту інформації;

– документи вважаються дійсними за наявності обов'язкових реквізитів, а також електронного підпису та графи про зміну чи доповнення цього документа,

хоча на сьогодні законодавчо затверджений перелік таких реквізитів відсутній, що, зі свого боку, ускладнює уведення системи електронного документообігу в дію;

– складність переведення документів з паперового носія та обробка отриманої інформації в графічному вигляді, що вирішується за допомогою скануючого обладнання або набору кожного шаблону документа вручну. Процес сканування є досить швидким, проте

подальше розпізнавання електронного графічного файла в дані, придатні для обробки комп'ютерною програмою, як і набір документа вручну, займає досить багато часу та потребує значних затрат праці.

Незважаючи на проблеми систем електронного документообігу, в ЗО є ряд основних переваг від упровадження систем електронного документообігу для конкретного співробітника, що працює з документами:

– перехід до більш зручного, швидкого й економного безпаперового юридично важливого документообігу;
– поліпшення процедур підготовки, доставлення, зберігання та обліку документів, їх автентифікація, неспростовність, цілісність і конфіденційність;
– особистий кабінет документів (від дати створення і до втрати чинності);
– паралельна робота над документом;
– єдиний шаблон документів;
– швидкий процес узгодження проєктів.

Під час відбору системи електронного документообігу у ЗО висуваються такі головні вимоги: адаптивність (система змогла б підтримувати будь-яку кількість користувачів), можливість розподілятися (система могла б підтримувати роботу з документами одночасно у відділах та ЗО), відкритість (практичний, відкритий інтерфейс для можливого подальшого опрацювання та інтеграції з іншими розподіленими системами) та модульність (коли, наприклад, користувачеві системи не потрібно відразу впроваджувати всі компоненти системи документообігу) [5]. Таким чином, система повинна мати механізм збереження електронних копій документів, гнучкий механізм відбору та пошуку даних, механізм формування друкованих форм усіх необхідних документів, аналітичних та статистичних звітів тощо.

Висновки. На сучасному етапі важливість інформатизації, зокрема електронного документообігу, важко переоцінити. Впровадження електронного документообігу в освітній сфері покликано вдосконалити якість управління, а саме зменшити часові витрати на пошук інформації, скоротити рівень бюрократизації під час затвердження та погодження документів, відійти від паперового ведення справ тощо.

Документообіг в установі є системою, яка втілить процеси зберігання, перетворення, збирання інформації, а ще допоможе реалізувати такі процеси управління, як: підготовка, прийняття та контроль за виконанням рішень. Запровадження інтегрованої системи електронного документообігу значно поліпшить усі ці процеси, саме тому її мета та призначення як елемента електронного урядування є надзвичайно важливими і мають посідати відповідне місце вже зараз.

Таким чином, використання електронного документообігу у сфері освіти сприяє оптимізації роботи системи, гарантує прозорість, зменшує витрати часу на роботи з паперовими документами. Електронний документообіг допомагає створити у ЗО єдиний інформаційний простір, інтегруючи в інформаційний вузол усі документальні системи. Інтеграція відбувається без втрати якості роботи. Впровадження системи електронного документообігу у ЗО, на нашу думку, здійснюється не настільки інтенсивно, як мало би бути, але можна стверджувати, що через певний час системи електронного документування будуть мати великий попит.

Одним із найважливіших завдань для подальших наукових розвідок з упровадження електронного документообігу є дослідження програмних продуктів для нього та вдосконалення інтернет-ресурсів для його реалізації.

Список літератури

1. Документообіг в навчальному підрозділі ВуЗу. URL: http://referaty.net.ua/referaty/ referat_62053.html.
2. Застрожнікова І. В. Зарубіжний досвід електронного урядування сфери освіти в Україні. Наук. вісн.: державне управління. 2020. № 2(4). С. 160 – 168. DOI: https://doi.org/ 10.32689/2618-0065-2020-2(4)-160-167.
3. Застрожнікова І. В. Система електронних державних закупівель у навчальних закладах України. Сучасні

технології в умовах освітньої парадигми інформаційно- комунікативного суспільства сб. тез доповідей Міжнар. наук.-практ. конф., м. Запоріжжя, 26 листоп. 2018 р. URL: http://elar.tsatu.edu.ua/handle/123456789/6086.
4. Застрожнікова І. В. Ульянченко Ю. О. Сучасний стан державного регулювання освітніх новацій в Україні. Акрутальні проблеми державного управління: сб. наук. пр. 2019. № 2(56). С. 192 – 198.
5. Ткачук Г. І. Використання електронної системи документообігу у НЗ. Магістратура в умовах євроінтеграційних процесів вищої школи. Житомир: ЖДУ, 2014. 254 с.
6. Прокопенко Л. Л., Тарасенко Т. М. Виховання та соціальний розвиток молоді як об'єкт впливу держави. Аспекти публічного адміністрування. 2014. № 1 – 2(3 – 4). С. 70 – 77.

УДК 574:631.1

Л. Коломієць, доцент
М. Доля, магістр гр. ЕО-20м
Центральноукраїнський національний технічний університет

ВПЛИВ НА ДОВКІЛЛЯ ТА ЕКОЛОГІЗАЦІЯ ПРОЦЕСІВ ПІДПРИЄМСТВ ТЕПЛОЕНЕРГЕТИКИ

Проаналізовано питання впливу підприємств теплоенергетики на об’єкти довкілля та запропоновано шляхи екологізації їх діяльності
теплоенергетика, утилізація, зола, шлак, осади стічних вод

Актуальність. Екологічна ситуація в Україні характеризується високим рівнем антропогенного впливу на навколишнє середовище і значними екологічними наслідками минулої економічної діяльності. У зв'язку з гострою необхідністю термінових змін підходів до забезпечення якості навколишнього середовища і збереження здоров'я населення в нашій країні з 2014 року активно розробляються і вводяться в дію нове природоохоронне законодавство і численні екологоорієнтовані нормативно-правові акти, які впроваджують нові механізми управління охороною навколишнього середовища. Паливно-енергетичний комплекс відноситься до галузей з найбільшим негативним впливом на навколишнє середовище, зокрема, це підприємства (об'єкти) паливно-енергетичного комплексу для забезпечення електричною енергією, газом і паром з використанням обладнання з встановленою електричною потужністю 250 МВт і більше при споживанні в якості основного твердого та (або) рідкого палива або зі встановленою електричною потужністю 500 МВт і більше при споживанні в якості основного газоподібного палива, тобто всі великі теплові електростанції.

Постановка проблеми. Відбувається накопичення різних видів відходів, що призводить до погіршення стану об’єктів довкілля, тому актуальним є оптимізація системи поводження з відходами. В Україні накопичено величезну кількість промислових відходів, що забруднюють довкілля та займають значні площі. До таких відходів слід віднести відходи від спалювання твердих горючих копалин (вугілля) – золошлакові матеріали золовідвалів, а також полімерні матеріали.

Мета дослідження. Визначити основні напрями утилізації відходів, що утворилися в процесі енерговиробництва.

Завдання:

- вивчити вплив підприємства теплоенергетики на довкілля
- з’ясувати можливість утилізації відходів осадів стічних вод без шкоди для довкілля
- запропонувати шляхи оптимізації використання золи, що утворюється від спалювання вугілля

Об'єкт дослідження: Вплив на довкілля технологічних процесів підприємства теплоенергетики.

Предмет дослідження: Утилізація відходів підприємства теплоенергетики.

Результати досліджень. ТОВ Теплоенергоцентр (м. Кропивницький) забезпечує постачання теплової енергії у відповідній кількості та якості згідно з вимогами договору до межі зовнішніх інженерних мереж постачання послуги виконавця та внутрішньобудинкових систем багатоквартирного будинку (індивідуального (садибного) будинку). Контроль якісних та кількісних характеристик послуги здійснюється за показаннями вузла (вузлів) комерційного обліку теплової енергії та іншими засобами вимірювальної техніки ТОВ Теплоенергоцентр (м. Кропивницький).

Безперебійне виробництво електричної та теплової енергії забезпечують основні цехи підприємства – котлотурбінний та електротехнічний.

Одна з причин взаємодії ТОВ Теплоенергоцентр (м. Кропивницький) з водним середовищем – це споживання води системами технічного водопостачання, в тому числі, безповоротне споживання води. Основна частина витрат води потрібна для того, щоб охолоджувати конденсатори парових турбін. Решта споживачів технічної води (системи золо- та шлакоусунення, хімводоочищення, охолодження і промивки обладнання) можуть споживати близько 7% загальної витрати води [1].

Теплова станція може бути головним джерелом забруднення об'єктів довкілля. Наприклад, при промиванні поверхонь нагріву котлоагрегатів серійних блоків ТОВ Теплоенергоцентр (м. Кропивницький) потужністю 300 МВт виділяється до 10000 м3 розбавлених розчинів соляної кислоти, їдкого натру, аміаку, солей амонію. Крім цього, в стічних водах ТОВ Теплоенергоцентр (м. Кропивницький) міститься ванадій, нікель, фтор, феноли і нафтопродукти.

Скидання стічних вод на ТОВ Теплоенергоцентр (м. Кропивницький) здійснюється відповідно до графіка скидання, узгодженим в установленому порядку. Скидання стічних вод узгоджений за умови непогіршення фонових показників забруднюючих речовин в річку Інгул.

Саме тому запропоновано два кроки поліпшення утилізації відходів виробництва. Застарілі методи утилізації та переробки осаду стічних вод продуктів енергетики негативно впливають на економіку підприємств. З огляду на літературні джерела є кілька шляхів вирішення цього питання. Традиційний підхід – це використання мулових майданчиків для поховання осаду стічних вод.

Причому цей осад містить багату складову, зольність сирих опадів становить середньому 25-40%, а зольність надлишкового мулу – 25-30%. Органічна складова надлишкового мулу містить до 50% білків, 30% жирів та до 10% вуглеводнів. До складової органічної частини сирих опадів входить приблизно вдвічі менше білків, але в 2,5-3 рази більше вуглеводнів, слід зазначити також велику бактеріальну забрудненість опадів та наявність у них значної кількості яєць гельмінтів [2].

Розглядається можливість перетворення осаду на комплексне добриво знешкодженням осаду стічних вод в умовах біосульфідогенезу при дисиміляційному відновленні малорозчинних сульфатів. Отримані результати узгоджуються з експериментальними даними, що відповідають динаміці вихідного біореактора біогенного газу. За характером зміни кінетики виходу біогенного сірковуглецю, зміни концентрації ацетату та швидкості поглинання сульфатів можна здійснювати прогноз процесу біосульфідогенезу та знаходити найбільш оптимальні параметри системи. Це вказує на можливість його використання в біотехнології знешкодження осаду стічних вод при централізованому відведенні стоків з отриманням комплексного органо-мінерального добрива [3].

Існує певний досвід використання осадів таких вод під час централізованого відведення стоків у дорожньому будівництві. Результати натурних досліджень експериментальних асфальтобетонних покриттів, модифікованих техногенними відходами

(осадом стічних вод), свідчать про їхню високу якість, не поступаючись своїм показникам покриттю з традиційного асфальтобетону [4].

Оцінюючи утилізацію осаду стічних вод, можна відзначити, що альтернативною є технологія утилізації осаду стічних вод в органо-мінеральний порошок з подальшим залученням отриманого на його основі асфальтобетону в дорожньому будівництві, за економічними та екологічними показниками даний метод, має перевагу над методом термічної обробки.

На малюнку 1, згідно з розглянутою проблемою питання знешкодження осаду стічних вод, проаналізовано ситуацію на прикладі ТОВ Теплоенергоцентр (м. Кропивницький).

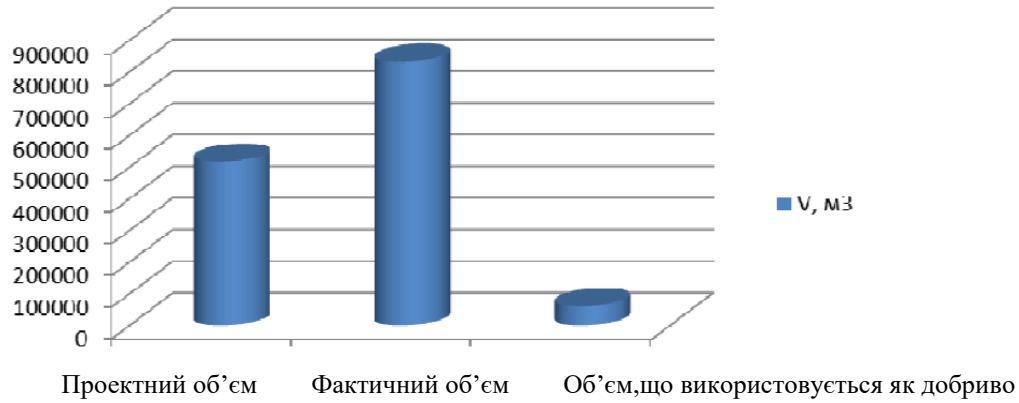


Рисунок 1 – Накопичення осаду відходів підприємства ТОВ Теплоенергоцентр (м. Кропивницький) у стічних водах [5].

Як бачимо обсяги зневодненого до 74% осаду, що утворюється на мулових майданчиках, звідки вивозиться як добриво на сільськогосподарські будівлі і загальний обсяг накопиченого осаду незрівнянно малі.

Розглядається також можливість вирішення екологічної утилізації відходів з метою одержання регуляторів росту рослин за допомогою метанового зброджування. Ці регулятори здатні викликати в організмі рослини зміни в обміні речовин, керувати їх зростанням та розвитком [6].

Раніше метод спалювання затримувала висока вологість осаду (понад 70%). Зараз використання нових сушарок для підсушеного осаду на мулових майданчиках вологістю 60-70% дозволяє зменшити його вологість до 25% і нижче. Таким чином, через метод новітнього способу спалювання осаду турбосушарках можна ліквідувати джерело парникового ефекту, який виникає при застарілій технології утилізації методом зневоднення осаду на мулових майданчиках, отримання альтернативного джерела теплової та електричної енергії. При такій потужній термічній обробці в 13 разів зменшується обсяг зневодненого осаду (з 15,6 т/год до 1,2 т/год), а 90% попелу може бути використане в цементній промисловості, виробляється приблизно 1,5 МВт/год електроенергії та 35000,0 Гкал/рік теплової енергії [7].

Приходимо до висновку, що серед розглянутих напрямів утилізації останнім часом поширеного використання набирає метод спалювання один з радикальних методів утилізації осаду, тому ми пропонуємо саме його для оптимізації системи поводження з відходами на підприємстві ТОВ Теплоенергоцентр (м. Кропивницький).

Також, за для запобігання забруднення ґрунтів у районі дослідження пропонуємо впровадження нової схеми уловлювання золи. Існуюча на ТОВ Теплоенергоцентр (м. Кропивницький) схема пиловловлювання не підходить для встановлених задач.

Технологія глибокої та повної переробки золи вуглеспалювання як альтернатива традиційному накопиченню та складуванню

Насамперед золу необхідно звільнити від сторонніх домішок, шлакових зростків тощо, для чого її необхідно класифікувати, наприклад, за класом – 200 мкм. Потім у

більшості випадків із золи необхідно видалити вуглецеву фракцію, так як для більшості видів сировини (наприклад, для виробництва бетонів) важливе значення має такий показник, як при прожарюванні, які не повинні перевищувати 2%. Великі класи можна використовувати для відсипання місцевих доріг. Класи – 200 мкм, кількість яких у ЗШО зазвичай становить 90-92%, можуть бути спрямовані на 100% переробку за технологією.

По кожному блоку розроблено схеми ланцюга апаратів, вибрано основне технологічне обладнання та складені матеріальні баланси по сухій речовині та водношламові баланси.

Подана схема переробки золи передбачає отримання вуглецевого та магнетитового концентратів, алюмосилікатного продукту, білітових шламів, а також глинозему – дефіцитної сировини для виробництва алюмінію

На першому етапі переробки золи (блок переробки фізичними методами) передбачається її гідрокласифікація, необхідна виділення дрібних фракцій, які у деяких випадках заважають процесам флотації і магнітної сепарації. У той же час тонкі та надтонкі фракції являють собою дефіцитний продукт для використання як наповнювачів у виробництві особливо міцних бетонів.

У блоці переробки фізичними методами із золи флотацією виділяється вуглецевий концентрат, придатний за якістю повернення його в котел в якості додаткового палива. Тим самим підвищується повнота використання вугілля та знижуються його втрати, пов'язані з недопалом. Алюмосилікатний продукт, що містить менше 5% вуглецю, затребуваний будівельною промисловістю як наповнювач бетонів та інших матеріалів.

Після виділення вуглецевого концентрату методом мокрої магнітної сепарації на електродинамічному сепараторі із золи може бути вилучена магнітна фракція, що містить до 56-58% Fe_2O_3 (при додаткових перечистках отриманий магнетитовий концентрат, що містить 72-76% Fe_2O_3).

Відходи збагачення золи (зольный концентрат), що є очищений від вуглецю і заліза алюмосилікатний продукт (приблизно 70-80% $A_{12}O_3$), разом з дрібною фракцією направляється на подальшу переробку. Для золи ТОВ Теплоенергоцентр (м. Кропивницький) найбільш раціональним є «недопал» і переробка їх у будівельні матеріали (цегла, окатиш, пенозол та інші продукти та матеріали).

У пропонованій схемі для утилізації відходів ТОВ Теплоенергоцентр (м. Кропивницький) передбачається блок хімічної переробки зольного концентрату (алюмосилікатного продукту) для вилучення кремнезему (SiO_2) методом розчинення його лугом з одержанням глиноземного концентрату та розчину силікату натрію. При регенерації розчину силікату натрію вапном (CaO) утворюється розчин лугу та мінерал беліт (осаджений двокальцієвий силікат). Луг повертається на початок процесу на розчинення кремнезему, а білить у вигляді білого шламу (сорт А) виводиться із процесу як готовий продукт («білий шлам»).

Білий шлам може мати і більш високотехнологічне застосування – для виробництва фарфорових виробів, промислової кераміки, силікатної цегли, білих і кольорових цементів та інше. Білитові шлами можуть знайти застосування в різних галузях будівельної промисловості. Глиноземний концентрат направляється в блок термохімічної переробки, де відбувається спочатку спікання його з вапняком, а потім вилуговування з жару розчином соди алюмінату кальцію. При цьому утворюються алюмінієвий розчин та сірий білітовий шлам (сорт Б). Алюмінатний розчин після знекремнення направляється в блок карбонізації для гідроксиду алюмінію за звичайною схемою, відомою в технології глинозему, а білитовий шлам (так званий «сірий шлам») направляється на виробництво цементу.

Переробка зольного концентрату фізичними методами неможлива, тому для поділу золошлаків на компоненти, придатні для використання як сировину та матеріали в інших галузях промисловості, необхідно застосовувати хімічні та термохімічні методи переробки золи, яку уловили запропонованим концентратором циклонного типу.

Спосіб включає пропускання повітря через шар охолоджуваного адсорбенту, а потім через шар каталізатора окислення оксиду вуглецю на основі окислів марганцю і міді. Після

каталізатора повітря, що пропускають підігрівається адсорбент, після чого змінюють напрямок повітряного потоку на протилежний, з одночасним охолодженням адсорбенту на вході потоку і підігрівом адсорбенту на виході. Адсорбент охолоджують і підігрівають за допомогою термоелектричних елементів, в яких здійснюють перемикання напрямку електричного струму синхронно зі зміною напрямку потоку повітря у новому апараті циклонного типу, схема якого наведена на рисунку 2 нижче:

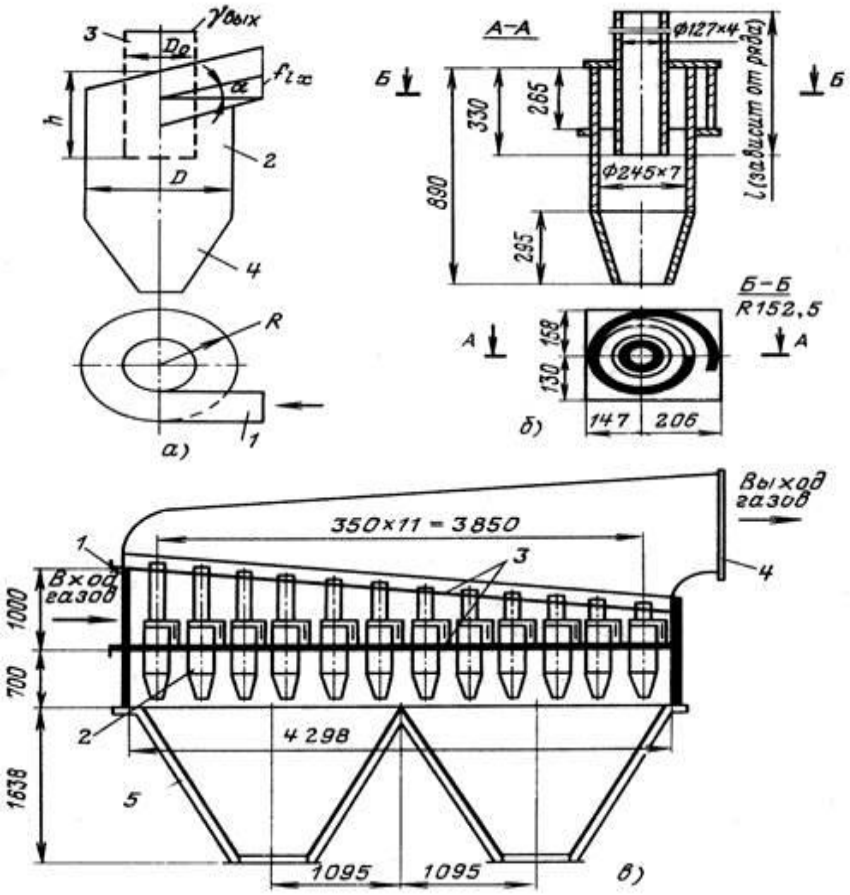


Рисунок 2 - Схема пристрою для уловлювання золи на ТОВ Теплоенергоцентр (м. Кропивницький)

Фільтруючий модуль містить адсорбер, який на виході з'єднаний з патроном. У патроні поміщений каталізатор окислення оксиду вуглецю. На виході патрона встановлений другий адсорбер. Адсорбери з'єднані з перемикачем повітряного потоку і виконані з внутрішнім оребренням, сполученим з термоелектричними елементами. Термоелектричні елементи підключені до джерела живлення через перемикач напряму електричного струму. Винахід дозволяє створити більш простий і надійний спосіб очищення, зменшити енерговитрати та кількість адсорбенту, спростити конструкцію і зменшити габарити пристрою, виключити зупинку роботи пристрою для проведення регенерації.

Винахід відноситься до сорбційно-каталітичного очищення відходів виробництва від зольних речовин і може бути використано для систем очищення від токсичних компонентів спалювання палива на ТОВ Теплоенергоцентр (м. Кропивницький), а також для очищення припливної вентиляції приміщень підприємства.

Основним споживачем золи та шлаку, що утворюються від спалювання вугілля, є промисловість. Зола і шлак використовуються у будівництві, додаються у бетон, при виробництві сухих сумішей для штукатурки. Також золу і шлак можна використовувати у рекультивації відпрацьованих кар'єрів, заповнення шахт, посипання доріг взимку. Можливість додавати в основу доріг. Так як на котельні використовується кам'яне вугілля, то з отриманої при спалюванні золи отримують цінний матеріал – алюмосилікатні мікросфери.

Так як з кожним роком золошлаковідвал збільшується в розмірах, отже і збільшується плата за утримання та зберігання золошлаковідвалу. Постачання золи та шлаку споживачеві дає додатковий прибуток. Від цього ТОВ Теплоенергоцентр (м. Кропивницький) отримає додатковий прибуток від продажу золи та шлаку та зменшення золошлаковідвалу, та зменшення плати за золошлаковідвал.

Можливі варіанти реалізації золи споживачам:

1. Безпосередньо із золосаджувальної станції (рис. 3)

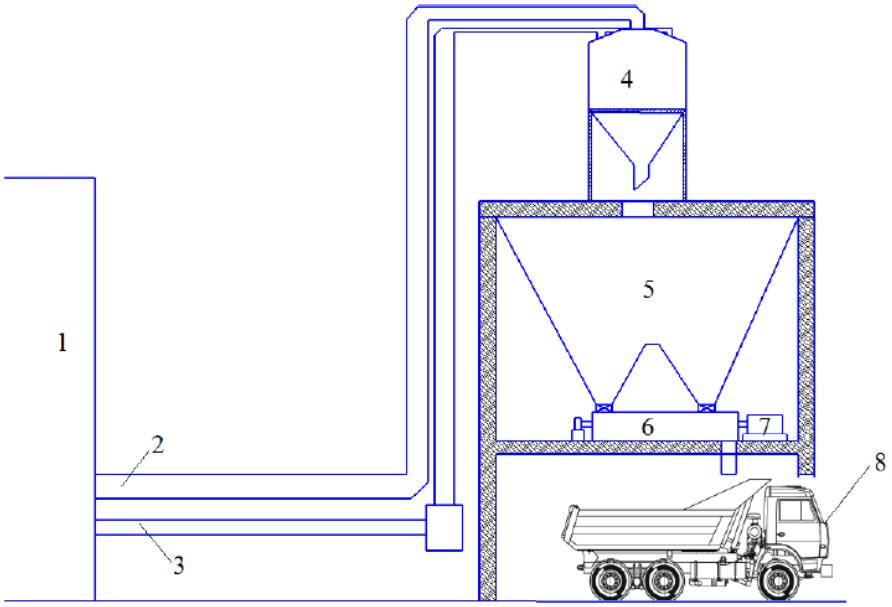


Рисунок 3 - Схема постачання золи споживачам через золоосаджувальну станцію:

1 – котельня; 2, 3 – золопроводи; 4 – циклон золоосаджувальної станції; 5 – бункер золоосаджувальної станції; 6 – шнек; 7 – електричний двигун; 8 – автосамоскид.

Зола та шлак із бункера золоосаджувальної станції шнековим живильником відвантажується споживачеві в автосамоскиди.

2. З золошлаковідвалу на ТОВ Теплоенергоцентр (м. Кропивницький)

Зола та шлак на котельні №10 на ТОВ Теплоенергоцентр (м. Кропивницький) транспортуються на золошлаковідвал у сухому вигляді, тобто можливість постачання золи споживачам із золошлаковідвалу за допомогою навантажувача в автосамоскиди.

Висновки. Серед розглянутих напрямів утилізації останнім часом поширеного використання набирає метод спалювання один з радикальних методів утилізації осаду, тому ми пропонуємо саме його для оптимізації системи поводження з відходами на підприємстві ТОВ Теплоенергоцентр (м. Кропивницький). Також, за для запобігання забруднення ґрунтів у районі дослідження пропонуємо впровадження нової схеми уловлювання золи. Принципова схема золошлаковловлювання, яка вже існує на ТОВ Теплоенергоцентр не підходить для встановлених задач. Тому була запропонована нова схема уловлювання та переробки золи.

Так як з кожним роком золошлаковідвал збільшується в розмірах, отже і збільшується плата за утримання та зберігання золошлаковідвалу. Постачання золи та шлаку споживачеві дає додатковий прибуток. Від цього ТОВ Теплоенергоцентр (м. Кропивницький) отримає додатковий прибуток від продажу золи та шлаку та зменшення золошлаковідвалу, та зменшення плати за золошлаковідвал.

Список літератури

1. СТАТИСТИЧНИЙ ЗБІРНИК ДОВКІЛЛЯ УКРАЇНИ - [Електронний ресурс]. – Режим доступу: http://www.ukrstat.gov.ua/druk/publicat/kat_u/2020/zb/11/Zb_dovk_2019.pdf
2. Экология города: Учебник / Под ред. Ф.В.Стольберга. – К.:Либра, 2000. – 464 с.
3. Hofmann K. The role of plants in subsurface flow constructed wetlands // Ecological Engineering for Wastewater Treatment. Proceedings of the International Conference at Stedsund Folk College. Sweden March 24-28, 2011 / Ed. Etnier, B. Guterstam, Bokskogen. - Sweden, 2011. - P. 199.
4. Brix, H. Wastewater treatment in constructed wetlands: system design, removal processes, and treatment performance. In: Moshiri, G.A. (Ed.), Constructed wetlands for water quality improvement, Boca Raton, USA: Lewish Publishers. -2013. -pp. 9-22/
5. Використання осадів стічних вод в експериментальному дорожньому будівництві / Г. Я. Дрозд, Р. В. Бреус, В. В. Рогулін, І. І. Бізірка // Водопостачання та водовідведення. – 2011. –№ 4. – С. 44–47.
6. Дрозд Г. Я. Оцінка технологій утилізації осадів стічних вод / Г. Я. Дрозд, В. В. Рогулін // Водопостачання та водовідведення. – 2011. – № 4. – С. 38–43.
7. EU (2015). 2nd Forum on Implementation and Enforcement of Community Environmental Law: Intensifying Our Efforts to Clean Urban Wastewater.

УДК 651.012.12

В. Барабаш, канд. пед. наук, доцент
Д. Іваніщев, магістр гр. ІС-20 М (1,4)
Центральноукраїнський національний технічний університет

ДОКУМЕНТАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА (НА МАТЕРІАЛАХ ВАТ “КІРОВОГРАДГАЗ”)

У статті досліджено особливості документаційного забезпечення ВАТ “Кіровоградгаз”, а саме проходження документів в Товаристві «Кіровоградгаз». Електронний документообіг, запроваджений у ВАТ «Кіровоградгаз» за допомогою новітніх інформаційних технологій, дозволяє забезпечити сучасне підприємство єдиним інформаційним простором, що значно покращує документообіг на підприємстві.
сучасне підприємство, управлінська діяльність, електронний документообіг, електронні програми, штрихкодування, електронний цифровий підпис

Постановка проблеми. У будь-якій компанії, підприємстві або в установі відділ діловодства займає важливе місце, оскільки є одним із головних компонентів управлінської структури, реалізуючи ряд важливих завдань, таких, як прийняття та реєстрація вхідних документів, оформлення вихідної документації тощо. Діловодство на підприємстві може вестись на основі Єдиної державної системи діловодства (ЄДСД), яка допомагає уникнути надмірностей і дублювання в роботі, оскільки в ній сформульовані єдині вимоги та рекомендації з питань підготовки документів, організації документообігу, обліку та пошуку інформації, здійснення контролю за виконанням документів та угруповання їх у справи. Для ефективної діяльності та подальшого вдосконалення системи управління сучасною організацією є накопичення, переробка, поширення та зміст необхідної документної інформації. Особливість управління багато в чому залежить від якості відомостей, тому що вони ґрунтуються на створенні та використанні даних. Поліпшення організації роботи з документами веде до швидкої передачі відомостей на ефективному етапі створення та оформлення документів та подальшої роботи з виконання управлінського рішення, що у результаті призведе до економності робітничих та матеріальних засобів.

Аналіз останніх досліджень та публікацій.

Особливої значущості у процесі дослідження документаційно-інформаційного забезпечення установи набувають численні наукові праці вітчизняних учених, таких як Г. Беспянська [3], В. Бездрабко [2], О. Загорецька [5], В. Кудлай [6], С. Кулешов [8], Н. Кушнаренко [9], Ю. Палеха [11] та інші. Проблемам електронного документообігу, який був створений на основі існуючого паперового документообігу, присвячено праці А. Гречко , М. Цивіна, О. Кукаріна [7] та інших. Наукові праці вищезгаданих авторів дозволяють всебічно дослідити предмет дослідження.

Мета й завдання дослідження. Метою роботи є дослідження документаційного забезпечення діяльності відкритого акціонерного товариства «Кіровоградгаз».

Для досягнення поставленої мети визначено такі завдання, як: теоретико-методологічні підходи до проблеми документаційного забезпечення підприємства, розглянути історію створення, основні напрямки діяльності ВАТ «Кіровоградгаз, проаналізувати особливості документообігу відкритого акціонерного товариства, охарактеризувати вимоги до створення та затвердження документації ВАТ «Кіровоградгаз», дослідити особливості ведення управлінської документації підприємства, проаналізувати роботу з документами установи на базі електронної програми 1С: Документообіг, визначити шляхи удосконалення документно-інформаційної діяльності ВАТ «Кіровоградгаз».

Об'єктом дослідження є документаційне забезпечення управління комерційної організації ВАТ «Кіровоградгаз».

Предметом дослідження є особливості документаційного забезпечення ВАТ «Кіровоградгаз».

Виклад основного матеріалу. Важливість документів та інформації зростає з кожним роком, бо документи стають все більш важливими в різних аспектах як у соціальному житті, так і в управлінні документами, оскільки є невід'ємною частиною будь-якого ефективного функціонування сучасного підприємства.

У ключі досліджуваної проблеми варто зазначити, що в Україні триває зростання обсягів інформації, що використовується в управлінській роботі установи, його структурна складність і швидка оновлюваність роблять необхідним використання вбудованих систем електронного документообігу. Без застосування технологій систем електронного документообігу і застосуванням технологій електронного цифрового підпису установа не може нормально функціонувати і розвиватися. Під поняттям "електронний документ" відповідно до закону України "Про електронні документи та електронний документообіг"[9] розуміємо документ, інформація в якому зафіксована у вигляді електронних даних, серед яких обов'язкові реквізити документа. Електронний документообіг (обіг електронних документів) – сукупність процесів створення, опрацювання, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності і в разі необхідності – з підтвердженням факту одержання таких документів. Тож в паперових документах використовують підпис і печатку, а для електронних документів запроваджено електронний підпис. Дана тема актуальна тим, що однією з найскладніших сфер для впровадження автоматизованих інформаційних систем в Україні є передусім документообіг на підприємствах, установах та в державних структурах. Документообіг у нашій державі є системою, що забезпечує роботу з документами, які надходять ззовні та готуються всередині установи, насамперед реєструються, передаються працівникам організації, допомагають здійснювати контроль за виконанням певних робіт, вести довідкову роботу і зберігати тощо.

ВАТ «Кіровоградгаз» – акціонерне товариство, діяльність якого полягає у розподілі газу. Відкрите акціонерне товариство по газопостачанню та газифікації «Кіровоградгаз» засноване відповідно до наказу державного комітету України по нафті і газу від 14 березня 1994 року №123 шляхом перетворення державного підприємства по газопостачанню та газифікації «Кіровоградгаз» у відкрите акціонерне товариство відповідно до Указу Президента України "Про корпоратизацію підприємств" від 15 червня 1993 р. №210/93.

Організація роботи з документами в ВАТ «Кіровоградгаз» визначає створення умов, що забезпечують рух, пошук та зберігання документів у діловодстві. Документообіг представляє собою рух документів в організації з моменту їх отримання або створення до завершення виконання та здачі в архів або відправлення адресату. Основними принципами організації документообігу є те, що проходження документів має бути швидким, щоб скоротити час їхнього перебування у сфері діловодства; кожне переміщення документа має бути обґрунтованим, необхідно виключити чи обмежити поворотні переміщення документів; порядок проходження та процес обробки основних видів документів мають бути однаковими. Документи, що надійшли до ВАТ "Кіровоградгаз", проходять такі етапи як: первинна обробка; попередній розгляд та розподіл реєстрація; напрямок на виконання; виконання; контроль виконання. Весь склад управлінських документів Товариства поділяється на три документопотоки: вхідний; вихідний; внутрішній. Задля повноцінної роботи з документами в електронному документообігу на підприємстві ВАТ «Кіровоградгаз» в 2021 році впровадили програму «1С: Підприємство». Дана програма відповідає вимогам усіх законів та нормативних актів, що регламентують порядок роботи з документами.

Програма «1С: Підприємство» має ряд функцій для обробки, пошуку, контролю інфорції, а також дозволяє вести швидкий облік документів. Впровадження електронного документообігу значно спрощує роботу підприємств та його співробітників.

Важливим пунктом в електронному документообігу підприємства є впровадження *штрихового кодування* та електронного підпису для електронних документів ВАТ «Кіровоградгаз». Штрих-код – це «масив чорних і білих смуг, які представляють деяку інформацію технічно читаним способом». Штрих-коди призначені для спрощення та прискорення пошуку файлів та документів у програмі «1С: Підприємство».

За допомогою електронної програми штрих-коди можуть бути присвоєні будь-якому листу, нотатці або замовленню з відповідними настройками. Штрих-коди встановлюються кожним співробітником особисто в самій електронній програмі на підставі відповідних інструкцій, складених співробітником, а потім автоматично штрих кодуються.

Електронно-цифровий підпис також є одним із сучасних способів підтвердження справжності документів. Завдяки цифровому підпису можемо скоротити витрати на власний робочий час.

Окреслюючи основні шляхи удосконалення документно-інформаційної діяльності установи, зазначимо, що сьогодні до найпопулярніших засобів автоматизації електронного документообігу фахівці відносять такі системи, як: «БОСС-Референт» А. Алексенцев [1], «ДЕЛО», «Евфрат-документооборот» [22], OPTiMA-WorkFlow, Lotus Notes, «Documentum», «Megapolis. Документооборот», «Кадри Плюс Україна 7», що допоможе значно підвищити рівень документацйного забезпечення досліджуваної установи та оперативної передачі інформації на різні рівні управління.

Висновки. Отже, електронний документообіг, запроваджений у ВАТ «Кіровоградгаз» за допомогою новітніх інформаційних технологій, дозволяє забезпечити сучасне підприємство єдиним інформаційним простором, що значно покращує документообіг на підприємстві. Всебічно проаналізовано електронну програму «1С: Підприємство», що дало змогу констатувати: використання даної програми дозволяє швидко і ефективно опрацьовувати документну інформацію підприємства. Ретельний аналіз такого нового виду роботи як штрихкодування довів його універсальність і практичність, є сприяє підвищенню конкурентоспроможності підприємства.

Удосконалення документно-інформаційної діяльності ВАТ «Кіровоградгаз», а саме: розширення використання сучасних електронних технологій, активне застосування таких інформаційно-аналітичних систем, як OPTiMA-WorkFlow, Lotus Notes, програми кадрового обліку «Кадри Плюс Україна 7», програми «Document. Online» – дозволять значно підвищити діяльність досліджуваного підприємства.

Таким чином, організація документно-інформаційної діяльності ВАТ «Кіровоградгаз» в разі застосування засобів автоматизації діловодства сумісно традиційним способом опрацювання документів істотно підвищує ефективність управлінської діяльності.

Список літератури

1. Алексенцев А. І. Автоматизація діловодства М.: ЗАТ Бізнес-школа. 2004. 240 с.
2. Бездрабко В. Термінологія документознавства: новітні здобутки й проблеми. Видавництво Львівської політехніки. 2012. С.16-22.
3. Беспянська Г. В. Діловодство: навч. посібник для дистанційногонавчання. Київ: Університет «Україна», 2007. 469 с.
4. Жежнич П. І. Основні підходи до організації електронного організаційно-розпорядчого документообігу / П.І. Жежнич, О.О. Сопрунюк, О. М. Марчик. 40. Інформація, комунікація, суспільство (ІКС-2012): матеріали І Міжнародної наукової конференції ІКС-2012. Львів : Видавництво Львівської політехніки, 2012. С. 34–36.
5. Загорецька О. Основні етапи проходження вихідного документа. URL: https://undiasd.archives.gov.ua/doc/zmi/DD_09_2013.pdf (дата звернення 22.08.2021).
6. Кудлай В. Документаційне забезпечення системи управління якістю на промисловому підприємстві: дис… канд. іст. наук. Нац. акад. керів. Кадрів культури і мистецтв. К., 2012. 239 с.
7. Rукарін О.Б. Електронний документообіг та захист інформації: навч. посіб. За заг. ред. Н.В. Грицяк. Київ: НАДУ, 2015. 84 с.
8. Rулешов С.Г. Управлінське документознавство: навч. посібник. К.: ДЛККЛМ, 2003. 57 с.
9. Кушнаренко Н. М. Новий етап інституалізації науки про документ. Студії з архів. справи та документознавства. К., 2004. Т.12. С. 126–130.
10. Жежнич П. І. Основні підходи до організації електронного організаційно-розпорядчого документообігу / П.І. Жежнич, О.О. Сопрунюк, О. М. Марчик.
11. Палеха Ю.І. Документування в підприємницькій сфері (зі зразками сучасних документів) : навч. посіб. К. : Ліра-К, 2010. 509 с.

УДК 556

С. Михайлов, магістр гр. ЕО-20М
Центральноукраїнський національний технічний університет

ЕКОЛОГІЧНІ ПРОБЛЕМИ ОХОРОНИ ПІДЗЕМНИХ ВОД ТА ЇХ ВИКОРИСТАННЯ У ПИТНОМУ ВОДОПОСТАЧАННІ НА ТЕРИТОРІЇ КІРОВОГРАДСЬКОЇ ОБЛАСТІ

У статті розглянуто екологічні фактори, що впливають на якість підземних вод Кіровоградської області. Мета – дослідження екологічних проблем підземних вод Кіровоградської області та розробка шляхів їх вирішення.

Об'єкт дослідження – підземні води Кіровоградської області та райони, що на них впливають. Методи дослідження: формально-логічний; порівняльний; балансовий; розрахунковий.

Результат роботи - розробка теоретичних і практичних питань, спрямованих на вирішення проблеми охорони, раціонального використання підземних вод та поліпшення якості питної води в Кіровоградській області.

Постановка проблеми. З розвитком промисловості, сільського господарства, та зростанням кількості населення, використання підземних вод неухильно збільшується. Не повністю вивчена кількісна характеристика підземних вод та їх якісний склад і часто спостерігаються випадки погіршення складу вод під впливом природних і штучних, та антропогенних чинників.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [9 - 17] було виявлено певні прогалини щодо дієвих механізмів досягнення гарного стану вод та покращення екологічного стану підземних вод.

Мета роботи – є дослідження екологічних проблем підземних вод Кіровоградської області та розробка шляхів їх вирішення.

Для реалізації зазначеної мети поставлені та вирішені такі завдання: дослідити значення підземних вод у водозабезпеченні Кіровоградській області; провести екологічну оцінку ресурсів підземних вод області; здійснити розрахунок індивідуальних технологічних норм водоспоживання з підземного джерела; надати рекомендації щодо покращання стану підземних вод на території Кіровоградської області.

Об'єктом дослідження є екологічні фактори, що впливають на якість підземних вод Кіровоградської області.

Предметом дослідження є підземні води Кіровоградської області.

Методи дослідження: формально-логічний; порівняльний; балансовий; розрахунковий.

На території Кіровоградської області технічні та питні підземні води, які використовуються для потреб господарсько-питного і виробничо-технічного водопостачання розвідані на тридцяти восьми ділянках, з яких використовується одинадцять. Загальна кількість затверджених (балансових) запасів питних та технічних вод складає 225,70 тис. м3/добу за категоріями А+В+С1.Залягання й поширення підземних вод пов'язане з геологічною будовою території.

Головним джерелом прісної води на території досліджуваної області є водоносний горизонт, що лежить біля основи порід бучакської свити палеогенового віку. Водомісткі породи представлені різнозернистими кварцовими пісками з потужністю до 25 м. Водоносний горизонт в бучакськихвідкладеннях експлуатується колодязями та свердловинами. За даними Кіровоградського обласного управління водних ресурсів за рік може бути зібрано 16,40 млн. м3 підземних вод. За хімічним складом ґрунтові води Кіровоградської області належать до гідрокарбонатних, гідрокарбонатно-сульфатних, деколи сульфатногідрокарбонатних, калієвих та натрієвих. Загальна жорсткість води складає 1,5-8 мг-екв./дм3.

Підземні мінеральні води Кіровоградської області належать до типу радонових, які використовуються для бальнеолікування, а також як природностолові води, придатні для розливу. Сумарна кількість затверджених (балансових) запасів мінеральних вод складає 483,0 тис. м3/добу за категоріями А+В+С1. Роботи по вивченню режиму та якості підземних вод на території Кіровоградській області проводяться ДП НАК "Надра України" "Центрукргеологія" на базі існуючої спостережної мережі. Більшість населення області для питного водопостачання користується водою зі свердловин, в яких відмічається підвищений вміст заліза, марганцю, азотних сполук, при загальній великій жорсткості.

Треба зауважити, що рівні забруднення нітратами в громадських колодязях області перевищують нормативи більш ніж у 9 разів (наприклад, вміст нітратів у воді з криниці на вулиці Жовтнева в селі Паліївка Маловисківського району становить - 476,2 мг/дм3 при стандартному значенні 50 мг/дм3), а у осіб вони перевищують понад 30 разів (с. ЗлінкаМаловисківського району - вміст ніртату 1731,6 мг/дм3). За бактеріологічними показниками кожна шоста проба води з громадських колодязів була з відхиленнями. Найбільша питома вага невідповідних проб у Олександрійському — 75% та Знам'янському — 46%, районах, а також по м. Олександрія — 42%. В межах 20-30% невідповідних проб спостерігалось в Новоукраїнському, Новгородківському, Гайворонському районах та по м. Кропивницький.

Підрахунок експлуатаційних запасів технічних підземних вод Суботцівського родовища виконаний гідравлічним методом. Відповідно до експертної оцінки величина прогнозного зниження рівня в експлуатаційній свердловині № 1 на розрахунковий строк експлуатації водозабору не перевищуватиме допустимого зниження. Попередньо розвідані

експлуатаційні запаси технічних підземних вод авторами правильно кваліфіковані категорією С1. До категорії С1 (код класу 122) віднесено прогнозний водовідбір по свердловині № 1 на розрахунковий строк експлуатації родовища, обґрунтований водовідбором у кількостях 48 і 77 м3/добу за результатами дослідних відкачок.

Для безпечного споживання води з колодязів розроблено ряд рекомендацій, яких слід дотримуватися для забезпечення питної води високої якості:

1. Після обробки водою:

- Не використовувати воду протягом перших 24 годин.
- Якщо у воді пахне хлором, необхідно прокачати колодязь.
- Не можна пити воду без обробки 5 - 10 днів, а краще не пити її зовсім без попереднього очищення.

2. Колодязі повинні розташовуватися в незабрудненій та захищеній зоні, яка знаходиться вище за течією підземних вод на відстані не менше 30 м. від магістралей з інтенсивним рухом та не менше 20 м. від туалетів, вигрібних ям, будівель та каналізаційних мереж, складів добрив, пестицидів та інших місць забруднення ґрунту та підземних вод.

3. Забруднення води також виникає, коли біля криниць є приміщення для домашніх тварин та місця для поїлок тварин, коли в криницю 37 потрапляють гризуни, які, ймовірно, хворі або є переносниками різних інфекцій.

4. Не залишати колодязь відкритим.

5. Необхідно ущільнити стінки колодязя, щоб запобігти ґрунтовим водам.

6. Потрібно не допускати стікання відходів у колодязь та не використовувати мінеральні добрива на задньому дворі.

Висновки. Необхідно розробити і спровадити систему важелів заохочувального і заборонного характеру, активно використовувати засоби масової інформації, використовувати системи очистки, розвивати екологічну культуру громадян Кіровоградської області та всієї країни в цілому, зокрема, у ставленні до водних джерел та підземних вод.

Список літератури

1. Александров В. Д., Ємельянов В. І. Отруйні речовини. Москва: Воениздат, 1990. – 310 с.;
2. Бережнов С. П. Питна вода як фактор національної безпеки. // СЕС профілактична медицина. – 2006, №4. – С. 8–13.;
3. Вахів С.Й, Грицик Т.Ю., фахівці дезінфектологічного відділення Дрогобицького міжміського відділу ДУ «Львівський обласний лабораторний центр МОЗ України». Стаття. Дезінфекція колодязя - профілактика розповсюдження інфекційних хвороб, 2018. – 1 с.;
4. Водопостачання. Зовнішні мережі та споруди. Основні положення проектування: ДБН В.2.5 – 74:2013 / Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України. – Київ, 2013. – 287 с.;
5. Водообмен в гидрогеологических структурах Украины: Водообмен в естественныхусловиях / В.М. Шестопалов, В.И. Лялько, Н.С. Огняник и др.; отв. ред. В.М. Шестопалов. АН УССР. Институтгеологических наук. К.: «Наукова думка», 1989, 228 с.;
6. Визначення якості води методами біоіндикації / В.І. Мальцев, Г.О. Карпова, Л.М. Зуб. – К.: НЦЕБМ НАН України, ІНЕКО, 2011. – 112 с.;
7. Внутрішній водопровід та каналізація. Частина І. Проектування. Частина ІІ. Будівництво: ДБН В.2.5-64:2012 / Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України. – Київ, 2013. – 113 с.;
8. Горєв Л. М., Пелешенко В. І., Хільчевський В. К. Гідрохімія України. – Київ: Вища школа, 1995. – 307 с.;
9. Екогеографія України : навч. посібник / О.П. Гавриленко. К. : Знання, 2008. 647 с.;
10. Екологічне право України: академічний курс / за ред. Ю. С. Шемшученка. К., 2008;
11. Енциклопедія Сучасної України. Кіровоградська область [Текст] : Стаття//М. М. Кір'янов, І. А. Козир, А. І. Кривульченко, В. М. МирзаСіденко, Л. Л. Семенюк, О. В. Чорний;
12. Залеський І.І., Клименко М.О. Екологія людини: Підручник. – Київ: Видавничий центр "Академія", 2005. – 287с.;
13. Зекцер И. С. Подземныеводыкак компонент окружающейсреды. – М.: Научный мир, 2001. – 328 с.;
14. Каменский Г.Н. Зональностьгрунтових вод и почвенно-географическиезоны. Тр. лабораториигидрогеол. пробл. АН СРСР, т. 6, 1949.;
15. Каналізація. Зовнішні мережі та споруди. Основні положення проектування: ДБН В.2.5-75:2013 /

Міністерство регіонального розвитку, будівництва та житловокомунального господарства України. – Київ, 2013. – 210 с.;
16. Краснова М. В. Проблеми компенсації шкоди за екологічним законодавством України: автореф. дис. … д-ра юрид. н.: 12.00.06. К., 2010.;
17. Дубняк С.С., Дубняк С.А. Оцінка стану і проблеми законодавчого регулювання водоохоронних зон водних об'єктів України // «Гідрологія, гідрохімія і гідроекологія»: Наук. збірник. – К.: ВГЛ «Обрії», 2005. – Том 7. – С. 25–39.

УДК 004

В. Нетребенко, магістр гр. КІ-19М-1,4
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ДЛЯ ОХОРОННОЇ СИСТЕМИ

У статті розроблено програмне забезпечення, яке призначено для системи кібербезпеки охоронної системи. Метою розробки є дослідження та програмна реалізація системи охоронної системи з впровадженням системи кіберзахисту. Об'єктом дослідження є процес управління охоронною системою з функцією кібербезпеки. Предметом дослідження є методи реалізації систем та систем віддаленого захисту об'єкта. Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація охоронної системи з проведеними заходами з кібербезпеки. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, IoT, відеонагляд, датчики, кіберзахист

Постановка проблеми. Відеоспостереження, як і цифрова система, являє собою програмно-технічний комплекс, призначений для організації технологічних і охоронних телевізійних систем. Це дозволяє організувати відеоспостереження, як за місцевими, так і територіально розташованими об'єктами. Сучасні цифрові системи відеомоніторингу дозволяють запрограмувати реагування сигналізаційних пристроїв у разі виникнення тривоги. Приховане відеоспостереження призначене для місць, де встановлена відеокамера не повинна бути помітна. Установка такої відеокамери проводиться таким чином, що при уважному огляді на місце її встановлення можна позначити лише невелику крапку. При використанні такого типу відеоспостереження можливе встановлення відеокамер у внутрішніх об'єктах, але бажано, щоб вони були стаціонарними. Бездротове відеоспостереження сконструйовано таким чином, що замість кабелю, встановленого між відеокамерою та відеоприймачем, використовується пара (передавач/приймач), яка передає/приймає відеосигнал по ефірі. Будуючи проект, встановлюючи різні системи, будь то відеоспостереження чи інша охоронна система, потрібно звернути увагу на безліч факторів, які будуть грати роль в роботі будь-якої системи відеоспостереження.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні захисту даних систем від втручань ззовні.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи кібербезпеки для охоронної системи об'єкта.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем захисту віддалених об'єктів.

– Дослідження системи захисту з використанням сучасних систем захисту каналів зв'язку передачі даних.

– Програмна реалізація системи кібербезпеки.

Об'єктом дослідження є процес кіберзахисту охоронних систем.

Предметом дослідження є методи розробки охоронних систем з впровадженням систем кіберзахисту.

Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Система «розумний будинок» умовно ділиться на кілька самостійних підсистем: безпека, освітлення, multiroom та клімат-контроль. Система безпеки розумного будинку включає в себе такі елементи, як сигналізація, протипожежні датчики, а також датчики, що реагують на несправність комунікативних ліній. Під час відсутності господаря в домі автоматично включається сигналізація та протипожежні датчики, а в разі виникнення небезпечної ситуації, будь то небажане вторгнення або загоряння, система сповістить вас про це на віддалене пристрій — мобільний телефон, планшет або комп'ютер. Також програма негайного оповіщення зреагує і в тому випадку, якщо в будинку несподівано протечуть труби чи станеться витік газу.

Система освітлення розумного будинку управляє усіма освітлювальними елементами об'єкта. При необхідності вона відключає непотрібні в даний момент джерела світла, автоматично регулює ступінь освітленості в залежності від часу доби і навіть пори року, а також включає світло, як тільки ви з'являєтеся в будинку. Крім того, щоб відвернути увагу зловмисників, у системі можна встановити програму періодичного включення/вимикання світла у якому-небудь приміщенні під час вашої відсутності в будинку.

Система multiroom відповідає за розподіл аудіо – і відеосигналу по всій квартирі. Вона може включати і вимикати техніку, передавати сигнал на всі пристрої, регулювати звук, а також створювати оптимальні умови для перегляду відео або прослуховування музики. Крім того, якщо інтегрувати систему multiroom з системою безпеки, то запис з камер відеоспостереження можна переносити на будь-який підключений до програми пристрій. Наприклад, якщо ви знаходитесь далеко від дому, ви завжди можете спостерігати за тим, що відбувається під час вашої відсутності з допомогою допоміжних пристроїв комп'ютера або мобільного телефону, підключеного до системи.

Система клімат-контроль в «розумному будинку» керує пристроями, що відповідають за опалення, кондиціонування, очищення і зволоження повітря. Вибравши необхідний режим, ви можете налаштувати систему так, щоб вона нагрівала приміщення до вашого приходу, періодично очищала повітря, а також зволожувала його до оптимальних показників. Крім своєї зручності, ця система привабліва ще і можливістю заощаджувати енергоресурси. Клімат-контроль самостійно визначає необхідний рівень температури, вимикає прилади в разі перегріву і реагує на погоду за вікном.

Крім вищеназваних підсистем, «розумний будинок» має масу інших допоміжних функцій. Наприклад, ви можете автоматизувати роботу системи так, щоб обмежити доступ дітей до небезпечних елементів, встановити режим поливу, включити цілодобове внутрішнє і зовнішнє відеоспостереження, налаштувати роботу техніки на необхідні режими і т. д.

Безпека

Розумний Дім забезпечує безпеку Вашої оселі, як від зовнішнього проникнення, так і від аварій всередині будинку.

До всіх вікнах і дверях підключаються датчики відкриття. У кімнатах встановлюються датчики руху та відеокамери. При бажанні, Ви з будь-якої точки світу, завжди будете бачити, що відбувається у Вашому домі. Це важливо, як при захисті будинку від сторонніх, так і в разі, якщо Ви залишаєте дітей вдома з нянею.

Окремо, в будинку, встановлюються датчики витоку газу і протікання води. При спрацьовуванні вони перекривають захисні клапани, і Ваш будинок залишається цілим і

неушкодженим.

Відеоспостереження

Встановивши камери спостереження, Ви завжди можете контролювати ситуацію в Вашому домі. При цьому, камери можуть виконувати не тільки охоронну функцію. Ви можете простежити за тим, як доглядає за близькою людиною доглядальниця або займається з дитиною няня. Приклад прекрасного взаємодії системи відеоспостереження та домофона: Ви, перебуваючи поза домом, можете побачити гостя, який зателефонував в домофон, і, при необхідності, навіть, впустити його в будинок.

Мікроклімат

У вашому домі завжди підтримується комфортна температура і вологість. В потрібний час включається провітрювання. У нічний час, Розумний Дім охолоджує спальню і забезпечує вам міцний і здоровий сон. З настанням ранку він включає підігрів підлоги в спальні і у ванній кімнаті. Де б Ви не знаходилися і що б ви не робили, Розумний Дім стежить, щоб вам було комфортно.

Коли всі їдуть, і будинок залишається порожнім, опалення переходить в економний режим і «Розумний Дім» чекає вашого приїзду, економлячи ресурси.

Мультирум

Система мультирум - дозволить вам слухати музику в будь-якій кімнаті, без установки в кожній з них аудіосистем. При цьому, в кожній кімнаті може звучати своя музика. Управління всією системою мультирум відбувається за допомогою планшета або телефону.

На динаміки системи може бути виведений звук з домофона. Вона ж може озвучувати будь-які попередження або події. Наприклад, при відкритті гаражних воріт, Ви можете отримати оповіщення про те, що хтось приїхав.

Догляд за садом

Система розумного будинку стежить за вологістю ґрунту в Вашому саду і поливає його, не даючи рослинам засохнути. Вона вибирає потрібний режим поливу для кожної зони з рослинами. Якщо Ваші рослини вимагають поливу строго за розкладом - Розумний Дім зробить і це. Догляд за садом може бути повністю автоматичним і не вимагати Вашої участі.

Всі ці «електронні чудеса», на превеликий жаль, не можуть працювати без електрики, а точніше без електроенергії належної якості. Приведемо простий приклад, з якого стане ясно, що саме розуміють під «електроенергією належної якості». Дуже часто ми, як споживачі, навіть не замислюємося над тим, чому саме трапилася та чи інша поломка і у всьому прагнемо звинуватити недбайливого виробника. Перш ніж когось звинувачувати, варто уважно прочитати інструкцію з експлуатації, наприклад рідкокристалічного телевізори Full HD 1080 фірми SONY BRAVIA. Там можна побачити такі цікаві цифри, як напруга 230 В (+\- 10%). Це означає, що виробник гарантує працездатність свого вироби тільки в тому випадку, якщо напруга у Вашій домашній мережі знаходиться в межах від 207 до 253. В інших випадках Ваші претензії щодо якості виробу будуть відхилені як безпідставні. Зробіть вимір напруги у Вашій домашній мережі — багато хто з Вас будуть неприємно здивовані отриманими результатами.

Особливо це стосується будівель, які знаходяться в сільській місцевості, де напруга в 190В вважається межею мрій. Природно, що якщо Ви плануєте встановити в будинку систему управління «Розумний будинок», так і просто використовувати складну побутову техніку, то без нормалізатор (стабілізатора напруги) Вам просто не обійтися. Без цього приладу вся «розумна» електроніка просто не буде нормально функціонувати. Такий прилад буде цілком доречний як у міській квартирі, так і в заміському будинку.

Крім цього можна подбати про аварійному електропостачанні будинку на випадок відключення електроенергії. Для цих цілей можна встановити електростанцію відповідної потужності, яка зможе забезпечити в автономному режимі нормальне електропостачання всіх домашніх приладів.

Аварійне електропостачання є одним із важливих випадків коли ваш

автоматизований будинок не буде працювати належним чином. Для вирішення проблеми можна використати акумулятивні накопичувальні батареї, що дадуть можливість продовжити роботу системи навіть при аварійному вимкнені живлення в будинку, в такому випадку є електростанції. За рахунок стрімкого розвитку технологій все більше і більше впроваджуються електростанції, що отримують енергію сонця і перетворюють її на електроенергію в свою чергу контролер заряду контролює процес акумулювання отриманої електроенергії та накопичує її в спеціальних акумуляторах. Після чого напругу яка зберігається в акумуляторах підвищують та стабілізують за допомогою перетворювачів та стабілізаторів, і потрапляє в мережу через двонаправлений лічильник електроенергії.

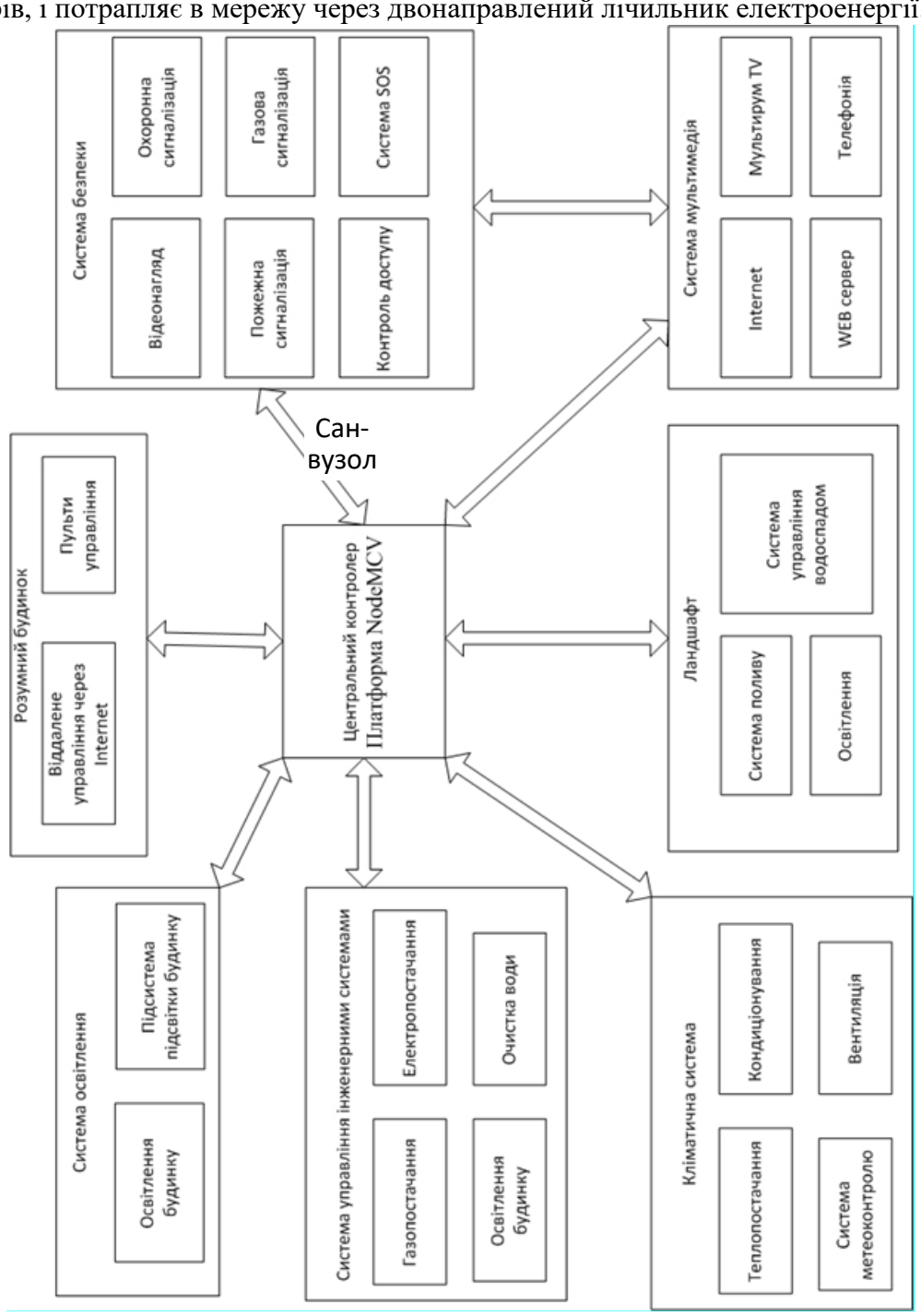


Рисунок 1 – Структурна схема системи управління віддаленим об’єктом

Система безпеки для захисту системи від кібератак

Схема передачі даних в системі охорони віддаленого об’єкта. База сертифікатів – частина фізичного сервера, що зберігає всі цифрові підписи, до яких має повний доступ

логічний сервер та частковий доступ користувач зі свого мобільного пристрою. Мікроконтроллер – пристрій, що безпосередньо відповідає за керування віддаленим об’єктом. В рамках локальної мережі (мережі сервера) дані вважаються умовно захищеними. Небезпеку становить незахищений канал користувача. Один з класичних сценаріїв – man-in-the-middle, тобто можливість інших осіб підключитись в канал між сервером та користувачем та видавати себе за когось з цих ключових осіб, беручи на себе роль невидимого посередника. Для того, щоб не допустити витік інформації, слід використовувати схеми з шифрування даних.

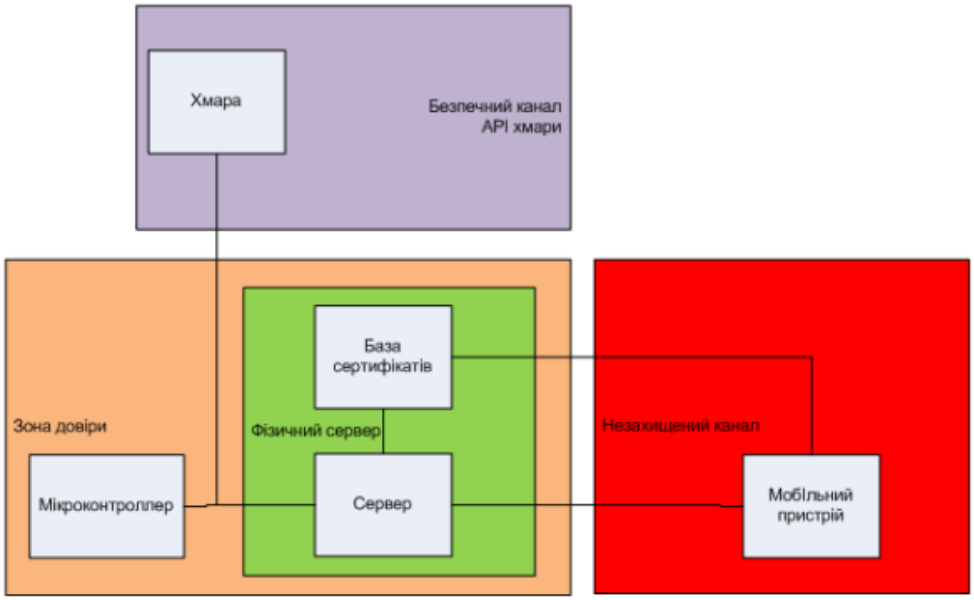


Рисунок 2 – Схема передачі даних на об’єкті

Вибір системи шифрування

В в ході роботи над даним розділом було досліджено роботу схем шифрування:

- Симетричні системи
- Системи з відкритим ключем
- Інфраструктура відкритих ключів

Алгоритми шифрування:

- Симетричні: Base64, AES, DES,
- Асиметричні: RSA, Еліптичні криві.

Було визначено змішану схему шифрування, що використовує Base64, AES, RSA, тести для її перевірки та описано програмну реалізацію, що задовольняє їх.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів охорони віддалених об’єктів з впровадженням систем кіберзахисту. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем IoT з використанням продуктів різних кмпаній; Досліджено системи шифрування та кіберзахисту; На основі отриманих результатів досліджень створена програмна реалізація системи управління віддаленим об’єктом. Розроблені під час виконання магістерської роботи алгоритми дозволяють успішно вирішувати завдання керуванням різними віддаленими об’єктами Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых

телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
2. Умный дом– Режим доступу : http://www.directinfo.net/index.php?option=com_content&view=article&id=139%3 A2010-07-06-13-57-09&catid=1%3A2008-11-27-09-05-45&Itemid=84&lang=ru - Дата доступу : 14.05.2013
3. Босько В.В. Разработка методики оценки середнего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
4. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
5. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
6. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
7. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
8. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку ІТ-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
9. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-53.
10. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
11. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.
12. Можаєв О.О. Часова прозорість мережі, як характеристика, що визначає виконання необхідної якості обслуговування / О.О. Можаєв, О.Д. Анохіна, С.Ю. Гайдаров, С.Г. Семенов // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 11(39). – С.133-139.
13. Е.А. Тесля. «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире / Е.А. Тесля – Санкт Петербург, 2008. – 224с.
14. М. Э. Сопер. Практические советы и решения по созданию « Умного дома » / М. Э. Сопер. – М.: НТ Пресс, 2007. – 432.
15. Mark Gasson, Martin Meints, Kevin Warwick (2005), D3.2: A study on PKI and biometrics, FIDIS deliverable (3)2, July 2005.

УДК 651.012.12

А. Франько, магістр гр. ІС-20 М (1,4)
Центральноукраїнський національний технічний університет

ФОРМУВАННЯ, СКЛАД ТА СТРУКТУРА ФОНДУ № Р – 823 «ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ» В ДЕРЖАВНОМУ АРХІВІ КІРОВОГРАДСЬКОЇ ОБЛАСТІ

Постановка проблеми. Уся діяльність ЦНТУ на усіх етапах його становлення і розвитку, а також трансформацій відображена в документах і матеріалах фонду № Р – 823 «Центральноукраїнський національний технічний університет» в Державному архіві Кіровоградської області.

Аналіз останніх досліджень та публікацій. Серед корпусу праць з історії ЦНТУ особливе місце посідають дослідження з історії даного навчального закладу підготовлені його працівниками. Це, зокрема, Історичний нарис підготовлений І. Федотовим [10] та колективна монографія «Технічна освіта на Кіровоградщині: історичний нарис» [9].

Мета й завдання дослідження. Проаналізувати порядок формування, склад та структура фонду Р-823 «Центральноукраїнський національний технічний університет»

Об'єктом дослідження **ф**онди Державного архіву Кіровоградської області

Предметом дослідження фонд № Р – 823 «Центральноукраїнський національний технічний університет»

Виклад основного матеріалу.

Фонд № Р – 823 поділяється на 5 описів. Проте досить інформативною у плані дослідження історії формування, складу та структури фонду № Р – 823 «Центральноукраїнський національний технічний університет» в Державному архіві Кіровоградської області є так звана «Справа фонду». Так, зокрема, відповідно до «Внутрішнього опису документів, які знаходяться у справі №» № Р – 823, відображається історія формування, складу та структури фонду № Р – 823. Так, зокрема, вказується, що 15 жовтня 1948 р. створено лист фонду на 1 аркуші.

Зупинимось детальніше на характеристиці описів. Так, зокрема, опис 1, структурно поділяється на 4 блоки за навчальними роками 1929-1930 рр. – 10 справ, 1930-1931 рр. – 27 справ, 1931-1932 рр. – 37 справ, 1932-1933 рр. – 44 справи [1]. Цікаво, що офіційна назва опису №1 «Елисаветградский индустриальный институт сельскохозяйственного машиностроения имени В.И. Ленина» суттєво відрізняється від назви самого навчального закладу Зінов'євський вечірній робітничий індустріальний інститут сільськогосподарського машинобудування імені В.І. Леніна. Це повязано з тим, що фонд було сформовано в 30-х роках XX ст. і товариш Г. Зинов'єв, на честь якого було перейменовано м. Єлисавет (Єлисаветград), став «ворогом» більшовицького режиму, його було реабілітовано лише 1988 р., тому відповідно, на час створення листа фонду 15 жовтня 1948 року та даного опису – 12 березня 1958 р., опис не міг містити імені «ворога народу».

Саме тому, ймовірно архіваріусом було прийнято рішення дещо змінити назву навчального закладу. Загалом до опису внесено 118 справ, 3 справи мають літерні номера – 45-а, 80-а, 96-а.

Опис 2, Фонду № Р – 823 охоплює справи 1956-1976 рр. Структурно опис складається із історичної довідки, опису справ канцелярії, навчальної частини, виробничої практики, механіко-машинобудівного факультету, факультету сільськогосподарського машинобудування, ремонтно-технологвчного факультету, факультету будівельних і дорожних машин, загальнотехнічного факультету, вечірнього факультету, підготовчого відділення, науково-дослідного центру, а також профілюючих кафедр – технології машинобудування, металорізальні станки та інструменти, сільськогосподарського машинобудування, електропостачання промислових підприємств, автоматизації промислових виробничих процесів, організації і технології ремонту машин, машини і технології обробки металів тиском, дорожні і будівельні машини та обладнання, машини і технології ливарного виробництва [2,2], загальноінститутських кафедр - історії КПРС, філософії та наукового комунізму, політичної економії, економіки і організації виробництва, фізичного виховання, непрофілюючих кафедр – деталі машин і ПТМ, опору матеріалів, загальної хімії, загальної електротехніки, нарисної геометрії і графіки, металознавства і технології металів, теорії механізмів і машин, гідравліки, вищої математики, загальної фізики, іноземних мов, теоретичної механіки, справи відділів – навчально-методичного кабінету, бібліотеки, відділу кадрів, бухгалтерії, а також справи громадських організацій – НДРС (науково-дослідна робота студентів), первинної організації товариства «Знання» [2,3], первинної профспілкової організації працівників інституту, первинної студентської профспілкової організації [2,4]. Історична довідка до опису було затверджена 17.06.1977 р. Кіровоградським обласним архівним відділом, та скріплена його печаткою. Вона містить короткий але детальний опис створення навчального закладу, процес його еволюції від Кіровоградського вечірнього відділення Харківського політехнічного інституту до Кіровоградського інституту сільськогогосподарського машинобудування [2,5-6], визначені головні завдання інституту [2,9], наводиться структура КІСМу, зокрема, 5 факультетів, 23 кафедри та 6 інших підрозділів [2, 10-11].

В даному описі також наводиться інформація про історію фонду. Указується, що у квітні-травні 1977 року було здійснено науково-технічне впорядкування архівних документів Кіровоградського заочного відділення Харківського політехнічного інституту за 1956-1961 роки, Кіровоградського філіалу Харківського політехнічного інституту за 1962-1966 роки, Кіровоградського інституту сільськогосподарського машинобудування за 1967-1976 роки. У результаті чого було відібрано і оформлено для зберігання в державному архіві документи за 1956-1976 роки, до опису внесена 881 справа, у тому числі відібрані і оформлені документи по особовому складу за 1956-1976 роки, складені списки, до опису внесена 321 справа [2,15]. У передмові до опису міститься характеристика документів які були передані до ДАКіО, а також вказуються документи постійного зберігання не збереглися, що було виявлено під час впорядкування документів КІСМу. Причиною незбереження документів названо несвоєчасну передачу їх до архіву інституту [2,20].

Щодо опису 3 фонду № Р – 823, то в ньому зосереджені документи 1964-1965 та 1967-1970 років, всього 28 справ [8, 5]. У передмові до опису міститься пункт «Історія архівного фонду».

Опис 4 міститься справи 1977-1988 років. Судячи з передмов до даного опису, в ньому об’єднані справи передані 1982 р. та 1988 р. Так, зокрема, вказується, що у квітні 1982 р. документи КІСМу «були піддані науковій обробці співробітниками відділу відомчих архівів держархіву Кіровоградської області» [4, 5]. Під час даної обробки документів, були упорядковані документи постійного строку зберігання за 1977 – 1981 рр. у кількості 657 одиниць зберігання, а також складено акт на «знищення макулатури в 1983 р. у кількості 390 справ. Документи зберігаються в спеціальному приміщенні, за збереження яких відповідає завідуюча архівом» [4, 6]. Наступною є передмова до справ 1982-1988 рр. у якій зазначається, що в березні-червні 1990 року «бригадою госпрозрахункового відділу Держархіву Кіровоградської області здійснено впорядкування архівних документів за 1982-1989 навчальні роки. Під час упорядкування були виявлені і впорядковані документи

постійного терміну зберігання, які не увійшли до попереднього впорядкування за 1964-1981 роки» [4, 17]. Проте, даний опис був доповнений вже на початку XXI ст., під час передачі 325 справ опису №4 до ДАКіО, про що свідчить Акт №10 від 07.05.2002 р.

У травні 1984 р. начальний навчальної частини С.Д. Полонська звертається до ректора КІСМу Кучеренка В.Г. з службовою запискою в якій висловлює клопотання про дозвіл на постійне зберігання в навчальному відділі наступних документів: Полодення про ДЕК (від 15.10.74), навчальні плани ОТФ (від 28.03.1975 р.) та статистичні звіти за 1975-1976 рр. Мотивуючи клопотання тим, що «ці документи наявні в одному екземплярі і необхідні для роботи». Документ містить резолюцію ректора «Дозволяю», а також підпис завідуючої архівом [3, 3].

Опис 5 міститься справи 1989-2009 років. Враховуючи, що до опису увійшли справи декількох часових періодів, зокрема, 1989-1991 рр., 1992-1997 рр., 1998-2002 рр., 2003-2005 рр., 2008-2009 рр., то й передмов до цього опису декілька. У першій передмові, складеної завідуючою архівом КІСМу В. М. Михайловою, вказується на зміни в структурі навчального закладу, створення секцій на кафедрах, введення в експлуатацію навчальних лабораторій, ліквідацію кафедр [5, 4-6], створення економічного факультету[5, 6], перейменування кафедр та ін. Досить інформативним для вивчення фонду № Р – 823 є інформація у передмові про історію фонду та діловодства КІСМу. Так, зокрема, вказується, що «на державне зберігання в Держархів Кіровоградської області, інститут здав – 2 253 справи на постійне зберігання за 1956-1965 рр. Найбільш типовими для даного фонду є наступні документи: накази ректора і проректорів інституту; плани і звіти про роботу інституту; плани і звіти про роботу кафедр і факультетів; бухгалтерські звіти; кошториси по спецкоштам і держбюджету; штатні розписи та ін.» [5, 12]. У передмові за 1992-1997 рр. щодо документів фонду вказується, що до нього увійшли «накази Міністрерства освіти України, накази ректора інституту з основної діяльності, підсумки роботи інституту, протоколи засідань державних екзаменаційних комісій по захисту дипломних проетів, звіти голів державних екзаменаційних комісій, річні бухгалтерські звіти, звіти про роботу кафедр інституту, статистичні звіти по всіх видах діяльності інституту та інші документи. Документи постійного зберігання передані в Державний архів Кіровоградської області на державне зберігання по 1988 рік включно. Документи з особового складу та постійного зберігання впорядковані по 1991 рік і зберігаються в архіві інституту. Цей опис складено у жовтні 1999 року при впорядкуванні документів постійного зберігання та з особового складу за 1992-1997 роки. На впорядковані архівні документи складено описи: - опис справ постійного зберігання за 1992-1999 роки в кількості 443 одиниці; - опис справ з особового складу в кількості 82 одиниці» [5, 15]. Також у даному документі зазначено, що під час впорядкування документів «виявлена доздача документів. На них складені описи: опис справ постійного зберігання за 1960-1991 роки в кількості 42 одиниці; опис справ з особового складу за 1982-1990 роки в кількості 5 одиниць» [5, 15]. Усі ці описи складалися за хронологічно-структурним принципом з розташуванням документів по підрозділах та ступенях важливості. До опису «справ постійного зберігання за 1992-1997 роки складений довідковий апарат: титульний аркуш, зміст, передмова, аркуш-завірювач, перелік відсутніх документів» [5, 15]. Так, під час даного впорядкування документів КІСМу, як і було під час попередніх, що ми вказували вище, було «виявлено, що частина документів постійного зберігання не збереглася. На них складений перелік відсутніх документів в кількості 21 одиниці за 1992-1997 роки» [5, 16]. В описі міститься перелік цих документів.

В наступній передмові до опису справ 5 постійного зберігання КДТУ за 1998-2002 роки, вказується, що «документи постійного зберігання передані в Державний архів Кіровоградської області по 1991 рік включно. Документи з особового складу та постійного зберігання впорядковані по 1997 рік і зберігаються у архіві університету. Цей опис складено в травні 2005 року при впорядкуванні документів постійного зберігання та з особового складу з 1998-2002 роки. На впорядковані документи складено описи: опис справ постійного зберігання за 1998-2002 роки в кількості 548 одиниць; опис справ з особового складу за 1998-

2002 роки в кількості 99 одиниць» [6, 6]. У передмові до опису справ постійного зберігання КНТУ за 2003-2005 роки, вказується, що «документи постійного зберігання університету передані до Державного архіву по 1997 рік включно, за 1998-2002 роки впорядковані і зберігаються в архіві університету… В вересні 2008 року проведена експертиза цінності та впорядкування документів за 2003 – 2005 роки. За підсумками впорядкування складені описи: опис справ постійного зберігання за 2003-2005 роки в кількості 341 одиниці зберігання; опис справ з особового складу за 2003-2005 роки в кількості 60 одиниць зберігання» [6, 6]. Щодо документів КНТУ які не мають наукового, практичного значення «та термін зберігання яких вичерпаний згідно «Переліку типових документів, що утворюються в діяльності органів державної влади та місцевого самоврядування, інших установ, організацій і підприємств, із зазначенням термінів зберігання докуиентів» К. 1998 р. складений акт про вилечення для знищення документів і справ, не віднесених до Національного архівного фонду в кількості 1683 лдиниць за 1992-2003 роки» [6, 7].

Інформативною щодо формування досліджуваного нами фонду є і «Передмова до опису справ 5 постійного зберігання Кіровоградського національного технічного університету за 2008-2009 роки (Фонд №Р-823)». Так, зокрема, вказується, що «документи університету постійного зберігання передані в Державний архів області по 2002 рік, за 2003-2007 роки впорядковані і зберігаються в архіві університету. В жовтні 2012 року проведено впорядкування документів університету за 2008-2009 роки і складений опис в кількості 161 одиниці зберігання. Опис складений за хронологічно-структурною ознакою та довідковим апаратом до нього: титульним аркушем, передмовою, аркушем-завірювачем. До опису ввійшли накази ректора з основної діяльності, протоколи засідань вченої ради університету, протоколи засідань рад факультетів та кафедр, звіти про роботу факультетів і кафедр, штатні розписи, кошториси доходів і видатків, бухгалтерські звіти, статистичні звіти про контингент студентів та інші документи по діяльності університету» [7, 3]. Щодо документів які не входять до НАФ і підлягають знищенню у визначений законодавцем термін, вказується, що «на документи, які не мають науково-історичного та практичного значення і термін зберігання яких вичерпаний, завідуючою архівом університету складений акт про вилучення для знищення документів (справ) не внесених до Національного архівного фонду від 2013 2013 року в кількості 1428 справ за 20__ -2009 роки» [7, 3].

Відповідно до «Внутрішнього опису документів, які знаходяться у справі №» № Р – 823, наступні передачі документів ЦНТУ до ДАКіО буи здійснені 20.09.2016 р., 13.09.2019 р. та 20.09.2021 р.

Під час передачі справ ЦНТУ до ДАКіО 20.09.2021 р. було передано 161 справу за 2008-2009 роки до опису 5 , підставою для передачі справ стало закінчення строків зберігання в університеті [8, 73]. Опис цих справ, як указувалося вище було здійснено у жовтні 2012 і з того часу вони зберігалися в архівному відділі університету.

Заклади вищої освіти Кіровоградщини передають да ДАКіО серед корпусу визначених законодавцем документів і науково-технічну документацію (НТД), для ЦНТУ це здійснюється традиційно, адже така процедура існувала з часу створення фонду цього навчального закладу. Так, наприклад згідно Акту №3 прийому-передачі документів від 29 вересня 1989 року, до ДАКіО КІСМ передав 13 одиниць зберігання НТД за 1970-1971 рр [8, 12]; Акт №4 від 22 березня 1990 р. засвідчив передачу 16 справ з НТД до фонду № Р – 823 ДАКіО за 1972-1973 рр. [8, 14] Відповідно до Акту №5 від 12 вересня 1991 р. була передана НТД (10 одиниць зберігання) за 1974-1975 рр. [8, 15] НТД за 1975-1976 рр. (13 одиниць зберігання) була передана до ДАКіО 29 вересня 1992 року (Акту №6) [8, 16]. НТД за 1977-1979 рр. у кількості 6 одиниць зберігання була передана до Державного архіву області 19 березня 1996 р. [8, 20].

Документи фонду № Р – 823 ДАКіО досліджувалися як архівістами – співробітниками ДАКіО так і науковцями і краєзнавцями. Так, зокрема, протягом 1990 р., архівістом ІІ-ї категорії Ларенко Н.В. було «переглянуто 130 одиниць зберігання фонду Р-823 «Єлисаветградський індустріальний інститут с/г машинобудування ім. В.І. Леніна» опис №1

(1929-1933 рр.), опис №2 (та 2 дод.) (1956-1976 рр), опис №3 (1970-1980 рр.). З них за каталогізовано 53 одиниці зберігання і складено таку ж кількість карток» [8, 19].

Висновки. Таким чином, Фонд Р-823 «Центральноукраїнський національний технічний університет» Державного архіву Кіровоградської області структурно складається із 5 описів і містить у собі документи і матеріали Зінов'євського індустріального інституту сільськогосподарського машинобудування ім. В.І. Леніна опис №1 (1929-1933 рр.), Кіровоградського вечірнього відділення Харківського політехнічного інституту, Кіровоградського інституту сільськогогосподарського машинобудування, Кіровоградського державного технічного університету, Кіровоградського національного технічного університету та Центральноукраїнського національного технічного університету. Вагому роль у формуванні даного фонду та збереженні документів НАФ була зроблена архівним відділом КІСМу-КДТУ-КНТУ-ЦНТУ. До складу фонду входить управлінська документація, звіти цього навчального закладу, звіти структурних підрозділів, фінансова документація, протоколи вчених рад фондоутворювача, факультетів, протоколи засідань кафедр, протоколи засідань ДЕК та звіти голів ДЕК, а також науко-технічна документація. Документи і матеріали даного фонду є важливим джерелом для дослідження історії вищої освіти, підготовки інженерних кадрів, історії науки і техніки, розвитку промисловості та краєзнавчих досліджень.

Список літератури

1. ДАКіО. Ф. № Р – 823 Елисаветградский индустриальный институт сельскохозяйственного машиностроения имени В.И. Ленина, опись №1.
2. ДАКіО. Ф. № Р – 823, опис.2.
3. ДАКіО. Ф. № Р – 823, опис.3.
4. ДАКіО. Ф. № Р – 823, опис.4.
5. ДАКіО. Ф. № Р – 823, опис.5.
6. ДАКіО. Ф. № Р – 823. Передмова до опису справ 5 постійного зберігання КНТУ за 2003-2005 роки.
7. ДАКіО. Ф. № Р – 823. Передмова до опису справ 5 постійного зберігання Кіровоградського національного технічного університету за 2008-2009 роки (Фонд №Р-823).
8. Державний архів Кіровоградської області. Справа фонду № Р – 823. 75 арк.
9. Технічна освіта на Кіровоградщині: історичний нарис. Кіровоград: «Імекс-ЛТД», 2009. 240 с.
10. Федотов І. А. Кіровоградський національний технічний університет: історичний нарис. Кіровоград: КНТУ, 2004. 216 с.

УДК 651.012.12

О. Коломієць, канд. пед. наук, доцент
Д. Чівікова, магістр гр. ІС-20М (1,4)
Центральноукраїнський національний технічний університет

ВИКОРИСТАННЯ ЕЛЕКТРОННОГО АРХІВУ НА ПРИВАТНОМУ ПІДПРИЄМСТВІ

У статті досліджено переваги сучасного виду електронного архіву та недоліки паперового. Також висвітлено електронний документообіг, організація архіву електронних документів. Подається опис комплектування архіву та організація роботи з електронними документами в ньому.
приватне підприємство, паперовий архів, електронний документообіг, електронний архів,документація

Постановка проблеми. Нині спостерігається стрімке збільшення обсягів інформації, яка використовується в різних сферах управлінської діяльності. Її складність та швидке оновлення, обумовлює необхідність застосовування інтегрованих систем документообігу, які в

сучасних умовах стали не просто засобами оптимізації внутрішніх процесів діяльності підприємства чи установи, а й основою динамічного розвитку новітніх інформаційних технологій. Важливим завданням сьогодення є організація електронного архіву на підприємствах. Робота в цьому напрямку допоможе подолати недоліки паперового архіву.

Аналіз останніх досліджень та публікацій. Сучасні інформаційні технології є невід'ємною складовою прогресивних підходів ефективної реалізації управлінської діяльності різного роду установ.

Проблематикою електронного документообігу підприємства займається чимало дослідників, серед яких В. І. Волинець [1], О. Б. Кукарін [2], І. В Куршатова [3], А. В. Ткачов [7], М. В. Ларін [4; 5], О. Матвієнко [6], Є. О. Плешкевич [8], М. Цивін [6] та ін. У наукових розвідках розглядаються, зокрема, такі питання: нормативно- методологічне регулювання, впровадження електронного документообігу; збереження електронних документів на підприємствах; використання досвіду інших країн для організації електронного документообігу на вітчизняних підприємствах. Однак низка важливих питань щодо впровадження та використання електронного документообігу в сфері підприємницької діяльності потребує додаткового дослідження.

Мета й завдання дослідження. Метою роботи є порівняльний аналіз сучасного виду електронного архіву та традиційного паперового на приватному підприємстві, дослідження їх переваг та недоліків.

Для досягнення поставленої мети визначено такі завдання:

- Визначити проблематику паперового виду архівів.
- Розглянути організацію електронних документів.
- Визначити переваги електронного архіву.

Об'єктом дослідження є електронний архів.

Предметом дослідження є використання електронного архіву на приватному підприємстві.

Виклад основного матеріалу. Досліджуючи проблеми застарілого виду архіву, а саме паперового було виявлено такі проблемі :

- Втрата документів

Ця проблема часто виникає і при передачі документів до паперового архіву та після тривалого зберігання, а також у процесі релокації архіву.

- Швидкість пошуку документа

Як правило, пошук документів дуже трудомісткий процес, особливо якщо йдеться про пошук документа двадцятирічної давності, а локацій паперового архіву кілька, і знаходяться вони в різних містах

- Вартість оренди приміщення для зберігання

Поряд з величезною кількістю документів приходить необхідність їх десь зберігати, але не всі установи мають вільні приміщення для організації паперового архіву. У цьому випадку оренда додаткових приміщень – дорога, але все ж таки необхідність.

- Можливість працювати в документі спільно

Найчастіше існує необхідність роботи з одним документом кільком співробітникам віддалено, що неможливо, використовуючи паперовий носій без перекладу його в цифровий формат

- Відсутність версіонування

При зміні архівного документа, а такі випадки теж трапляються, особливо коли проводиться зміна у наказі з особового складу або відпусток, немає можливості зберігати історію змін цього документа, крім як завести повторний паперовий бланк

- Підготовка звітності

Звітність – досить трудомісткий процес, а за відсутності швидкого доступу до єдиного електронного архіву він затягується на тривалий термін

- Залежність від надзвичайних ситуацій

Пожежа або затоплення архіву загрожує тим, що частина даних на паперових носіях може бути втрачена та не підлягати відновленню. Резервних копій документів на паперових носіях, як правило, не передбачено

Ці та інші недоліки стандартного архіву роблять його ведення застарілим процесом, який давно настав час замінити електронним архівом.

Так що ж таке електронний архів та які його переваги? Електронний архів є сховищем, в якому з ЕДО або інших цифрових джерел надходить потік документації, який за певними правилами розбивають, організуючи облік та архівування документів.

Організація архіву електронних документів передбачає:

Локальний архів - зберігання документів в електронному вигляді на сервері користувача;

Хмарне сховище – зберігання документів в електронному вигляді на сторонньому сервері та організація доступу через Інтернет;

Сховище системи ЕДО та архіву – зберігання документів у провайдера ЕДО. Організація та доступ обумовлюються з провайдером.

У процесі дослідження нами було виявлено ряд переваг електронного архіву. Перевагами електронного архіву є:

- Простота та швидкість роботи з архівом, зумовлені доступністю будь-якого документа за будь-який період у кілька кліків. Усі документи зберігаються у єдиній базі.
- Швидка відповідь на вимоги податкової. Полегшується та прискорюється пошук документів для відповіді на численні вимоги органів контролю.
- Підтвердження ставки ПДВ – 0%. Підтверджувати обґрунтованість пільгового оподаткування, у тому числі ставку ПДВ 0%, стає простішим Надійність та безпека. Організація електронного архіву відбувається таким чином, що доступ на запис та зміну файлів, по суті, має лише автоматизована система, а користувачам доступне лише читання документів. Зберігання документації виконується на носії інформації, з якого створюються резервні копії інших носіях, у своїй сервера повинні перебувати різних (фізично) машинах. Якщо якимось чином згорить або буде затоплений один сервер, завжди є його резервна копія, яку неважко було зробити. Відсутня можливість несанкціонованого доступу до даних, оскільки працює система розмежування доступу та прав.
- Ефективність роботи**.** Архів електронного вигляду дозволяє не тільки структурувати, а й сортувати документи щодо явних признаків, наприклад, дата, найменування та ін.
- Можливість масштабування. Зі зростанням компанії поступово зростає потік документації та відповідно місце, яке займає на носіях. У разі електронного архіву достатньо придбати додатковий носій інформації та підключити його до системи архівування. При цьому для деяких документів можна задавати термін придатності, після закінчення якого вони будуть автоматично стерті.
- Відсутність потреби у приміщеннях. На відміну від архіву з паперовими носіями зі зростанням електронного архіву не потрібно розширення приміщень, а значить компанія отримує велику економію, суму якої можна розглядати як частину прибутку при переведенні з паперового варіанта архіву на електронний.

Комплектування архіву та організація роботи з електронними документами у ньому проводиться за певними правилами. Перед передачею документів до електронного архіву проводиться експертиза цінності цих документів, що також регламентовано. Критеріями такої експертизи можна вважати можливість забезпечення тривалого зберігання, спосіб утримання, ступінь безпеки та ін.

Основним етапом комплектування архіву є запис упорядкованих документів на електронні носії. До вимог, що висуваються, у цій галузі може належати відповідність

певним форматам запису файлів або їх шифрування, застосування ліцензійного ПЗ, відповідність ГОСТу та інші вимоги.

Заключним етапом роботи з організації архіву електронних документів є перевірка носіїв із записаними файлами, створення на них відповідної документації та направлення до архіву для зберігання.

Облік електронних документів в архіві має свої особливості. Облік електронних документів ведеться у певних одиницях – справах. Кожна справа отримує свій обліковий номер, який є частиною шифру. Шифр та деякі облікові дані можуть бути нанесені на вкладку футляра цифрового носія. Архівний шифр повинен містити:

- Номер архівного фонду;
- Номер опису справ;
- Номер одиниці зберігання згідно з описом.
- Вкладиш цифрового носія повинен містити:
- Найменування компанії;
- Найменування підрозділу;
- Тип екземпляра;
- Номер опису;
- Дата запису на електронний носій;
- Відмітки про обмеження доступу.
- Відповідно до ДСТУ встановлено необходимость створення опису, де будуть перераховані документи, які входять у певну справу. Такий опис прикладається до справи, і у ній може здійснюватися пошук подальшої обробки документів чи утилізації. Описи необхідно об'єднувати в реєстр описів, що сприяє швидкому пошуку потрібної документації.

Будь-яка передача документів до архіву повинна бути відображена в обліковій книзі надходження носіїв, і факт зберігання повинен бути відображений у книзі обліку одиниць зберігання (справ). Всі ці та інші записи можуть виконуватися також в електронному вигляді. Це дозволяє повністю автоматизувати архів, як у поєднанні із системою ЕДО або СЕД, коли вся документація, включаючи документи бухгалтерського обліку, надходить у вже відсканованому вигляді, і її потрібно тільки помістити в архів, так і у поєднанні з ручним оцифруванням документації, що, звичайно менш ефективно, але все одно не заважає використовувати всі переваги електронного архіву, які були описані вище.

Висновки. Отже, електронний архів є більш надійним та прогресивним аналогом паперового архіву. Завдяки електронному архіву передача документів та їх пошук здійснюється набагато швидше і продуктивніше, що значно полегшує роботу.

Перехід від паперового до електронного архіву в системі інформаційно-документаційного забезпечення діяльності приватного підприємства має посилити вплив інформаційних процесів на різноманітні аспекти його життєдіяльності, а також підвищити конкурентоспроможність, створити умови наскрізного автоматизованого контролю на всіх етапах роботи з документами, що кардинально поліпшить якість роботи виконавців, зробить терміни підготовки документів більш прогнозованими і керованими, дозволить виконувати завдання, які складно або неможливо виконати традиційними методами.

Список літератури

1. Волинець В.І. Електронний цифровий підпис: сутність, принципи дії та порядок отримання. URL: http://dspace.tneu.edu.ua/ bitstream/316497/23292/1/111-112.pdf. (дата звернення 07.12.2020).
2. Кукарін О.Б. Електронний документообіг та захист інформації: навч. посіб. За заг. ред. Н.В. Грицяк. Київ: НАДУ, 2015. 84 с.
3. Куршатова І.В. Електронний документообіг і його особливості. Актуальні проблеми економіки. 2009. № 3. 237 с.
4. Ларин М.В. Некоторые проблемы эволюции управленческого документа. Вестник архивиста. 1999. № 6. 43 с.

5. Ларин М.В. Управление документацией в организациях. М.: научная книга. 2002. 288 с.
6. Матвієнко О., Цивін М. Основи організації електронного документообігу: навчальний посібник. К.: Центр учбової літератури, 2008. 112с. URL: http://kul-lib.narod.ru/bibl.files/Teach/Teachposibnuk.pdf (дата звернення 07.12.2020)
7. Нужный А. М., Сафронов В. В., Барабанов А. Б., Гаганов А. В. Создание электронного архива средствами pdm-систем. М., 2013. С. 6–10.
8. Тихонов В. И. Организация архивного хранения электронных документов. М., 2012. С. 211–214.
9. Миронов С., Слепко В., Хахамов С. Электронный архив: сделать самим или заказать «под ключ». М., 2006. С. 12–15.

УДК 657

М. Козакул, магістр гр. ОО(А)-20м-1.4
Центральноукраїнський національний технічний університет

ОСОБЛИВОСТІ ОБЛІКУ ВИРОБНИЧИХ ЗАПАСІВ НА СІЛЬСЬКОГОСПОДАРСЬКИХ ПІДПРИЄМСТВАХ

У статті розглянуто особливості обліку виробничих запасів на сільськогосподарських підприємствах. Визначено, що виробничі запаси обіймають значну питому вагу в складі оборотних активів агровиробників. Визначено проблеми та авторські перспективи удосконалення обліку операцій з виробничими запасами на сільськогосподарських підприємствах.
запаси, виробничі запаси, облік, сільськогосподарські підприємства, удосконалення, автоматизація обліку

Постановка проблеми. На сучасному етапі економічного розвитку агропромисловий сектор України (особливо центральної її частини) є однією з найважливіших ланок національної економіки. Виробництво конкурентоспроможної та якісної сільськогосподарської продукції, яка буде відповідати міжнародним стандартам, а її реалізація відбуватиметься за достойними справедливими цінами як на вітчизняному, так і на зарубіжних ринках є надзвичайно актуальним.

Сільськогосподарські (фермерські) господарства, здійснюючи виробничо-господарську діяльність, використовують в процесі виробництва, тобто у формуванні кінцевого продукту, виробничі запаси, які займають суттєву питому вагу в їх оборотному капіталі. Виробничі запаси з одного боку забезпечують постійність, безперервність та ритмічність діяльності підприємства, гарантують його економічну безпеку, з іншого – від чіткої та правдивої проінформованості про їх наявність, рух й організацію обліку залежить точність визначення прибутку, його фінансовий стан, конкурентоспроможність на ринку ефективність роботи в цілому. Через зміни, які можуть бути викликані погодними умовами, людським фактором, строками внесення добрив, гербіцидів, інсектицидів тощо, не завжди вдається вчасно отримувати достовірну інформацію щодо стану запасів на агропідприємствах та даних про їх точну наявність. Все це свідчить про необхідність удосконалення обліку виробничих запасів на сільськогосподарських підприємствах, що й стало метою даного дослідження.

Аналіз останніх досліджень і публікацій. Питанням обліку виробничих запасів сільськогосподарських підприємств увага приділяється постійно, адже майже кожен підручник з галузевого обліку містить окремий однойменний розділ. Серед досліджень, які було проаналізовано нами, виокремлюються роботи [1, 4, 6, 7], проте, наразі все ще залишається невирішеними ряд питань прикладного характеру.

Мета й завдання дослідження. Метою роботи є дослідження особливостей обліку виробничих запасів на сільськогосподарських підприємствах.

Для досягнення поставленої мети статті було визначено такі завдання: з'ясувати питому вагу, яку обіймають виробничі запаси в складі оборотних активів агровиробників; визначити проблеми з якими стикаються сільськогосподарські підприємства при обліку виробничих запасів; окреслити перспективи удосконалення обліку операцій з виробничими запасами на сільськогосподарських підприємствах.

Дослідження базувалось на основі системного підходу з використанням методів аналізу, узагальнення, групування та порівняння, а також з використанням графічного методу представлення інформації.

Основні результати дослідження. Запаси є активами, які: утримуються для подальшого продажу (розподілу, передачі) за умов звичайної господарської діяльності; перебувають у процесі виробництва з метою подальшого продажу продукту виробництва; утримуються для споживання під час виробництва продукції, виконання робіт та надання послуг, а також управління підприємством [2].

І. Садовська розглядає виробничі запаси за класифікаційними ознаками, які згруповано в таблиці 1.

Таблиця 1 – Класифікація виробничих запасів [6]

Класифікаційні групи запасів	**Вид запасів**	**Характеристика**
За призначенням і причинами утворення	Постійні	Частина виробничих запасів, що забезпечують безперервність виробничого процесу між двома черговими поставками
	Сезонні	Виробничі запаси, що утворяться при сезонному виробництві продукції чи під час сезонного транспортування
За місцем знаходження	Складські	Виробничі запаси, що знаходяться на складах підприємства У виробництві Що знаходяться у процесі обробки
	У виробництві	Що знаходяться у процесі обробки
За рівнем наявності на підприємстві	Нормативні	Виробничі записи, що відповідають запланованим обсягам виробничих запасів, необхідних для забезпечення безперебійної роботи підприємства
	Понаднормові	Що перевищують їх нормативну кількість
Відносно до балансу	Балансові	Запаси, що є власністю підприємства і відображаються в балансі
	Позабалансові	Запаси, що не належать підприємству, і знаходяться у нього через певні обставини
За походженням	Первинні	Запаси, що надійшли на підприємство від інших підприємств і не підлягають обробці
	Вторинні	Матеріали та вироби, що можуть застосовуватися вдруге у виробництві
За складом і структурою	Виробничі запаси	Запаси сировини, основних і допоміжних матеріалів, напівфабрикатів власного виробництва, купівельних напівфабрикатів, комплектуючих виробів, палива, запчастин, тари і тарних матеріалів, МШП
	Запаси незавершеного виробництва	Частина продукції, що не пройшла всіх стадій обробки та не прийнята відділом технічного контролю (ВТК)
	Запаси готової продукції	Продукція, виробництво якої завершене, що прийнята ВТК і знаходиться на складі
	Товарні запаси	Товари, що знаходяться, у сфері обігу, а також продукція, що знаходиться в дорозі

При відпуску запасів у виробництво, з виробництва, продаж та іншому вибутті оцінка їх здійснюється за одним з таких методів: ідентифікованої собівартості відповідної одиниці запасів; середньозваженої собівартості; собівартості перших за часом надходження запасів (ФІФО); нормативних затрат; ціни продажу [2]. Більшість сільськогосподарських підприємств при відпуску запасів у виробництво використовують саме метод середньозваженої собівартості.

Бухгалтерський облік виробничих запасів регламентується Законом України «Про бухгалтерський облік та фінансову звітність в Україні», НП(С)БО 1 «Загальні вимоги до фінансової звітності», НП(С)БО 9 «Запаси», Інструкцією про застосування Плану рахунків бухгалтерського облік активів, капіталу, зобов'язань і господарських операцій підприємств і організацій та Методичними рекомендаціями з бухгалтерського обліку запасів.

Необхідними передумовами правильної організації обліку запасів є: раціональна організація складського господарства; наявність інструкції з обліку виробничих запасів; розробка номенклатури запасів; правильне групування (класифікація) запасів; розробка норм витрачання запасів.

У роботі [3, с. 974] зазначається, що для вирішення проблеми організації обліку запасів на сільськогосподарському підприємстві, що перш за все необхідно дати відповідь на ряд запитань: Коли, звідки, скільки і на яку суму надійшли запаси, як виконуються програми постачання? Кому, коли і скільки відпущено запасів? Як виконується програма виробничого споживання? Який залишок по окремих видах запасів і як дотримуються встановлені ліміти тощо?

Однією з проблем сільськогосподарських підприємств є відсутність аналітичного обліку виробничих запасів, тобто їх деталізація. Інформація аналітичного обліку є релевантною для управлінців різних рівнів, тобто через відсутність номенклатури неможливо відслідкувати, яка кількість виробничих запасів була використана на ті чи інші потреби. Управлінці зацікавлені в ефективному виробництві сільськогосподарської продукції, тобто в зменшенні витрат на виробництво, зокрема виробничих запасів та збільшенні прибутку.

З метою збереження виробничих запасів до моменту використання їх у сільськогосподарському виробництві та готової продукції (товарів) до моменту її реалізації, організовується їх складське господарство. Складський облік запасів – це попредметний облік за разовими та накопичувальними видатковими документами. Складському обліку притаманні два методи: кількісно-сумовий – сутність полягає в паралельному веденні регістрів кількісно-сумової й кількісно-гатункової форм бухгалтерії на складі; оперативно-бухгалтерський – сутність полягає у тому, що бухгалтерія відкриває картки/книги складського обліку та передає їх під розписку в журналі реєстрації завідувачеві складу.

Для організації синтетичного обліку виробничих запасів призначено рахунок 20 «Виробничі запаси». Сільськогосподарські запаси, такі як посівний матеріал, засоби захисту рослин, добрива, корми тощо, мають обліковуватись на синтетичному рахунку 20 «Виробничі запаси». На наш погляд, доцільним буде використання субрахунку 208 «Матеріали сільськогосподарського призначення». На великих за площею господарствах, практикується відкриття субрахунків 2-го порядку, а саме 2081 «Добрива», 2082 «Посівний матеріал», 2083 «Засоби захисту рослин», 2084 «Десиканти», 2085 «Корми» (наведені субрахунки є умовними). Можливою ситуацією, коли при обліку у великих господарствах, відкривають субрахунки 3-го порядку при обліку власного насіння, саджанців, кормів, проте, у такому випадку обов'язковою умовою їх відображення в обліку є відокремлення придбаних подібних запасів «на стороні».

Для автоматизації обліку виробничих запасів пропонують використовувати найбільш розповсюджену в Україні програму 1С:Підприємство, а саме її версію 8.2. Це універсальна програма масового призначення для автоматизації обліку, що включає підготовку обов'язкової (регламентованою) звітності. Методика бухгалтерського обліку забезпечує одночасну реєстрацію кожного запису господарської операції як за рахунками

бухгалтерського обліку, так і за необхідними розрізами аналітичного, кількісного і валютного обліку [1]. У програмі 1С:Бухгалтерія версія 8 підтримуються наступні способи оцінки матеріально-виробничих запасів при їх вибутті: за середньою собівартістю; за собівартістю перших за часом придбання матеріально-виробничих запасів (спосіб ФІФО).

Використання сучасних інформаційних систем і технологій в обліку виробничих запасів сільськогосподарськими товаровиробниками, дозволяє оцінити стан справ на поточному етапі, перелік недоліків, невідповідностей, можливих ризиків, пов'язаних з ними, і рекомендації з їх усунення. Це дозволить керівникам оцінити якість впровадження, можливості системи, пріоритетність планованих завдань і вибір подальшої стратегії розвитку [5, с. 227]. Безсумнівно, що процес автоматизації був би у нагоді українським сільськогосподарським товаровиробникам, однак він вимагає додаткового спеціаліста, який буде займатись внесенням даних та перевіряти їх на достовірність. Через додаткові витрати, пов’язані з впровадженням сучасних інформаційних систем і технологій, не всі фермерські господарства погоджуються на такі оновлення в своєму робочому процесі. Ще одним негативним фактором, щодо впровадження повної автоматизації процесів формування запасів, є схильність керівників агропідприємств до дотримання «традиційних» правил господарювання, ведення обліку та небажання впроваджувати «щось нове», тобто проблемою є людський фактор.

Висновки. Ознайомившись з різними варіантами шляхів ведення та вдосконалення обліку виробничих запасів, запропонованих І. Принадою й О. Назарчуком [4, с. 66] та Г. Шинкарьовою й М. Подопригорою [7] можна зробити висновок, що кожен з них має як свої переваги так і недоліки, а спираючись на зазначені цими авторами напрямки, пропонуємо такі варіанти вдосконалення обліку виробничих запасів сільськогосподарських підприємств:

- підвищення оперативності інформаційного забезпечення управління виробничими запасами підприємств, яке забезпечується запровадженням інформаційних технологій обробки економічної інформації;
- удосконалення системи автоматизації обліково-аналітичних робіт в управлінні виробничими запасами шляхом впровадження програмного забезпечення 1С:Бухгалтерія, зокрема версії 8.2 конфігурацію «Сільське господарство»;
- чітка організація обліково-контрольних процедур руху запасів підприємств (застосування прийомів обліку за центрами відповідальності, заходів контролю та оперативного регулювання процесів утворення запасів). На практиці, всі ці процеси контролюються головним агрономом фермерського господарства чи безпосередньо головою господарства.

Підсумовуючи результати дослідження, можна стверджувати, що реалізація перелічених шляхів удосконалення обліку запасів призведе до більш ефективного їх використання та значного підвищення результативності фінансово-економічної діяльності аграрного сектору національної економіки України.

Список літератури

1. Головацька С.І., Бурдейна Л.І. Особливості обліку і оцінки виробничих запасів підприємств. Глобальні та національні проблеми економіки. 2015. Вип. 5. С. 973-976.
2. Національне Положення (стандарт) бухгалтерського обліку 9 «Запаси» : Наказ М-ва фінансів України від 20 жовт. 1999 р. № 246. URL: http://zakon4.rada.gov.ua/laws/show/z0751-99. (дата звернення: 01.10.2021)
3. Покоса Є., Підлепнюк О. Автоматизація бухгалтерського обліку запасів з допомогою програми 1С: Бухгалтерія 8.2. URL: http://sophus.at.ua/publ/2011_11_15_16_kampodilsk/section_7_011_11_15_16/avtomatizacija_bukhgalterskogo_obliku_zapasiv_z_dopomogoju_programi_1s_bukhgalterija_8_2/9-1-0-253. (дата звернення: 01.10.2021)
4. Принада І.В., Назарчук О.Д. Сучасні проблеми обліку виробничих запасів на підприємстві. Наука й економіка. 2014. № 3. С. 64-67.
5. Пугаченко О.Б. Особливості аудиту інформаційних систем і технологій. Наукові праці Кіровоградського національного технічного університету: Економічні науки. 2009. Вип. 16. Ч. ІІ. С. 223-228

6. Садовська І.Б. Класифікація виробничих запасів. URL: http://pidruchniki.com/1852102453245/klasifikatsiya_virobnichih_zapasiv. (дата звернення: 02.10.2021)
7. Шинкарьова Г., Подопригора М. Проблеми обліку виробничих запасів на підприємствах України. URL: http://rusnauka.com/36_PVMN_2012/Economics/7_123882.doc.htm. (дата звернення: 02.10.2021)

УДК 504.75

М. Ришкуляк, магістр гр. ЕО-20м,
Л. Коломієць, доцент
Центральноукраїнський національний технічний університет

ВПЛИВ ТОВ «ТЕПЛОЕНЕРГОЦЕНТР» НА ЕКОЛОГІЧНУ БЕЗПЕКУ АТМОСФЕРНОГО ПОВІТРЯ

Проаналізовано вплив підприємства теплоенергетики на стан довкілля та з’ясовано можливості поліпшення екологічної ситуації

теплоенергетика, атмосферне повітря, котлоагрегати, скрубер, забруднюючі речовини, викиди, димові гази, приземні концентрації, ГДК

Сучасні енергетичні об'єкти є великими комплексами, які мають різноманітний вплив на багато сфер життя і діяльності суспільства. Ці об'єкти тісно взаємопов'язані з споживачами продукції, що виробляється, з постачальниками сировини і між собою, і утворюють енергетичні системи з великою кількістю екологічних, соціальних і технологічних зв'язків. У плані найбільшого впливу на довкілля слід відмітити такі структурні одиниці підприємства, як котлотурбінний цех, електротехнічний цех, ремонтно-механічну службу. Використання технічних засобів, транспорту, паливно-енергетичних ресурсів передбачає утворення викидів. Зокрема атмосферне повітря забруднюється внаслідок спалювання палива та недосконалої системи очищення викидів [1,2].

Актуальність. Екологічна ситуація на Кіровоградщині характеризується високим рівнем антропогенного впливу на навколишнє середовище і значними екологічними наслідками минулої економічної діяльності. У зв'язку з гострою необхідністю термінових змін підходів до забезпечення якості навколишнього середовища і збереження здоров'я населення в нашій країні з 2014 року активно розробляються і вводяться в дію нове природоохоронне законодавство і численні екологоорієнтовані нормативно-правові акти, які впроваджують нові механізми управління охороною навколишнього середовища [3]. Як відомо, паливно-енергетичний комплекс відноситься до галузей з найбільшим негативним впливом на навколишнє середовище. Тому вкрай актуальним є впровадження нових технологій очищення викидів від шкідливих речовин.

Мета дослідження: визначити шляхи зниження негативного впливу ТОВ «Теплоенергоцентр» на атмосферне повітря.

Завдання: - вивчити екологічні аспекти впливу підприємства теплоенергетики на стан довкілля

-з’ясувати технологічні виробничого процесу та джерела утворення шкіливих речовин

-запропонувати можливі шляхи зниження негативного впливу підприємства на стан атмосфери

Об’єкт дослідження: вплив на довкілля підприємства теплоенергетики

Предмет дослідження: впровадження очисного обладнання для зниження рівня викидів

Результати досліджень.

Найбільш впливовим наслідком роботи ТОВ Теплоенергоцентр у місті Кропивницький є забруднення атмосферного повітря. Закон України «Про охорону атмосферного повітря» спрямований на збереження та відновлення природного стану атмосферного повітря, створення сприятливих умов для життєдіяльності, забезпечення екологічної безпеки та запобігання шкідливому впливу атмосферного повітря. Конституцією України передбачено, що атмосферне повітря є об'єктом права власності Українського народу, а кожний громадянин має право користуватися цим об'єктом права відповідно до закону (ст. 13). [3].

Модернізування очисного обладнання є складовою частиною сучасного процесу виробництва теплоти та електроенергії, і витрати на них враховуються в економічних показниках підприємства. У зв'язку з цим основні критерії обґрунтування ефективності капітальних вкладень в енергетичні об'єкти в рівній мірі справедливі і при оцінці ефективності капіталовкладень в здійснювані на них природоохоронні заходи .[4]

Устаткування для здійснення технологічного процесу вироблення енеңргії на сьогодні являє собою:

- два енергоблоки з котлом ТГМЕ-464 і паровою турбіною Т-110 / 120-130 загальною тепловою потужністю 350 Гкал / год і електричною - 240 МВт;
- один блок з котлом ТГМП-344 А і паровою турбіною Т-300 / 250-240 тепловою потужністю – 350 ГКал / год і електричної - 300 МВт
- чотири водогрійних котла типу ПТВМ-180 продуктивністю по 180 ГКал / год кожен.

Котел ТГМЕ-464 вже багато десятиліть користується визнанням в теплоенергетиці. Працює на природному газі та високосірчистому мазуті. Конструктивно являє собою однобарабанний однокорпусний котел; 16 штук газомазутних пальників на задній стінці камери згоряння, розміщені у два яруси. Вода з барабана потрапляє в екрани по опускних вертикальних стійках.

У верхній частині топки по периметру розміщено два ряди горизонтальних двоходових радіаційних трубних напрямків первинного пароперегрівача. У опускному вертикальному газоході встановлено економайзер.

Котел виготовлений без каркаса, тобто підвішений тягами до перекриття будівлі котельні.

Для очищення поверхонь нагріву використовується дробоочищення.

Технічні характеристики котла ТГМЕ-464 наведені в табл. 1.

Таблиця 1 ─ Технічні характеристики котла ТГМЕ-464

№ n/n	Показники	Значення
1	Паропродуктивність, т/ч	500
2	Тиск пари на виході з котла, МПа	13,73
3	Температура нагріву повітря, ◦С	259
4	Температура вихідних газів, ◦С	137
5	Температура живильної води, ◦С	230
6	Температура холодного повітря, ◦С	30
7	Температура гарячого повітря, ◦С	336
8	Температура пари на виході з котла, ◦С	560
9	ККД (брутто), %	94,3
10	Тепронапруження об’єму топки, кДж/м^3·год	2409·10^3

11	Поверхня нагріву, $м^2$: - топки - пароперегрівач - економайзер - повітряпідігрівач	 809 3780 2570 55600
12	Аеродинамічний опір, кПа: - по газах - по повітрю	 4,14 5,49

У котлотурбінному цеху ТОВ Теплоенергоцентр (м. Кропивницький) встановлено 16 котлоагрегатів ПК-39-І, ІІ. Основним паливом для котлоагрегатів ПК-39 є вугілля; розпалювальним – мазут марки М-100. Частка розпалювального мазуту у структурі паливного балансу становить 1.28 %, тому максимально разові викиди від котлоагрегатів ПК-39 визначається тільки при спалюванні вугілля [4,5].

Викиди димових газів від джерела 001 (котлоагрегати 1-4 енергоблоків) здійснюється через димову трубу №1 (висота 250 м, діаметр гирла – 9 м). Викиди димових газів від джерела 002 (котлоагрегати 5-6 енергоблоків) здійснюється через димову трубу №2 (висота 180 м, діаметр гирла – 7,6 м). Викиди димових газів від джерела 003 (котлоагрегати 7-8 енергоблоків) здійснюється через димову трубу №3 (висота 180 м, діаметр гирла – 7,6 м).

Викиди забруднюючих речовин з димовими газами ТОВ Теплоенергоцентр у місті Кропивницький становлять 125 362,147 тон або 99,85 % від загальної кількості викидів. Викиди димарів містять 58617,715 тонн золи вугілля, 48219,387 тонн діоксиду сірки, 13713,989 тон діоксиду азоту, 222,85 тонн оксиду азоту, 2581,246 тон оксиду вуглецю та 0,075 тонн мазутної золи (у перерахунку на ванадій) [4].

Серед інших забруднюючих речовин у викидах ТОВ Теплоенергоцентр у місті Кропивницький є пил вугільний, зварювальний аерозоль, оксиди марганцю, заліза, нікелю, хром шестивалентний, фтористий водень, фториди, сполуки кремнію, пил абразивний, пил деревний та вуглеводні, загальною кількістю 182,568 т. З забруднюючих речовин, що викидаються в атмосферу, ефект суммації мають: діоксид сірки і діоксид азоту, діоксид сірки, оксид азоту і мазутна зола, діоксид сірки і фтористий водень, пилу з різними коефіцієнтами осідання [4,6,7].

Для зниження величини викидів забруднюючих речовин в атмосферу пропонується використовувати очищення газоповітряної суміші від котлоагрегату електрофільтром з коефіцієнтом очищення 99,6%.

На ТОВ Теплоенергоцентр (м. Кропивницький) працюють 16 котлоагрегатів, утворюючи викиди димових газів, які об'єднано в три димові труби. Викиди димових газів від семи котлів виведені на дві димові труби; для зниження викидів на джерелах 002 та 003 було встановлено електрофільтри ЕГС фірми «LUK» (Німеччина) .

Джерело 001 (найбільший котлоагрегат 1А, 1Б) – перший енергоблок має вихід на трубу окремим газоходом, який в даний час для очищення димових газів обладнаний скрубером Вентурі. Даний скрубер для очищення димових газів має недостатній рівень ефективності очищення, що досягає до 97%. Скрубер має підвищені експлуатаційні та технологічні витрати, які пов'язані з додатковими витратами на очищення димових газів (розгін газів, що очищаються, подача води під високим тиском в сопла скрубера Вентурі, наявність додаткового технологічного обладнання, а саме краплеуловлювача з утворенням шламу).

Робота скрубера Вентурі полягає в очищенні атмосферного повітря від пилу. Намоклі порошинки, рухаючись в газоповітряному потоці, при зіткненні злипаються і відокремлюються в уловлювачі.

Головне завдання мокрого очищення повітря від пилових часток – забезпечення максимальної площі контакту газоповітряної суміші з рідиною.

Запилене повітря подається в конфузор. Просуваючись по трубі діаметру, що звужується, газоповітряний потік набирає швидкість. Чим більше перепад площі поперечного перетину на вході і виході конфузора, тим вище швидкість. У порожнину секції, що звужується, по форсунках подається технічна вода або розчин абсорбуючого реагенту. Проходячи через горловину, повітря поступає в дифузор. Тут швидкість руху потоку сповільнюється. Мікрокраплі з уловленим пилом або газом з'єднуються.

На виході з пристрою зважена рідина затримується в краплеуловлювачі, а очищене повітря викидається в атмосферу.

Шлам який осідає в колекторі, в залежності від технічної придатності і складу, може бути в результаті утилізованим або відправленим у повторний виробничий цикл за допомогою рециркуляції [8].

Швидкісні газопромивачі (скрубери) об'єднують у велику групу апаратів, загальним для яких є наявність труби-розпилювача, в якій здійснюється інтенсивне дроблення газовим потоком, що рухається з високою швидкістю (порядку 40-150 м/с), що зрошує його рідини та встановленого за нею краплеуловлювача. Спочатку як труба розпилювача використовувалася труба Вентурі в її чистому вигляді, звідки і з'явилася назва газопромивачів подібного типу. Скрубери Вентурі – найбільш ефективні з апаратів мокрого очищення газів. Осадження частинок на краплях зрошуючої рідини сприяють високі відносні швидкості між ним у трубах розпилювачах. У скрубері Вентурі реалізується краплинна абсорбція, яка складається з «сопла Вентурі» (конфузор, дифузор) та краплеуловлювача. У конфузорній частині сопла підводиться запилений потік газу, а через форсунки під тиском впорскується рідина для зрошення цього потоку. У конфузорі відбувається розгін газу від початкової швидкості газу (wг = 15...20 м/с) до швидкості wг = 30...200 м/с у вузькій частині сопла [8].

Процес осадження частинок пилу на краплі рідини обумовлений великою різницею між масами (щільністю) рідини та газу, розвиненою поверхнею крапель та високою різницею (до 100 м/с) швидкостей частинок пилу та рідини в конфузорі. Ефективність очищення значною мірою залежить від рівномірності розподілу рідини по перерізу конфузора. У дифузорній частині сопла різко падає тиск із конденсацією пари. Потік із конденсованими парами поступово гальмується до швидкості wг = 15...20 м/с і потрапляє в краплеуловлювач, який зазвичай виконується у вигляді прямоточного циклону.

Скрубери Вентурі забезпечують досить високу ефективність очищення аерозолів (до = 0,99) із середнім діаметром розмірів частинок 1...10 мкм і більше при початковій концентрації домішок до 100 г/м^3. Питома витрата води зрошення у своїй становить 0,1…6 л/м^3.

Джерелом можливого забруднення атмосферного повітря на ТОВ «Теплоенергоцентр» у місті Кропивницький є котли, при спалюванні в яких природного газу в атмосферу виділяються димові гази, що містять зокрема діоксид азоту та оксид вуглецю. На ТОВ «Теплоенергоцентр» у місті Кропивницький на джерелах викидів 002 та 003 рекомендовано встановити електрофільтри типу ЄГС фірми «LUK» ФРН. Реконструкція системи очищення димових газів на джерелі 001 шляхом заміни існуючого скрубера Вентурі на електрофільтр ЄГС фірми «LUK» ФРН з ефективністю очищення 99,6 % дозволить значно зменшити викиди шкідливих речовин.

Електрофільтри являють собою апарат з вертикальним та горизонтальним рухом газового потоку, в якому розміщені осаджувальні та коронуючі електроди. Осаджувальні електроди заземлені, а до коронуючих підводиться випрямлений електричний струм високої напруги від перетворювальної підстанції.

Процес очищення газів в електрофільтрі можна розділити на стадії: заряджання зважених частинок у полі коронного розряду, рух заряджених частинок до електродів, осадження частинок на електродах, видалення осаджених частинок з поверхні електродів. Будову запропонованого електрофільтру наведено на рисунку 2.

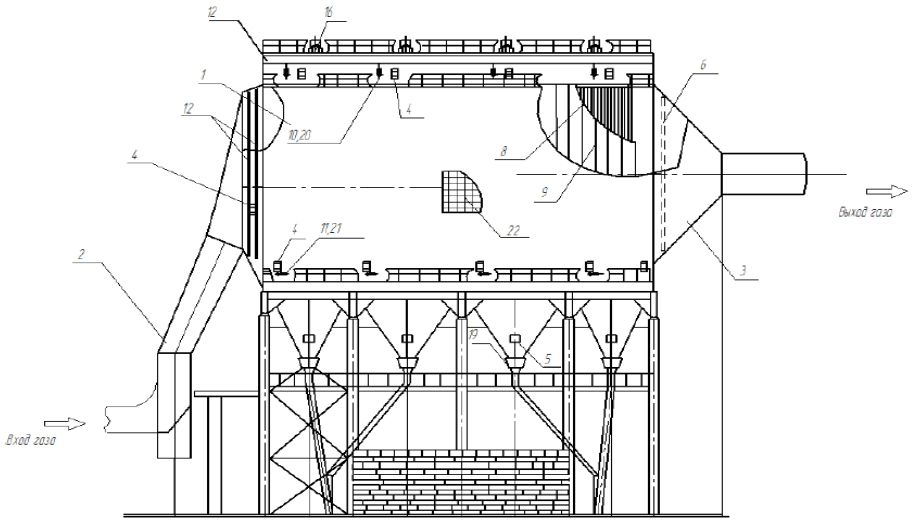


Рисунок 2 - Схема електрофільтра ЄГС «LUC» (Німеччина):

1-корпус електрофільтра; 2-дифузор односекційний; 3-конфузор односекційний; 4-двері інспекційні; 5-люк інспекційний; 6-система газорозподілу на виході; 7-газовідбійні екрани в бункерах та корпусі ел.фільтра; 8-комплект системи коронуючих електродів; 9-комлект системи осаджувальних електродів; 10-комплект струшування для системи коронуючих електродоа; 11-комплект струшування для системи осаджувальних електродів; 12-тунель опорних ізоляторів; 13-ізолятор опорний; 14-ізолятор прохідний; 15-електронагрівальний елемент опорного ізолятора; 16-токопровід; 17-агрегат харчування; 18-масляний піддон; 19-електронагрівальний елемент бункера; 20-електропривод струшування коронуючих електродів; 21-електропривод струшування осадових електродів; 22-теплоізоляція електрофільтра.

Переваги електричних фільтрів:

низькі енерговитрати (0,1-0,5 кв год) на м3 газів;

високий ступінь очищення газів – до 99% і вище при уловлюванні частинок будь-яких розмірів;

низький газодинамічний опір (100-150 па);

можливість роботи в агресивних середовищах;

можливість очищення високотемпературних газів;

можливість повної автоматизації; процеси регулювання напруги, видалення з електродів уловлених частинок та вивантаження пилу в електрофільтрах можуть бути повністю механізовані та автоматизовані;

широкий діапазон застосування;

можливість очищення як від твердих, так і від рідких частинок.

Очищення димових газів відбувається наступним чином: у котел котлотурбінного цеху надходить вугілля з БСУ. При спалюванні вугілля в котлах, закипає вода і утворюється тепла пара, яка призводить до руху турбіни. Обертаючи турбіни виробляють електричну енергію. При спалюванні палива важкий дим із золою виходить на електрофільтри. Дим проходить через електрофільтри та очищається до 99.6% і відводиться у димові труби. При очищенні диму із золою через електрофільтри зола випадає в спеціальні накопичувачі і далі відправляється на золовідвал.

Розрахунки розсіювання забруднюючих речовин в атмосфері від одиночних стаціонарних джерел забруднення атмосфери виконували на основі «Методики розрахунку концентрацій в атмосферному повітрі шкідливих речовин, які є в викидах підприємств. Загальносоюзний нормативний документ-86».

На існуюче положення максимальні приземні концентрації золи вугілля, діоксиду сірки та групи сумації (азота діоксид, азоту оксид, сірка діоксид та мазутна зола), (азота діоксид та сірки діоксид), (вуглецю оксид та пил неорганічний) вище гранично-допустимих значень. За іншими речовинами максимальні приземні концентрації у промисловій зоні, охоронній зоні, санітарно-захисній зоні та у житловій зоні не перевищують ГДК.

Здійснено розрахунок розсіювання викидів забруднюючих речовин після запропонованих заходів щодо зниження викидів запровадження системи очищення димових газів.

Таблиця 2 – Результати розрахунку розсіювання після реконструкції системи очищення

Найменування забруднюючої речовини	Код	Максимальна концентрація, частки ГДК			
		Промислова зона	СЗЗ	Охоронна зона	Житлова зона
Азоту діоксид	0301	0,06	0,18	0,31	0,30
Азоту оксид	0304	0,005	0,02	0,03	0,02
Сірки діоксид	0330	0,005	0,26	0,45	0,44
Вуглецю оксид	0337	розрахунок недоцільний			
Зола вугілля	2908	0,17	0,49	0,84	0,81
Група сумації (азоту діоксид, азоту оксид, сірка діоксид та мазутна зола)	6006	0,16	0,47	0,79	0,77
Група сумації (азоту діоксид і сірки діоксид)	6009	0,16	0,45	0,76	0,74
Група сумації (вуглецю оксид та пил неорганічний)	6046	0,17	0,49	0,84	0,82

При аналізі результатів розрахунку виявлено, що на перспективу максимальні приземні концентрації сірки діоксиду, золи вугілля та групи суммації (азота діоксид, азоту оксид, сірка діоксид та мазутна зола), (азота діоксид та сірки діоксид), (вуглецю оксид та пил неорганічний) не перевищуватимуть гранично-допустимих значень.

Таким чином, після реконструкції при виконанні очищення газів в електрофільтрах несприятливий вплив на довкілля зведеться до мінімуму, оскільки частки ГДК забруднюючих речовин всі без винятку, згідно результатів розрахунку розсіювання, будуть становити менше одиниці (<1).

Висновок. З метою запобігання забруднення атмосферного повітря запропоновано встановлення електрофільтру ЄГС фірми «LUK» (Німеччина). Після реконструкції системи очищення димових газів на першому енергоблоці турбінного цеху викиди золи вугілля значно знижуються і, якщо до реконструкції цей показник становив 2,02 частки ГДК в житловій зоні, то тепер – лише 0,81 ГДК . Виконані природоохоронні заходи спрямовані на підвищення промислової та екологічної безпеки виробництва.

Список літератури

1. Забруднення атмосферного повітря міста, ризик для населення / І. О. Черниченко, О. М. Литвиченко, Я. В. Першегуба [та ін.] // Гігієна населених місць. – № 51. – 2018. – С. 151–159.
2. Мельник, Л. Г. Основи екології. Екологічна економіка та управління природокористуванням: підруч. [Текст] / Л. Г. Мельник, М. К. Шапочка – Суми: ВТД «Університетська книга», 2007. – 759с.

3. Закон України «Про охорону атмосферного повітря» № 124-IX від 20.09.2019, ВВР, 2019, № 46, ст.295 ─ [Електронний ресурс]. ─ Режим доступу: https://zakon.rada.gov.ua/laws/show/2707-12#Text
4. https://teploenergetik.kr.ua/ Офіційний сайт ТОВ Теплоенергоцентр м Кропивницький
5. Долина Л. Ф. Практикум по очистке пылегазовых выбросов промышленных и аграрных предприятий. Учебное пособие. – Днепропетровск: Континент, 2019 – 253 с.
6. Другов Ю. С. Газохроматографический анализ загрязненного воздуха: Практическое руководство / Ю. С. Другов, А. А. Родин.- М.: БИНОМ. Лаборатория знаний, 2016. – 528 с.
7. Новожилова Л.Л, Росляков П.В, Єгорова Л.Є. Організація моніторингу шкідливих викидів із димових труб ТЕС на основі чисельних досліджень//Вісник МЕІ, 2018, N4.С.28-35.
8. Скруббер Вентури 86 ─ [Електронний ресурс]. ─ Режим доступу: https://gas-cleaning.ru/article/skrubber-venturi-princip-raboty-harakteristiki-preimushchestva-i-nedostatki

УДК 004

М. Грішин, магістр гр. КІ-20М1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ОБ'ЄДНАННЯ ВІДЕО, АУДІО, WEB-СТРІММІНГУ ТА ПОВІДОМЛЕНЬ

У статті розроблено програмне забезпечення, яке призначено для системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень. Метою розробки є дослідження та програмна реалізація системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.Об'єктом дослідження є процес інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень. Предметом дослідження є методи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень. Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, інформаційний простір, об'єднання відео, аудіо, Web-стріммінгу та повідомлень

Постановка проблеми. Уніфіковане співробітництво – один з основних драйверів підвищення продуктивності праці. І це нова реальність, у якій завдяки використанню сучасних технологій стає можливим перехід від звичних комунікацій на новий рівень взаємодії усередині робітників груп. Якщо говорити більше просто, уніфіковане співробітництво являє собою об'єднання відео, голосу, Web-стрімінгу й обміну повідомленнями в одному інформаційному просторі.

Тенденції ринку такі, що програмне забезпечення грає все більшу роль. Це дозволяє, зокрема, охопити набагато більше клієнтів рівня СМБ, які раніше подібними послугами не користувалися. У цьому велика заслуга Microsoft, що відкрила цим клієнтам двері в світ відео-конференц-зв'язку й уніфікованих комунікацій.

Що ж у дійсності відбувається на ринку ВКЗ і UC? Коло споживачів відповідних сервісів розширюється за рахунок малих і середніх компаній. Тим часом великі корпорації були й залишаються консервативними прихильниками традиційних рішень ВКЗ. У них є свої вимоги й очікування з погляду продуктивності, надійності, масштабованості.

Великому бізнесу потрібні звичні рішення певного класу. У доступному для огляду майбутньому Microsoft навряд чи буде пропонувати відповідні рішення, – поки ніщо на це не вказує. Рішення ж для невеликих і середніх компаній зовсім інша справа. Вони будуть

з'єднуватися завдяки появі конвергентних систем, які можуть бути використані для різного класу завдань.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

– Дослідження системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

– Програмна реалізація системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

Об'єктом дослідження є процес інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

Предметом дослідження є методи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

Методи дослідження базуються на методах теорії кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У процесі читання технічних описів різних відеоконференцій у тексті й, особливо, у таблицях часто попадаються символьні позначення всіляких стандартів, характеристик і параметрів.

На перший погляд, всі ці стандарти здаються декілька одноманітним потоком абревіатур, однак, спробуємо послідовно розібратися в деяких позначеннях.

У цьому розділі даний короткий огляд стандартів (протоколів) передачі даних використовуваних у відеоконференціях.

Протокол – формальний опис набору правил і угод, які визначають, як саме пристрою в мережі обмінюються даними. Протоколи розробляються міжнародною організацією по стандартизації – ITU-**T**.

ITU-T – (International Telecommunication Union – Telecommunication sector) сектор стандартизації електрозв'язку Міжнародного союзу електрозв'язку.

H.320 – протокол передачі даних по мережах **ISDN**, тобто по звичайних провідних телефонних лініях, за допомогою модему. Даний стандарт описує вимоги до різних пристроїв уведення/виводу зображення, звуку або потоку даних для систем відео-телефонії й **відео-конференц-зв'язку**.

H.321 – модифікація протоколу **H.320** для використання в широкополосних мережах B-**ISDN на** основі технології асинхронної передачі даних **ATM**, призначеної для роботи в мережах із сильно, що розрізняється швидкістю, передачі даних.

H.322 – також, модифікація протоколу **H.320** для роботи в мережах з комутацією пакетів з гарантованою пропускною здатністю.

H.323 – протокол пакетної передачі даних широко використовуваний в IP телефонії й відео-конференц-зв'язку, що дозволяє проводити двосторонні «точка-точка» і багатобічні «точка-багато точок» мультимедіа-конференції.

SIP – як заміна стандарту **H.323**, що включає в себе: простоту, незалежність від транспортного рівня, персональну мобільність користувача (на підставі унікального ідентифікатора користувача), масштабованість мережі, розширюваність протоколу новими функціями, інтеграція з існуючими протоколами Інтернет.

H.324 – протокол для передачі голосу, відеосигналу й даних по звичайних телефонних лініях з низькою пропускною здатністю, за допомогою модему. H.324-термінал може бути інтегрований, наприклад, у персональний комп'ютер або відеотелефон і забезпечувати

двосторонню або багатобічну відео-конференц-зв’язок – при наявності окремого сервера багатоточечного зв'язку (MCU).

H.239 – протокол підтримуючий подвійний відео-потік, наприклад, зображення учасника конференції й презентація (або сигнал з додаткової камери), трансльовані на один або на різні дисплеї. Стандарт розроблений в 2003 році, спільно компаніями Tandberg і Polycom під назвами DuoVideo **i** People+Content.

H.460 – як розширення протоколу для відеоконференцій H.323 з метою обходу NAT (трансляція мережних адрес) і Firewall (система мережного захисту), що дозволяє з'єднуватися двом кінцевим точкам без проміжного вузла.

Стандарт H.323

H.323 є одним з найстарших стандартів, використовуваних для організації VoIP-Телефонії й відео-конференц-зв’язку. Це ціла система протоколів і елементів, які дозволяють передавати медіадані по пакетних мережах з негарантованою пропускною здатністю. Структура рекомендації H.323 забезпечує різні можливості комунікації – від звичайної телефонії до відео-конференц-зв’язку з передачею медіаданих.

Одним з переваг стандарту H.323 є його сполучна функція, що дозволяє пристроям різних виробників взаємодіяти один з одним.

До появи протоколу H.323 всі VoIP-застосунки працювали на власних сигнальних протоколах, тому зв'язок між ними була неможлива. Однак в 1996 році опублікували першу версію H.323 і цей стандарт одержав широке поширення.

З моменту появи стандарту H.323 пройшло багато років, і, природно, він удосконалювався з кожною версією. З 1996 року до сьогоднішнього дня було випущено 7 версій стандарту.

Перша версія була досить убогою, тому як випускалася з головною метою – налагодити комунікацію між терміналами різних виробників. Про надійність, безпеку й гарну якість зв'язку мови поки не йшло, до того ж, раннє несумісні один з одним, термінали могли “спілкуватися” тільки усередині корпоративної мережі.

Проривом стала друга версія, що вийшла через два роки й була спрямована на активне використання в VoIP-Телефонії й багатобічних конференціях. Цього разу ключовим словом стала надійність – підтвердження вірогідності кінцевих точок (учасників конференції), незмінність пакетних даних при передачі, захист від несанкціонованого злому даних і, як не дивно, відсутність відхилення вхідних викликів. Також було прискорене з'єднання між терміналами й додана можливість переадресації дзвінків.

Третя версія забезпечила передачу сигналізації для більшого числа викликів за допомогою одного TCP-з'єднання. Міжмережеві шлюзи, які могли забезпечити до тисячі одночасних викликів, особливо виграли тоді.

Зміни в четвертому випуску торкнулися нарощування ємності H.323-терміналів, а вихід п'ятої версії був спрямований на загальну стабілізацію стандарту. До речі, рішення TrueConf працюють на четвертій версії протоколу H.323.

У червні 2006 року затвердили шосту версію стандарту зі змінами по частині транспортних протоколів H.225 і H.245. З'явилася підтримка Assigned Gatekeeper – призначеного воротаря, на якому реєструється кінцева точка зі списку альтернативних гейткіперів. Крім цього, минулого підтримані документи й ряд застосунків, що дозволяють використовувати кодеки GSM і H.264 в H.323-рішеннях.

Фінальна – сьома версія H.323 вийшла в листопаді 2009 року. Серед безлічі відновлень варто виділити дві важливі для користувачів можливості:

– передача інформації про користувачів кількома мовами (це дозволило співробітникам різних міжнародних організацій без праці взаємодіяти один з одним);

– автоматична доставка даних про групову конференцію, що проходить на MCU-сервері, всім H.323-терміналам (це дозволило користувачам підключатися до конференції без уведення яких-небудь даних про неї).

Архітектура

Стандарт Н.323 ґрунтується на чотирьох компонентах для організації відеоконференцій типу точка-точка або багатоточка:

- термінали;
- шлюзи;
- контролери зони (воротар);
- сервер багатоточечних конференцій (MCU).

Термінал – це по суті інструмент для керування Н.323-пристроєм, етакий користувальницький інтерфейс, кінцева точка. Термінали можуть зв'язуватися один з одним у режимі VoIP-Телефонії або відео-конференц-зв’язку. Для зв'язку терміналів з різних мереж – приміром, Н.323 і ISDN, використовуються **шлюзи**. Вони виконують наступні функції:

- установка з'єднання між терміналами;
- конвертація звукових форматів;
- обмін інформацією.

Якщо термінали перебувають в одній Н.323-мережі, шлюзи не використовуються.

Контролер зони або **гейткіпер** – це центральна точка Н.323-мережі, оскільки саме гейткіпер відповідає за адресацію викликів, управляє шириною смуги пропущення й установлює дійсність терміналів і шлюзів під час з'єднання. Хоча рекомендація Н.323 не визначає воротар як обов'язковий елемент, все-таки без нього неможливе використання безлічі сучасних функцій, які впроваджують у свої рішення виробники VoIP-застосунків і рішень відео-конференц-зв’язку.

Для зв'язку трьох і більше терміналів використовується сервер багатоточечних конференцій MCU (Multipoint Control Unit). Всі термінали, які беруть участь у конференції, спочатку зв'язуються з MCU-сервером, а MCU у свою чергу розподіляє відеопотоки по всіх терміналах. Сам пристрій MCU звичайно також поєднує в собі ролі гейткіпера й шлюзу.

Протоколи Н.323

Кожний Н.323-термінал або пристрій, що підтримує протокол Н.323, має свій власний IP-адреса. По ньому здійснюється механізм маршрутизації Н.323-пакетів усередині мережі. Для зв'язку терміналів зі шлюзами й гейткіпером, а також для передачі медіатрафіку використовуються протоколи UDP. Транспортні протоколи TCP використовуються тільки для встановлення дзвінка між терміналами й обміну додатковими можливостями.

Передача медіаданих за рекомендацією Н.323 розділена на п'ять основних етапів:

- виявлення гейткіпера й реєстрація на ньому;
- установка з'єднання між двома й більше терміналами;
- обмін голосом і відео – передача за допомогою транспортних протоколів;
- обмін мультимедіа – передача різних графічних або текстових документів, спільна робота над ними;
- завершення виклику.

Процес виявлення потрібний для того, щоб кінцеві точки (термінали) могли знайти воротар по мережній адресі й зареєструватися на ньому. Ця процедура може виконуватися автоматично (багатоадресне розсилання – обмін повідомленнями між кінцевими точками й гейткіпером, якщо гейткіперів декілька, термінал самостійно вибирає, на якому йому реєструватися) або вручну (коли мережна адреса гейткіпера відома заздалегідь при конфігурації пристрою). Переважніше перший варіант виявлення гейткіпера, оскільки у випадку яких-небудь несправностей у його роботі термінал (кінцева точка) зможе автоматично перемкнутися на інший гейткіпер, без втручання в конфігурацію.

Процедура реєстрації необхідна для того, щоб кінцеві точки (термінали) могли повідомити свої адреси гейткіперу й увійти в його зону керування.

Для установки з'єднання між терміналами й для обміну медіатрафіком використовуються наступні протоколи:

TCP:

– **H.225** – установка з'єднання між H.323-пристроями.

– **H.245** – обмін інформацією про можливості (підтримувані кодеки, наприклад). Один термінал “повідомляє” іншому терміналу про підтримувані можливості (кодеках), і вибирає кодек для відправлення з можливостей іншого термінала.

UDP:

– **RAS** – використовується між терміналами, шлюзами й гейткіпером. Відповідає за реєстрацію, дозвіл на дзвінки й статуси.

– **RTP** – використовується при передачі медіатрафіку в реальному часі.

Для завершення з'єднання термінали посилають повідомлення гейткіперу, після чого канал закривається й зв'язок переривається.

Кодеки H.323

Стандарт H.323 визначає функцію обміну аудіоинформацией як основну свою можливість (так було споконвічно, адже H.323 завжди застосовувався саме в VoIP-Телефонії), тому кожний термінал повинен був підтримувати як мінімум один кодек із сімейства G.7XX. А от відеозв'язок у відношенні H.323 позиціонувалося як другорядне завдання, у виді чого підтримка видеокодеков не була обов'язковою. Однак сьогодні, в епоху існування відео-конференц-зв’язку й інтеграції її в безліч H.323-терміналів, видеокодеки входять до числа обов'язкових. Для кодування відео в H.323 використовуються видеокодеки сімейства H.26X.

До голосових кодекам в H.323 існує ряд певних технічних вимог, оскільки саме звук в VoIP-Телефонії є основним елементом. Вимоги наступні:

– низький рівень затримки;
– можливість відновлення загублених пакетів;
– висока якість звуку;
– мала смуга пропущення (не більше 8 kbit/s).

Всім цим вимогам відповідають кодеки сімейства G.7XX. Однак якщо говорити про останній пункт даного списку, те лише деякі з G.7XX відповідають йому.

За замовчуванням в H.323 використовується кодек G.711, що має досить високий коефіцієнт смуги пропущення – 64 kbit/s. До того ж, G.711 на сьогоднішній день уважається застарілої кодеком, адже його частота дискретизації (перетворення аналогового сигналу в цифровий) становить усього 8 kHz, у той час, як в іншого кодеку – більше сучасного G.722.1 ця цифра у два рази більше (16 kHz). До речі, для інтернет-з'єднань раніше використовувалися низькочастотні кодеки G.723 (5.3/6.3 kbps) і G.729 (8 kbps).

Що стосується видеокодеков, отут все просто: стандартом уже багато років є видеокодек H.264. Його послідовник H.265 поки не знайшов популярності й підтриманий тільки на нових пристроях, тому ми не думаємо що він буде масово використовуватися раніше 2022 року.

Розробка структурної схеми

Система інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень оснащена підтримкою Omni-Protocol для WebRTC, Skype для бізнесу, SIP і H.323, надаючи користувачам більше різноманітні й прості у використанні можливості для спільної роботи. На додаток до підтримки Omni-Protocol підтримує прийом, спільне використання й потоковий уміст у всіх протоколах підключення.

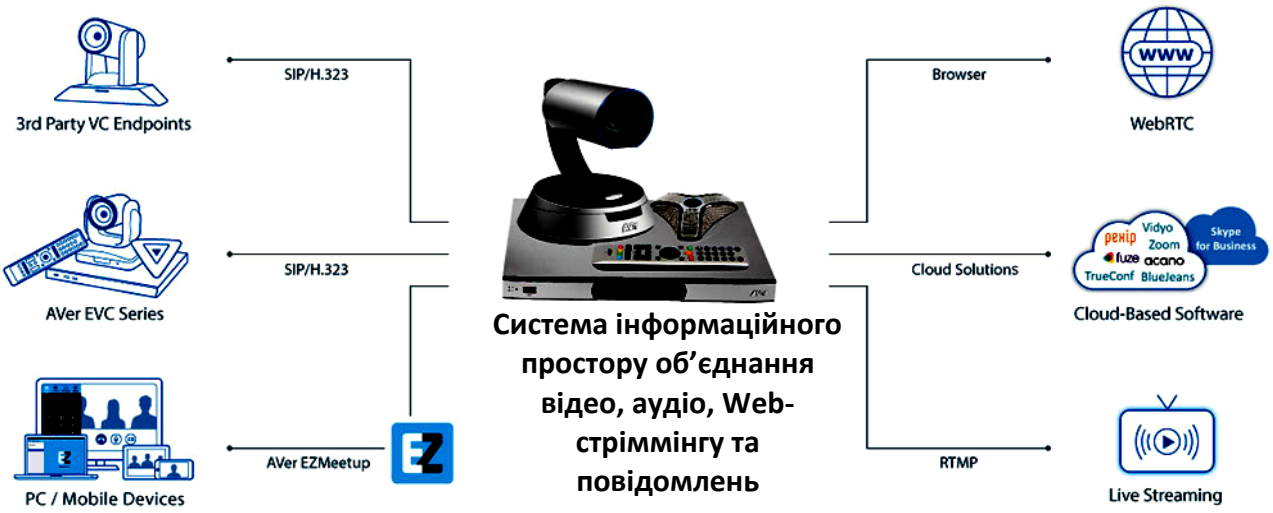


Рисунок 1 – Структурна схема системи

Web Real-Time Communication (WebRTC)

Система інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень забезпечує комунікацію в реальному часі через веб-браузери (Chrome або Firefox) за допомогою технології WebRTC. Підключайтеся до веб-платформи відеоконференцій WebRTC і відразу ж починайте спілкуватися. За допомогою WebRTC ви зможете легко обмінюватися слайдами зі своєї системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень або настроїти службу онлайн-підтримки клієнтів без використання дорогих сторонніх послуг. Потрібне відновлення служби

Підтримувати дисплей подвійної камери / Подвійні презентації

Із системою ви одержуєте можливість вибору. Тепер ви можете вибрати зображення з 1-й камери, з 2-й камери, або з обох камер. Також система інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень може приймати вхідний сигнал з різних джерел і в режимі презентацій. На блоці кодеку можна вибрати кожної із двох джерел вхідного сигналу – вхід HDMI або DVI/VGA, або ж обидва входи одночасно. Таким чином, система інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень здатна забезпечити неперевершені зручності при проведенні відеоконференцій!

Потокова передача RTMP для трансляції відео

Система інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень оснащена функцією потокової передачі. Виконавши нескладні налаштування, ви відразу зможете виконати потокову трансляцію своєї відеоконференції, презентації, виступу, лекції й т.д. Крім того, у системі також передбачена життєво важлива функція запису, що реалізується всього одним клацанням миші.

Убудоване сховище даних обсягом 32 ГБ

Вам більше не буде потрібно підключати USB-дисковід для запису ходу нарад – система інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень оснащена внутрішнім сховищем даних обсягом 32 ГБ. На додаток до всього, підтримка протоколу ISCSI забезпечить завантаження ваших даних у середовище хмарних обчислень. Ви більше ніколи не пропустите жодного події.

Можливість розширення ліцензії до 16 точок підключення

Користувачі системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень можуть скористатися нашою програмою розширення ліцензії, у яку можна включити до 16 точок підключення. Таким чином, ви зможете легко розширити куплену систему для задоволення зростаючих потреб своєї компанії в області комунікацій.

Нижче приведемо характеристики системи інформаційного простору об'єднання відео, аудіо, Web-стріммінгу та повідомлень.

1. Зв'язок

– Стандарти H.323, SIP, SIP TLS.
– Microsoft Lync 2013, Skype for Business 2015.
– WebRTC (Потрібна ліцензія).
– Змішане використання різних протоколів: H.323, SIP, Microsoft Lync 2013, Skype for Business 2015, WebRTC.
– Пропускна здатність 64 Кбіт/с ~ 4Мбіт/с.
– Мережний порт RJ45 (LAN 10/100/1000).
– Ручне налаштування пропускної здатності.
– Manual Max. bandwidth settings (up to 12Mb).

2. Камера

– Камера eCam PTZ III.
– 2-мегапіксельна CMOS-матриця.
– 18-кратне загальне збільшення.
– Поворот ±110°; нахил +25°/-25°.
– Зона огляду 72° (Г); 43° (В); 82° (Діагональ).

3. Дозвіл відео при зйомці людей

– HD1080p (1920 x 1080) із частотою до 60 кдр/сек.
– HD720p (1280 x 720).
– 480p (848 x 480).
– 4CIF (704 x 576).
– CIF (352 x 288).
– SIF (352 x 240).
– Всі дозволи зазначені для частоти 30 кдр/сек.

4. Дозвіл відео при передачі контенту

– Підтримувані дозволи із входу HDMI.
– 1080p (1920 x 1080).
– 720p (1280 x 720).
– D1 (720 x 480).
– SXGA (1280 x 1024).
– XGA (1024 x 768).
– SVGA (800 x 600).
– VGA (640 x 480).
– Підтримувані дозволи із входу DVI (цифровий).
– 1080p (1920 x 1080).
– 720p (1280 x 720).
– D1 (720 x 480).
– SXGA (1280 x 1024).
– XGA (1024 x 768).
– SVGA (800 x 600).
– VGA (640 x 480).
– Вихідний дозвіл.
– До HD1080p (1920 x 1080) із частотою до 60 кдр/сек.

5. Стандарти відео

– H.264, H.264 HP, H.264 SVC, H.263+, H.263, H.261.
– Подвійні відеопотоки H.239.
– Обмін контентом за протоколом BFCP.
– Потокова передача RTMP для трансляції відео.

6. Характеристики відео

– 3D-Шумозаглушення.

7. 3D-Шумозаглушення

– Вхід для основної камери eCam PTZ III.
– Вхід HDMI для 2-й камери.
– Вхід DVI-I (VGA) для презентацій.
– Вхід HDMI для презентацій.

8. Відеовиходи

– HDMI x 2.

9. Стандарти аудіо

– G.711, G.722, G.722.1, G.728, G.722.1C, AAC-LD, g.729.

10. Функції аудіо

– Автоматичне керування посиленням (AGC).
– Поліпшене придушення шумів.
– Функція придушення акустичного луна (AEC).

11. Аудіовходи

– Послідовне підключення до 4 мікрофонів системи інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень SVC.
– HDMI.
– Лінійний вхід (3,5 мм).

12. Аудіовиходи

– HDMI.
– Лінійний вихід (3,5 мм).

13. Інші підтримувані стандарти

– H.224, H.225, H.245, H.281, H.323 Annex Q, H.460.
– RTP, RTCP, H.350, SRTP, H.235.

14. Інтерфейс користувача

– Одиночне/подвійне (з поділом) компонування екрана.
– Зручне екранне меню.
– Показ/редагування ім'я ділянки з'єднання.

15. Мережа

– 10/100/1000 Мб/сек.
– Перетворення мережних адрес (NAT) /обхід брандмауера (H.460).
– Функція відновлення загублених пакетів даних (HELPeR™).
– Підтримка API через Telnet.
– Підтримка функції віддаленого включення системи інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень (WOL, Wake-on-LAN).
– Підтримка IPv4 і IPv6.
– Перевірка мережі.
– Механізм якості обслуговування (QoS).
– VLAN\802.1Q\802.1P.
– EAP 802.1x.

16. Безпека

– Алгоритм шифрування AES (Advanced Encryption Standard) (128 біт).
– Захист паролем для налаштувань системи інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень.
– Захист паролем для віддаленого керування системою.

17. Веб-інструмент керування

– Дистанційне керування.
– Моніторинг у режимі реального часу.
– Відновлення прошивання.

– Завантаження /вивантаження / редагування телефонної книги.

– Відновлення налаштувань системи інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень.

– Експорт журналу викликів.

18. Функції для додаткової зручності

– Запис конференції.

– Запис у режимі конференції й поза мережею.

– Збереження на USB-накопичувач.

– Підтримка перекомпонування екрана під час відтворення.

– Відтворення й конвертація файлів за допомогою застосунку VCPlayer (формати .mov і .mp4).

– Підтримка відеокодеку H.264.

– Прийнятий дозвіл до Full HD 1080p при 30 кдр/сек.

– Переданий дозвіл до Full HD 1080p при 30 кдр/сек.

– Функції обміну контентом, захвата й запису.

– Імпорт файлів .JPG, .PNG, .GIF і .BMP.

– Експорт файлів PNG.

– Можливе підключення до 10 пристроїв.

– Підтримка режиму подвійного екрана.

– Швидкий набір за допомогою клавіш швидкого доступу (10 наборів).

– Передвстановки камери (100 позицій).

– Відновлення прошивання через Ethernet або флеш-накопичувач USB.

– Заставка екрана й режим автоматичного відключення живлення.

– Протокол мережного часу (NTP).

– Моментальний знімок.

– Груповий виклик.

– Підтримка голосових викликів SIP-Телефонії.

– Подвійна камера й зображення із двома контентом Side-by-Side або Picture-in-Picture.

– Налаштування запам'ятовувального пристрою iSCSI.

– Вбудований SIP-сервер.

– Режим високого дозволу.

– Підтримка сервера реєстрації (ARS).

– Метод ідентифікації зустрічі.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень; Досліджена система інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень; На основі отриманих результатів досліджень створена програмна реалізація системи інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень. Розроблені під час виконання магістерської роботи алгоритми дозволяють успішно вирішувати завдання інформаційного простору об’єднання відео, аудіо, Web-стріммінгу та повідомлень. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
2. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
3. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
4. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
5. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19
6. Дреев А.Н. SPIHT кодирование с отложенной передачей значимых битов / А.Н. Дреев // Тези доповідей. Новітні технології – для захисту повітряного простору. Дев'ята наукова конференція 17 квітня 2013 р. – Х.: ХУПС. – 2013. – С. 206
7. Дреев А.Н. Повышение оперативности доставки данных повышенной востребованности в телекоммуникационных системах и сетях / А.Н. Дреев, А.А. Смирнов, Е.В. Мелешко // Проблеми і перспективи розвитку ІТ-індустрії 25-26 квітня 2013 р. Системи обробки інформації. – Випуск 3 (110). Том 2. – Харків: ХУПС. – 2013. С. – 199.
8. Дрєєв О.М. Середньостатистичний та найімовірніший час доставки багатопакетного повідомлення в телекомунікаційній системі або мережі / О.М. Дрєєв, О.А. Смірнов // V Всеукраїнська науково-практична конференція "Інформатика та системні науки" ІСН – 2014, 13-15 березня 2014 року, м. Полтава – С. 92
9. Дрєєв О.М. Визначення оптимального розміру блоку при бітовому арифметичному кодуванні / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 11-12 квітня 2014 р. – Кіровоград – С. 44
10. Дреев А.Н. Экстраполяция квазипериодических процессов с аддитивными помехами / А.Н. Дреев, А.А. Смирнов // П'ята Міжнародна науково-практична конференція "Інформаційні технології та моделювання в економіці" 15-16 травня 2014 р. – Черкаси – С. 59

УДК 621.793.724

В. Тук, група АТ-19
С. Маркович, доц., канд. техн. наук
Центральноукраїнський національний технічний університет

ВПЛИВ ПІДГОТОВКИ ОСНОВИ НА МІЦНІСТЬ ЗЧЕПЛЕННЯ ЕЛЕКТРОДУГОВИХ ПОКРИТТІВ ПРИ ВІДНОВЛЕННІ ГАЛЬМІВНИХ БАРАБАНІВ

Постановка проблеми. Відновлення деталей машин є важливою задачею сучасного ремонтного виробництва. Особливо це актуально для групи гальмівних барабанів транспортних засобів з підвищеною вантажопідйомністю. Це обумовлено значною металоємністю, матеріалом деталі та величиною зносу котрий сягає кількох міліметрів. Відновлення внутрішньої поверхні деталі до номінального розміру вимагає нанесення значного шару покриття. Технологічні методи відновлення деталей машин, виготовлених з чавуну, на відміну від сталевих деталей, характеризуються підвищеною трудомісткістю, складністю через специфічні фізико-механічні властивості чавуну і його малою пристосованістю до різних процесів нарощування шарів [1, 2]. Тому розробка оптимальної

технології відновлення даного типу деталей є актуальною задачею.

Аналіз останніх досліджень і публікацій. Розглянувши існуючі способи нанесення покриттів значної товщини з придатністю до механічної обробки та забезпеченням високої продуктивності відновлення встановлено, що спосіб електродугового напилення є єдиним прийнятним методом відновлення важконавантажених гальмівних барабанів транспортних засобів підвищеної вантажопідйомності [3]. Разом з тим покриття, нанесені методом електродугового напилення, характеризуються низьким рівнем зчеплення з основою, що є важливою механічною характеристикою для відновлюваної деталі [3,4,5].

Постановка завдання. Розробити технологічні методи підготовки внутрішньої поверхні чавунної деталі для нанесення електродугових покриттів з адгезією, що відповідає специфічним умовам роботи вузла.

Виклад основного матеріалу. Міцність зчеплення покриття з поверхнею основи (адгезія) є одним із основних показників, який визначає його експлуатаційні характеристики. Для визначення адгезійної міцності при відновленні деталей електродуговим напиленням не існує єдиної методики проведення досліджень, що затруднює проведення порівняльного аналізу. Серед методів визначення адгезії покриттів найуживанішими є штифтовий та шляхом склеювання. Недоліком склеювання є те, що найкращі клеї мають міцність на відрив того ж порядку, що і міцність зчеплення високоякісних електродугових покриттів. Тому в роботі застосовувався штифтовий метод визначення адгезії [5]. Для його реалізації виготовлялись спеціальні зразки (рис. 1), які складаються із оправки 1, штифта 2, закріпленого гвинтом 4. Суть методики полягає в визначенні відриву торця конічного штіфта від напиленого покриття і послідуючого розрахунку міцності зчеплення. Дослідження проводили з застосуванням розривної машини ИР-М-авто (рис. 2) При виготовленні зразків враховувались рекомендації [6], що вимагають використовувати для виготовлення штифта та шайби один і той же матеріал з однаковою структурою, точність виготовлення не нижче 12-го квалітету, допуск діаметра конуса в будь якій точці перетину шайби і штифта відповідно H7 і h7. Для визначення адгезії покриттів використали конічні штифти діаметром 3,0 мм. Кількість зразків для випробування однієї серії вимірювань складала 5 штук. Виміри діаметру штіфтів проводились з точністю 0,01 мм. Штіфт притирався до отвору за допомогою алмазної пасти до стану при якому він щільно входить в отвір. При підготовці до обробки штифт щільно вставлявся в отвір до повного контакту з'єднуваних поверхонь, однак під дією власної ваги шайба повинна вільно спадати з штіфта. Перед обробкою штифт фіксується гвинтом, що відгвинчується перед випробуванням на розрив. Після попередньої обробки зразок розбирали, промивали і повторно збирали, зафіксувавши його гвинтом 4. Підготовлені зразки розташовували у касеті, виконаній у фланцевому варіанті. Хвостовик фланця закріпляли в обертовому механізмі.

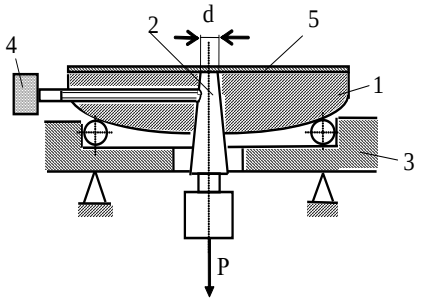


Рисунок 1. Пристрій для визначення адгезії покриття до підкладки за штифтовою методикою: 1 – оправка; 2 – штифт; 3 – основа пристрою для розтягування; 4 – гвинт; 5 – покриття.

Рисунок 1. Розривна машина ИР-М-авто

Досліджували слідуючі технологічні методи підготовки поверхні основи: 1 – дробоструменева обробка електрокорундом нормальним 15А (ГОСТ 2МТ-715-84) , 2 – дробоструменева обробка чавунним колотим дробом ДЧК 1,4 (ГОСТ 11964-81Е), 3 – нарізання «рваної» різьби, 4 - нарізання «рваної» різьби з дробоструменевою обробкою

чавунним колотим дробом ДЧК з добавкою 30% електрокорунду нормального. Режими струменевої обробки: тиск повітря 0,6 МПа, оберти вала 10 об/хв., дистанція 120-150 мм., кут нахилу дробоструменевого пістолета 75 - 90°.

Нарізання «рваної» різьби здійснювалось на токарному верстаті ФТ-11Д твердосплавним різцем Т5К10, розташованого нижче лінії центрів деталі та оснащеного підпружиненою державкою,

Для нанесення покриття використовувався порошковий дріт слідуючого складу, % мас.: Cr - 4,2; C - 0,48; Al – 2; Mo – 1; Si – 2; Mn – 1,5, що формує покриття з мартенситним типом зміцнення та забезпечує підвищення адгезивної міцності через протікання екзотермічних алюмотермічних реакцій та виділенням великої кількості тепла розплавом Mo на поверхні сталевої підкладки [7].

Товщина покриття на зразках для визначення адгезії становила 300 мкм. Для одержання достовірних результатів з визначення адгезії на кожен тип попередньої підготовки поверхні наносили покриття за однакового режиму напилювання.

Додатково в склад наповнювача дослідних зразків порошкових дротів вводили добавки з`єднань легкоіонізуючих елементів і галогенідів лужних і лужно - земельних металів згідно [8].

Порошкові дроти виготовляли згідно розроблених нами методик [9].

Покриття наносили з застосуванням головки для нанесення зносостійких електродугових покриттів на внутрішні поверхні деталей сільськогосподарської техніки [10] на зразки із чавуну на наступних режимах: напруга U=32В, сила струму I=180-200 А, тиск розпилюючого повітря Р = 0,6 МПа., відстань від сопла розпилювача до деталі L=150 мм.

Відхилення товщин покритя, що напилювалось на шайбу не перевищували 0,01 мм.

Кожне значення виміру усереднювалось не менше ніж по трьом зразкам. При проведенні випробування фіксувались значення P1 - загальне зусилля, що необхідне для відриву штіфта, Р5 - сила тертя між штіфтом та стінками шайби. Для визначення Р2 штіфт, після визначення Р1 знову вставляли в отвір шайби і повторювали випробування зразка по аналогічній схемі навантаження. Для того щоб врахувати дію на кінець штіфта попередньої обробки основи, яка викликає його розклепування, внаслідок чого виникають додаткові сили що утруднюють відрив його вад шайби, вводилась поправка Р6. Для її визначення брали партію пристосувань аналогічної схеми, але без покриття і визначали Р4 - зусилля, що необхідне для відриву штіфта. Потім штіфт знову вставляли в отвір і визначали силу тертя Р5. Поправку Р6 визначали по формулі:

$$P_6 = P_4 - P_5$$

Значення підставляли в формулу

$$P = \frac{P_1 - P_2 - P_6}{\pi}$$

Крім того проводився огляд торця штіфта після відриву його від покриття. Якщо на більш ніж на 10 % поверхні залишалось невідділене покриття то результат не враховувався. Реєстрація зусилля проводилась з похибкою менше ніж 0,5 %.

Результати випробувань відображено в діаграмі (рис.3)

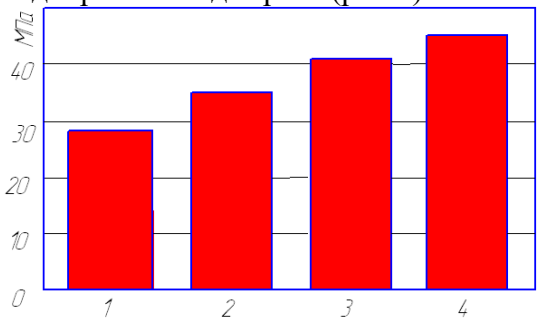


Рисунок 3. Діаграма значень адгезії електродугового покриття в залежності від типу попередньої обробки

Використання для попередньої обробки основи струменевої обробки електрокорундом забезпечує адгезію на рівні 28 МПа за рахунок активації поверхневої енергії деталі. Застосування дробоструменевої обробки підвищує адгезію до 35 МПа за рахунок підвищення шорсткості поверхоні та збільшення сили механічного зчеплення розплавлених часток з основою. Застосування методу нарізання «рваної» різьби з послідуючою дробоструменевою обробкою підвищує адгезію до 45 МПа, застосувавши таким чином обидва фактори впливу.

Висновок.

Оптимальним технологічним методом підготовки внутрішньої поверхні гальмівних барабанів є нарізання «рваної» різьби з послідуючою дробоструменевою обробкою чавунним колотим дротом ДЧК-1,4 з добавкою 30% електрокорунду нормального, що підвищує адгезію до 45 МПа, не знижуючи при цьому механічних характеристик деталі.

Список літератури

1. Черноиванов В.И. Восстановление деталей машин. - М.: ГОСНИТИ, 1995.-278 с
2. Воловик Е.Л. Справочник по восстановлению деталей. - М.: Колос, 1981.-351 с.
3. Багатофункціональні електродугові покриття : монографія / М. М. Студент, Г. В. Похмурська, В. М. Гвоздецький [та ін.]. - Львів : Простір-М, 2018. - 335 с.
4. Студент М. М., Абразивна зносостійкість та трибологічні характеристики електрометалізаційних композиційних покриттів/ М. М. Студент, С. І. Маркович, В. М. Гвоздецький [та ін.] // Фізико-хімічна механіка матеріалів. – 2022. – № 1, - С. 90-97
5. Маркович С.І . Дослідження звязку зносостійкості з фізико-механічними властивостями покриттів, нанесених електродуговим напиленням різнорідних дротів. // Проблеми тертя та зношування.–Київ, 2007 с. 16-18
6. Тушинский Л.И., Плохов А. В. Исследование структуры и физико - химических свойств покрытий - Новосибирск. : Наука, 1986.- 200 с.
7. Мажейка. О.Й. Методологія формування та трибологічні характеристики електродугових покриттів при зміцненні внутрішніх поверхонь./ Мажейка О.Й., Маркович С.І., Рябоволик Ю.В. // Проблеми тертя та зношування, 2010. с. 154-162
8. Маркович С.І. Оптимізація складу додатків в шихту порошкових дротів для електродугового напилення зносостійких покриттів //Зб. наукових праць Кіровоградського технічного університету „Техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація". Кіровоград – 2007. №18. С. 158- 164.
9. Черновол М.І. Дослідження впливу вмісту легуючих елементів в шихті порошкового дроту на придатність до обробки електродугових покриттів / Черновол М.І., Мажейка О.Й., Маркович С.І. //Конструювання, виробництво та експлуатація сільськогосподарських машин № 41(2). , 2011 с. 20-26
10. Мажейка. О.Й. Конструкція головки для нанесення зносостійких електродугових покриттів на внутрішні поверхні деталей сільськогосподарської техніки. / Мажейка. О.Й., Маркович С.І., Рябоволик Ю.В. // Конструювання, виробництво та експлуатація сільськогосподарських машин, №39 с. 433-441

УДК. 621.791.011

А. Демченко, група АТ-19
С. Маркович, доц., канд. техн. наук
Центральноукраїнський національний технічний університет

ТЕХНОЛОГІЧНІ ОСОБЛИВОСТІ ВІДНОВЛЕННЯ НАПІВВІСЕЙ АВТОМОБІЛІВ ЕЛЕКТРОКОНТАКТНИМ НАВАРЮВАННЯМ

Постановка проблеми. В процесі експлуатації автомобіля напіввісь слугує для передачі перетвореного редуктором крутного моменту безпосередньо на колесо автомобіля. При цьому вона сприймає на себе безліч різних навантажень, це і моменти, що вигинають, від вертикальної реакції на дію сили тяжіння, що доводиться на колесо, і дотична реакція, яка обумовлена тяговою і гальмівною силами, і від бічної сили, що виникає при занесенні автомобіля, а також бічні навантаження під дією бічного вітру. Найбільші навантаження піввісь випробовує при русі по ґрунтових дорогах і по шосе з твердим покриттям що має поганий стан [1, 2].

Зазначені навантаження викликають прискорене спрацювання посадочних місць під підшипники кочення. Тому розробка оптимальної технології відновлення даної деталі є актуальною задачею.

Аналіз останніх досліджень і публікацій. Економічно доцільно відновлювати до 40% деталей, 30% деталей використовувати повторно без ремонтних дій і 30% деталей необхідно замінювати новими. Фактично в даний час відновлюється від 12 до 15% деталей, а використовуються повторно без ремонтних дій більше 50% деталей [1,2].

Найбільш поширеними способами відновлення зовнішніх циліндрових поверхонь є напилення, наплавлення металів (у середовищі вуглекислого газу, під флюсом, вібродугова, плазмова) і електролітичне залізнення та хромування. Застосування даних методів для відновлення напіввісей викликає певні складнощі: напилені поверхні не сприймають знакозмінні навантаження та знижують втомну міцність деталі, наплавлення створює термічні перетворення та значні напруження, котрі можуть привести до руйнування деталі, застосування гальванічних покриттів недоцільне через значну товщину покриття [1, 2, 3, 4].

Однією з перспективних і ефективних технологій відновлення деталей є електроконтактне наварювання (ЕКН) металевого шару (стрічки, дроту, порошкових матеріалів) [5,6,7].

Позитивними властивостями ЕКН є: малий нагрів деталі, відсутність вигорання легуючих елементів, мінімальний припуск на подальшу механічну обробку наплавленого металу, можливість наплавлення сталевої стрічки, дроту і металевих порошків, зменшення витрати металу (в порівнянні з вібродуговим наплавленням) в 2,4 разу, сприятливі санітарні умови роботи оператора [8,9].

Разом з тим шар навареного металу після ЕКН характеризується наявністю зон відпуску в місцях перекриття валиків, що приводить до наявності структурної неоднорідності [10], небажаної при експлуатації деталей машин з поверхнями кочення. Крім того зазначені процеси викликають зниження втомної міцності. Це утрудняє використання ЕКН для відновлення поверхонь кочення.

Постановка завдання. Розробити оптимальні технологічні параметри відновлення напіввісей та експериментально визначити рівень зниження втомної міцності.

Виклад основного матеріалу. Для здійснення застосовувалась одно точкова технологічна схема з застосуванням установки ЕКП 011-1-02Н-Ремдеталь. Відновлення шийок здійснювалось з застосуванням дроту Св 65Г.

Розрахунок електротеплової обстановки в зоні наварювання одиничного контактного майданчика проводився методом кінцевих елементом із застосуванням математичного процесора Math Cad. Передбачувані розміри зон термічного впливу на картині розрахованого температурного поля визначалися по місцю розташування ізотерм початку аустенітного перетворення при нагріві (ТАсз) і початку мартенситного перетворення при відпуску (Тмн)

На основі даних проведених досліджень були складені рекомендації по вибору режимів, що забезпечують зменшення ширини зон відпуску на поверхні шару навареного металу, основними чинниками впливу на глибину гарту поверхневого шару після ЕКН є сила і тривалість імпульсу струму, а на ширину зон відпуску і ступінь роззміцнення в цих зонах - швидкість наварювання, тривалість пауз і витрата охолоджуючої рідини.

Попередні експерименти показали, що для присадного дроту діаметром 1,6 - 1,8 мм розбризкування відсутнє при зусиллі стиснення, рівному 1,5 кН і вище. Звідси, зусилля стиснення електродів слід приймати рівним 1,5 кН.

Ширина робочої поверхні електроду знаходиться в діапазоні значень до 7 мм.

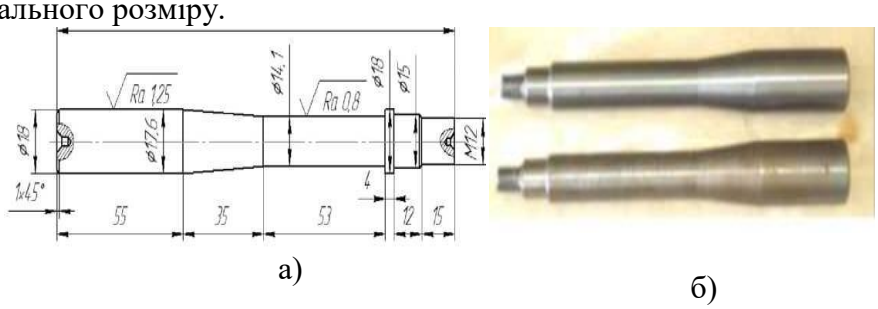
Найбільш значущими чинниками впливу на глибину зони гарту є сила і тривалість імпульсу струму. Значення струму наварювання I і тривалість імпульсу струму t_i приймалася відповідною максимально допустимому ступеню осідання дроту під центром електроду 70,9 % : I= 6,7 кА, t_i = 0,08 с. Твердість коливається в межах від 47 до 63 HRC.

Відповідно до отриманих експериментальних залежностей були вибрані наступні параметри режиму наварювання: струм наварювання I = 6,7 кА, тривалість паузи tn = 0,24 с, тривалість імпульсу = 0,08 с, тривалість наростання імпульсу (модуляції) - $t_{мод}$ = 0,06 с, перекіс фаз - позиція перемикача “5”, швидкість наварювання V = 3 мм/с, витрата води Qe, що охолоджує = 0,00006 м^3/с, радіус електрода R = 150 мм, зусилля притиснення електроду P = 1,5 кН.

Випробування на зносостійкість на машині СМЦ-2 по схемі «диск-колодка» показали підвищення зносостійкості близько 22%.

Для визначення рівня зниження втомної міцності проведені експериментальні дослідження на машині вигину і кручення марки У20, за умовами, описаними в ГОСТ 2860-65. Загальний вид машини для випробувань показаний на рис 1. Випробування проводили на зразках (рис.2 а) б), виготовлені сталі 45 ГОСТ 1050-88, на яких приварювали вибрані присадні матеріали. Контактне приварювання здійснювали на установці 011-01-02Н «Ремдеталь» за один прохід на режимах приварювання, які забезпечують якнайкращу міцність зчеплення присадного матеріалу. Після ЕКН проводили механічну обробку заготовок на універсальному круглошліфувальному верстаті марки 3М151 до отримання відповідної шорсткості і номінального розміру.

Рисунок 1 - Установка для втомних випробувань циліндрових зразків типу «вал» У-20



а) б)

Рисунок 2 - Ескіз зразка (а) і загальний вигляд (б) для втомних випробувань

Порівняння наварених заготовок проводилося із зразками, виготовленими із сталі 45 ГОСТ 1050-88 і загартованими до твердості HRC48..50. Випробування заготовок

проводилося вантаженням по симетричній схемі вигину двох заготовок з постійним обертанням на машині У20. При цьому розрахункова внутрішня напруга визначалася по формулі:

$$\sigma_{\text{а}} = \frac{M_{з}}{W_0} = \frac{32FL}{\pi d^3},$$

де: $M_з = FL$ - момент згину в небезпечному перетині, Н-м; $W_o = \pi d^3/32$ - момент осьовий опору розрахункового перетину, м ; F - навантаження, прикладене до заготівки, Н; L - плече (відстань від небезпечного перетину зразка до точки додатку навантаження), м; d - діаметр заготівки, м.

Проведені дослідження показали зниження втомної міцності зразка з ЕКН в порівнянні з контрольним зразком до 6%, що є допустимим в умовах ремонтного виробництва.

Висновок. Розроблено технологію відновлення напіввісей автомобілів з застосуванням ЕКН з оптимальними параметрами режиму, що склали струм наварювання I = 6,7 кА, тривалість паузи tn = 0,24 с, тривалість імпульсу = 0,08 с, тривалість наростання імпульсу (модуляції) - $t_{мод}$ = 0,06 с, перекіс фаз - позиція перемикача “5”, швидкість наварювання V = 3 мм/с, витрата води Qe, що охолоджує = 0,00006 м^3/с, радіус електрода R = 150 мм, зусилля притиснення електроду P = 1,5 кН. Зносостійкість деталі з покриттям збільшилась на близько 22% при цьому втомна міцність знизилась на 6%.

Список літератури

1. Черноиванов В.И. Восстановление деталей машин. - М.: ГОСНИТИ, 1995.-278 с
2. Воловик Е.Л. Справочник по восстановлению деталей. - М.: Колос, 1981.-351 с.
3. Багатофункціональні електродугові покриття : монографія / М. М. Студент, Г. В. Похмурська, В. М. Гвоздецький [та ін.]. - Львів : Простір-М, 2018. - 335 с.
4. Студент М. М., Абразивна зносостійкість та трибологічні характеристики електрометалізаційних композиційних покриттів/ М. М. Студент, С. І. Маркович, В. М. Гвоздецький [та ін.] // Фізико-хімічна механіка матеріалів. – 2022. – № 1, - С. 90-97
5. Каракозов Э.С. Соединение металлов в твердой фазе. М.: Металлургия, 1976. 264 с.
6. Клименко Ю.В. Электроконтактная наплавка. М.: Металлургия, 1978. 128 с.
7. Каракозов Э.С., Латыпов Р.А., Молчанов Б.А. Состояние и перспективы восстановления деталей электроконтактной приваркой материалов.М.: Информагротех, 1991. 85 с.
8. Булычев В.В., Латыпов Р.А. Особенности пластической деформации при получении покрытий электроконтактной приваркой // Международный научный журнал. 2010.№5. С.78 – 85.
9. Кочергин К.А. Контактная сварка. Л.: Машиностроение, 1987. 240 с.
10. Булычев В.В., Латыпов Р.А. К вопросу о формировании соединения при электроконтактной приварке // Международный технико-экономический журнал. 2010.№5. С.59-65.

УДК 004

Р. Перекос, магістр гр. КІ-20М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ КЕРУВАННЯ ІНФРАСТРУКТУРОЮ ЦОД НА ОСНОВІ ТЕХНОЛОГІЇ UNIFIED COMPUTING SYSTEM

У статті розроблено програмне забезпечення, яке призначено для системи керування інфраструктурою ЦОД на основі технології Unified Computing System. Метою розробки є дослідження та програмна реалізація системи керування інфраструктурою ЦОД на основі технології Unified Computing System.Об'єктом дослідження є процес керування інфраструктурою ЦОД на основі технології Unified Computing System. Предметом дослідження є методи керування інфраструктурою ЦОД на основі технології Unified Computing System. Методи дослідження базуються на методах теорії телекомунікацій, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи керування інфраструктурою ЦОД на основі технології Unified Computing System. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп'ютерна інженерія, ЦОД, Unified Computing System

Постановка проблеми. В умовах, що швидко міняються потреби бізнесу вимагають швидкого реагування, зверніть увагу на систему уніфікованих обчислень Cisco Unified Computing System (UCS). Cisco UCS – це перша в галузі конвергентна платформа для створення центрів обробки даних, що надає інтелектуальну, програмуєму інфраструктуру, що спрощує й прискорює розгортання застосунків і сервісів корпоративного класу в традиційних, віртуалізованих і хмарних обчислювальних середовищах.

Ця платформа для центрів обробки даних наступного покоління поєднує уніфіковане керування на основі моделі, наскрізне виділення ресурсів і підтримку міграції для прискорення й спрощення розгортання застосунків, підвищуючи рівень надійності й безпеки.

Система Cisco Unified Computing System:

- поєднує сервери Cisco, мережні ресурси й ресурси вводу-виводу в одну систему;
- підвищує доступність і продуктивність корпоративних застосунків;
- масштабує надання сервісів для забезпечення більше оперативної діяльності;
- оптимізує ресурси центра обробки даних для зниження сукупної вартості володіння;
- значно знижує кількість пристроїв, що вимагають налаштування, керування, енергопостачання, охолодження й прокладки кабелів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування інфраструктурою ЦОД на основі технології Unified Computing System.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи керування інфраструктурою ЦОД на основі технології Unified Computing System.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем керування інфраструктурою ЦОД на основі технології Unified Computing System.

– Дослідження системи керування інфраструктурою ЦОД на основі технології Unified Computing System.

– Програмна реалізація системи керування інфраструктурою ЦОД на основі технології Unified Computing System.

Об'єктом дослідження є процес керування інфраструктурою ЦОД на основі технології Unified Computing System.

Предметом дослідження є методи керування інфраструктурою ЦОД на основі технології Unified Computing System.

Методи дослідження базуються на методах теорії телекомунікацій, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Лінійка устаткування Cisco UCS – це платформа, що поєднує в єдину систему обчислювальні й мережні ресурси, доступ до систем зберігання даних, а також засобу віртуалізації. Поява цього продукту пов'язане з необхідністю рішення таких завдань як ріст складності бізнес-застосунків, забезпечення безперервності бізнес-процесів, їхнє відновлення в аварійних ситуаціях, економія електроенергії й площ центрів обробки даних.

Такі завдання можуть бути вирішені за допомогою віртуалізації ЦОД, використання віртуальних машин. Однак при цьому виникають інші складності: проблеми безпеки, обмежені можливості керування, обмеження систем вводу-виводу й безліч інших проблем, з якими зіштовхуються центри даних минулого покоління. Спільний вплив цих факторів створює серйозні бар'єри на шляху до збільшення гнучкості й прискоренню впровадження застосунків, реалізації всього потенціалу віртуалізованих ЦОД.

Компанія Cisco має багаторічний досвід розробок продуктів для ЦОД. Ці розробки містять у собі мережі передачі й зберігання даних, системи балансування й оптимізації трафіку, рішення інформаційної безпеки, передові технології й нові протоколи. Виробник співробітничає з лідерами індустрії ЦОД, такими як Intel, VMware, EMC і BMC, що дозволяє йому пропонувати замовникам цілісну єдину уніфіковану систему Cisco Unified Computing System, що здатна забезпечити рішення перерахованих вище проблем. Cisco розробила дві лінійки серверного устаткування UCS – B-серії (блейд-сервери) і C-серії (стійкові сервери).

Блейд-сервери (B-серія)

Сервери цього типу відрізняються простим і продуманим дизайном системи, використовують можливості консолідації вводу-виводу (unified fabric) на базі технологій Data Center Bridging і Fibre Channel over Ethernet (FCoE). Дані технології дозволяють значно зменшити кількість компонентів і відповідно знизити витрати на елементи мережної інфраструктури (безліч мережних адаптерів, комутатори LAN, SAN, різні мережні кабелі й т.п.), що в остаточному підсумку знижує витрати на електроживлення й охолодження.

Один адміністратор може управляти всіма компонентами системи, що включає до 40 шасі, за допомогою програми UCS Manager. Програмне забезпечення Cisco UCS Manager реалізує концепцію керування на базі ролей і політик з використанням сервісних профілів і шаблонів. Інформація про параметри системи електроживлення, охолодження, а також про стан устаткування, конфігурації мережного середовища й мережі зберігання даних утримується в сервісному профілі. Реалізація технології Stateless Computing, або перенос сервісних профілів, дозволяє мінімізувати час обслуговування системи й легко адаптувати її під швидко мінливі вимоги.

Технологія розширення пам'яті дає можливість задіяти в окремому сервері 48 слотів для установки модулів пам'яті DIMM і одержати до 384 Гбайт оперативної пам'яті у двопроцесорній системі на максимальній частоті 1333 Мгц, створивши тим самим відмінну базу для віртуальних застосунків.

Віртуалізований мережний адаптер Cisco має виняткові характеристики – з його допомогою можна створити до 58 віртуальних адаптерів і здійснювати підтримку режиму Hypervisor Bypass. Підтримка технології VN-Link розширює границю мережі до віртуальної машини й стирає розходження в керуванні мережною інфраструктурою для фізичних і

віртуальних серверів. Всі мережні з'єднання налаштуються й управляються централізовано, без виділення додаткового рівня комутації для віртуальних середовищ. Конфігурації портів вводу/виводу й мережних політиків переміщаються між віртуальними серверами, що збільшує ефективність і знижує складність їхньої експлуатації.

Архітектура системи Cisco UCS заснована на технології 10 Gigabit Ethernet і широко розповсюдженої архітектури серверів Intel x86 з використанням процесорів серії Intel Xeon 5600, 6500 і 7500. Вся комутація трафіку в блейд-системі здійснюється через єдиний центральний комутатор за допомогою мережних модулів зі стандартними кабельними з'єднаннями SFP+. Далі від мережних модулів трафік передається серверам через адаптери, з'єднані з модулями за допомогою пасивної внутрішньої шини. Таким чином, тут застосовується принцип однократної кроссування. Це дозволяє, зкомутувати кабелі один раз і далі через інтерфейс керування налаштовувати кількість, типи й характеристики адаптерів для мережі передачі даних і мережі зберігання. У випадку зміни типу підключення сервера до мережі немає необхідності в установці додаткових адаптерів і прокладці нових кабелів.

Технологічні можливості лінійки Cisco UCS B-серії дозволяють вирішувати будь-які завдання як у віртуалізованому, так і у звичайному середовищі.

Стійкові сервери (C-серія)

Компанія Cisco пропонує своїм замовникам бюджетний варіант – стійкове виконання UCS. Тут реалізовані багато хто з розробок, характерних для B-серії, включаючи використання програмного забезпечення UCS Manager, технологію розширення пам'яті й архітектуру Intel. Все це дає замовникові можливість поєднувати сервери, мережі, доступ до сховищ і віртуалізацію в єдину інфраструктуру, що забезпечує зниження сукупної вартості володіння й збільшення гнучкості бізнесу. Управляти серверами C-серії можна як централізовано з UCS Manager, так і за допомогою убудованого в сервери інтерфейсу керування (графічного або командного рядка).

Лінійка C-серії охоплює будь-які потреби замовників – починаючи з недорогих серверів у корпусі 1U і закінчуючи потужними чотирипроцесорними серверами. Для серверів UCS сертифіковані багато застосунків Cisco і інших виробників. Зокрема, популярний додаток Unified Communications Manager (Unified CM), починаючи з версії 8.0 (2), за допомогою програмного забезпечення VMware працює на серверах UCS. По продуктивності така система набагато ефективніше й має набагато більші можливості, чим попередні версії.

Система об'єднаних обчислень Cisco Unified Computing System – це платформа для центрів обробки даних наступного покоління, що включає в себе мережні можливості, обчислювальні ресурси й підтримку віртуалізації, а також централізоване керування всіма її елементами. Cisco UCS дозволяє значно знизити витрати на експлуатацію ЦОД і збільшує операційну ефективність бізнесу при характерному для Cisco якості й надійності.

Cisco Unified Computing System Manager

Cisco Unified Computing System Manager забезпечує уніфіковане керування всіма програмними й апаратними компонентами в рамках Cisco UCS. Це рішення управляє безліччю серверних шасі й ресурсами тисяч віртуальних машин.

Cisco Unified Computing Systems (UCS) – це універсальний підхід до побудови обчислювальних систем і хмарної платформи. Рішення на базі UCS дозволяють створювати єдину архітектуру для всього ЦОДу, включаючи обчислювальні серверні ресурси, мережне устаткування для доступу до LAN/SAN-мережі, а також надають кошти повномасштабного контролю й керування серверами у фізичних і віртуальних середовищах, спрощуючи перехід до хмарних обчислень. Інтеграція систем у єдине ефективне середовище дозволяє скоротити вартість послуг DF Cloud, підвищити гнучкість і продуктивність інформаційних систем, забезпечуючи широкі можливості для підвищення ефективності бізнесу в цілому.

Підвищення ефективності роботи

Завдяки застосуванню єдиної, що вбудовується системи на основі політик і дружнього екосистемного підходу, Cisco UCS Manager допомагає скоротити управлінські й адміністративні витрати.

Збільшення гнучкості

Cisco UCS Manager підтримує автоматизацію центрів обробки даних, що допомагає підвищити експлуатаційну гнучкість і масштабованість, одночасно знижуючи ризик. Він забезпечує керування на основі політик із шаблонами сервісу і його профілів. Cisco UCS Manager полегшує навантаження на фізичні й віртуальні сервери в складі Cisco UCS, сприяючи консолідації серверів і гнучкості виконання робочих навантажень блейд-серверами або серверами стійкового виконання.

Поліпшення контролю

Інтеграція Cisco UCS Manager із провідними галузевими рішеннями керування системами підтримує діючі процеси, допомагає реалізувати навички IT-персоналу й інструментарій. Відкритий інтерфейс XML API надає 9000 точок інтеграції для полегшення спеціалізованих розробок і більше високих досягнень у керуванні системами.

Особливості й переваги

– Єдиний убудований інтерфейс керування, що поєднує сервери, мережі й доступ до сховищ.

– Керування на основі політик і моделей, профілів сервісу, здатні поліпшити маневреність і знижують ризик.

– Автовизначення устаткування для обліку й керування системними компонентами, які додаються або заміняються.

– Відкритий XML API що дозволяє полегшити інтеграцію інструментів системного керування сторонніх розроблювачів.

– Адміністрування на основі ролей

Cisco UCS Director

Cisco UCS Director – це програмний продукт, що автоматизує керування різнорідної IT інфраструктурою центра обробки даних. У цьому пості я коротко опишу, для чого цей продукт призначений і які завдання вирішує.

UCS (Unified Computing System) – це серверна платформа компанії Cisco, що базується на лінійках Rack і Blade. Природно, що CISCO позиціонує UCS Director як рішення, що хоч і універсально, але найбільше повно розкриває свої функціональні можливості в комплексі з устаткуванням лінійки UCS. Тому спочатку скажемо пари слів про сервера CISCO UCS.

Сервера Cisco UCS

Особливість серверної платформи Cisco UCS у тім, що в конфігурації є одна блейд-кошик і деякий набір серверів. При цьому немає градації рішень і є внутрішній комутатор – модель 62 серії, Fabric Interconnect.

Традиційний підхід побудови інфраструктури полягає в тому, що в кожну блейд-кошик містяться комутатори типу LAN, SAN або Management. З такого підходу ми одержуємо безліч точок керування й складне кабелювання. Далі все це виноситься в комутатор Top of Rack і в результаті виходить зайве накопичення.

Продукт Cisco UCS Director дозволяє вирішити проблему настільки складної організації інфраструктури. Спочатку даний продукт був виведений на ринок компанією Cloupia, потім після її покупки Cisco був зроблений ребрендинг і зараз цей продукт називається Cisco UCS Director.

Серверне рішення Cisco UCS відрізняється від традиційної схеми побудови інфраструктури тим, що на Fabric Interconnected будується єдиний внутрішній комутатор, що має винесені порти в кожну блейд-корзину. Завдяки цьому ми зменшуємо кількість сполучних ліній між центральними комутаторами й самими лезами. Ми одержуємо більшу масштабованість і легко нарощуємо ресурси.

Пари інтерконнектів може підтримувати до 20 шасі лез. На таких інтерконнектах ставиться System Manager, що саме й взаємодіє з UCS Director, завдяки чому ми можемо управляти пулами серверів і нав'язувати на них політики.

Керування фізичною інфраструктурою й віртуальними середовищами

Як відомо, сучасні вимоги до IT ростуть, потрібно постійно збільшувати оперативність розгортання тої або іншої інфраструктури. Традиційно у великих компаніях є розподіл системних адміністраторів по різних напрямках: адміністрування віртуальної інфраструктури, серверне адміністрування, адміністрування систем зберігання даних або мережної частини.

Ми одержуємо безліч учасників, який необхідно об'єднати між собою й налагодити ефективна їхня взаємодія. Також необхідно організувати ефективне виконання рутинних операцій, таких як прописування vLAN, фізична комутація чого-небудь і т.п. Із усього цього випливає загальна проблема – відсутність ефективного контролю. Через непогодженість у роботі різних фахівців строки впровадження часом виростають від декількох годин до декількох тижнів, а те й місяців. У результаті чого простоюють проекти бізнесу.

У продукті Cisco UCS Director усе зводиться до єдиної точки керування. Він дозволяє нам з єдиної точки управляти всіма чотирма рівнями:

- віртуалізація;
- обчислення;
- системи зберігання даних;
- мережа.

Архітектура Cisco UCS Director

Почнемо з фізичного середовища.

- Сервера: Cisco UCS, HP, IBM, Dell. Від них потрібне наявність менеджменту керування сервером.
- Системи зберігання даних: EMC, VNX, VNX2, NetApp, вся лінійка FAS.
- Мережна частина: комутатори Cisco Nexus v1000, залізні Nexus, ASA і Brocade.

Віртуальне середовище: підтримується Hyper-V, VMware. Також є інтеграція з публічними хмарами.

Все керування базується на ролях. Є три основні ролі:

- Кінцевий користувач, того хто користується панеллю самообслуговування.
- IT адміністратор.
- Оператор, що займається моніторингом і базовими операціями з інфраструктурою

Система є модульної, отже є можливість інтеграції у віртуальну інфраструктуру без вимоги додаткових обчислювальних потужностей.

За допомогою Cisco UCS Director ми одержуємо глобальний моніторинг всіх чотирьох складових: віртуалізація, сервера, мережа й системи зберігання. Все це здійснюється через користувальницький портал. Користувальницький портал надає деякий набір шаблонів, які вже зконфігуровані, і можливість відстеження виконання запитів. Через користувальницький портал можна сформувати запит на створення віртуальної віртуальної машини. Запити можуть вимагати попереднього твердження, а можуть виконуватися повністю автоматично. Їсти можливість створити віртуальну машину максимально швидко, не чекаючи дій з боку технічного фахівця.

Необхідність твердження запиту залежить від пула, у якому запитувана машина буде розташована. Є обчислювальні пули, які контролюються адміністратором, а є пули, з якими користувач взаємодіє прямо, і повідомлення приходить адміністраторові тільки по факті виконання.

Cisco UCS Director це продукт, що управляє всіма чотирма напрямками адміністрування інфраструктури й зводить їх у єдину точку. При цьому відсутня необхідність перемикання між різними системами керування й використання консолі. Cisco UCS Director є готовим коробковим продуктом, його налаштування займає порядку години

або двох залежно від глибини налаштування. Базова функціональність стає доступна буквально за 1 годину розгортання.

Розробка структурної схеми

Cisco Unified Computing System (UCS) – це платформа для ЦОД наступного покоління, що поєднує обчислювальні й мережні ресурси, доступ до систем зберігання даних, а також засобу віртуалізації в єдину систему. Рішення дозволяє значно знизити витрати на експлуатацію ЦОД і збільшує операційну ефективність бізнесу.

Система поєднує в собі універсальну високошвидкісну мережну інфраструктуру (unified fabric) на базі технологій 10-Gigabit Ethernet і широко використовувану x-86 архітектуру серверів компанії Intel. Рішення Cisco UCS дозволяє створити інтегровану й масштабовану платформу, у якій всі елементи рішення управляються централізовано.

Cisco UCS має у своєму составі єдину систему керування, що дозволяє управляти комплексами до 160 фізичних серверів, на кожному з яких можуть функціонувати десятки віртуальних машин, забезпечуючи чудове масштабування ЦОД без збільшення складності керування.

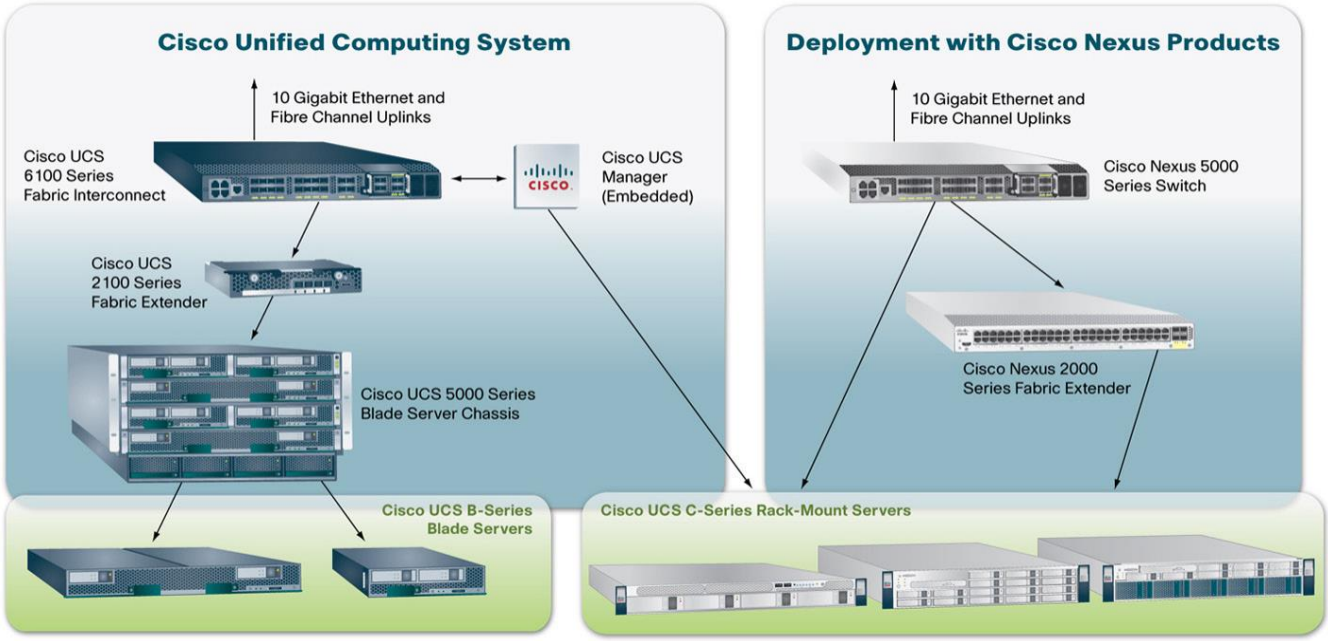


Рисунок 1 – Структурна схема системи

Архітектура системи Cisco UCS поліпшує переносимість профілів фізичних машин, тому що профіль сервера, конфігурація його LAN/SAN з'єднань і I/O, убудованого ПЗ й профілі мережних з'єднань можуть бути динамічно привласнені будь-якому фізичному серверу в системі. Така високодинамічне середовище з підтримкою принципу Stateless Computing можуть бути легко адаптована для задоволення швидко мінливих вимог сучасних центрів обробки даних. Це має на увазі впровадження в потрібний момент необхідних обчислювальних ресурсів і переміщення робочого навантаження.

Cisco Unified Computing System поліпшує доступність, безпеку й продуктивність завдяки інтегрованому дизайну системи.

Компоненти системи UCS:

– Центральні комутатори UCS 6200 Series Fabric.
– Шасі блейд-серверів UCS 5100 Series.
– Мережеві модулі UCS 2200 Series Fabric Extender.
– Блейд-сервери UCS B-Series.
– Стійкові-сервери UCS C-Series.
– Мережні адаптери UCS.
– Модуль керування UCS Manager.

Центральні комутатори UCS серії 6200 Fabric Interconnect

Конвергентні комутатори сполучать функції комутації трафіку Ethernet і Fibre Channel з керуванням системою UCS. Архітектура комутаторів передбачає комутацію трафіку на швидкостях до 10 Гбіт/с без втрат пакетів і із украй низькими затримками. Пристрої поставляються в корпусі 1RU з 48 портами або в корпусі 2RU з 96 портами. Підтримують модулі розширення, що забезпечують підключення Fibre Channel і 10 Gigabit Ethernet.

Основні функції:

– 10 Gigabit Ethernet порти SFP+, підтримка FCoE.

– Варіанти 48 і 96 убудованих портів зі слотами розширення для додавання портів Fibre Channel і 10 GE.

– Убудована система керування UCS Manager.

– До 1.04 Tbps продуктивності.

– Зарезервовані блоки живлення й вентилятори з «гарячою заміною».

– Керування до 40 шасі на систему UCS.

Мережний модуль UCS серії 2200 Fabric Extender

Модулі забезпечують зв'язку між центральними комутаторами й блейд-серверами. З їхньою допомогою спрощуються процеси діагностики, підключення кабелів і керування системою.

Основні функції:

– Підключення блейд-шасі UCS до центральних комутаторів (Fabric Interconnect).

– 8 зовнішніх порту 10 Gigabit Ethernet SFP+ з підтримкою FCoE.

– До двох модулів на шасі для забезпечення відказостійкості й до 80 Гбіт/с повнодуплексної продуктивності.

– Убудоване керування шасі.

– Управляється UCS Manager через центральний комутатор.

Шасі для блейд-серверів UCS серії 5100

Являє собою серверний кошик, що підтримує до восьми блейд-серверів і до двох мережних модулів у корпусі 6RU, не вимагаючи додаткових модулів керування.

Основні функції:

– 4 блоки живлення (резервування за схемою N+1 або N+N).

– 8 вентиляторів (за замовчуванням).

– Охолодження «з попереду назад».

– Висота шасі 6U.

– Усередину можна встановити до 8 блейд-серверів половинної ширини або 4 блейд-сервери повної ширини.

– Всі блейд-сервери одинарної висоти.

– Установка до 2-х мережних модулів.

– Індикаторна ідентифікація.

Блейд-сервери UCS (серія B)

Блейд-сервери UCS – це блейд-сервери архітектури x86 на базі процесорів Intel Xeon, які адаптуються під вимоги застосунків, регулюють використання електроенергії й забезпечують кращу віртуалізацію серед пристроїв свого класу. Унікальна технологія розширення пам'яті Cisco значно збільшує обсяг пам'яті, що підвищує продуктивність і пропускну здатність для ресурсномістких застосунків віртуалізації й обробки великих наборів даних. Крім того, ця технологія пропонує більше економічний варіант пам'яті для менш вимогливих робочих навантажень.

Стійкові сервери UCS (серія C)

Стійкові сервери UCS – сервери, призначені для роботи в автономних середовищах і в складі середовища уніфікованих обчислень Cisco, виконані в стандартному конструктивному виконанні. Вони підтримує модель покрокового розгортання з можливістю майбутнього переходу на уніфіковані обчислення.

Мережні адаптери Cisco UCS

У цей час всі мережні адаптери для блейд-систем умовно можна поділити на три типи: традиційні, конвергентні й віртуалізовані.

– Традиційні адаптери – класичні адаптери з апаратною підтримкою протоколу Ethernet і програмною підтримкою конвергентного протоколу Fibre Channel over Ethernet, призначені для передачі й обміну даними в мережі. Найбільш відомий виробник таких адаптерів – компанія Intel, Broadcom.

– Конвергентні адаптери – адаптери з інтегрованими чипами протоколів 10Gb і Fibre Channel або які мають конвергентний чип протоколу FCoE. На даний момент це найбільш використовуваний тип адаптерів в існуючих серверних системах. Найпоширеніші виробники цих типів – компанії Emulex і Qlogic.

– Віртуалізовані адаптери – адаптери, які дозволяють створити кілька логічних адаптерів як у динаміку (наприклад, при інтеграції із системами віртуалізації), так і статично. Використання віртуалізованого адаптера в середовищі гіпервізора дозволяє перенести завдання комутації трафіку між мережними машинами на мережне устаткування, що дозволяє визволити процесорні ресурси й надати їхнім віртуальним машинам, тим самим підвищити їхня продуктивність у цілому.

Компанія Cisco Systems розробила власний віртуалізований двопортовий конвергентний адаптер Cisco Virtualized Interface Card з винятковими характеристиками, що дозволяє мати перевагу перед іншими виробниками:

– Здатний створити до 58 віртуалізованих Ethernet або FC адаптерів (на одному фізичному адаптері з використанням мітки VNTag проекту стандарту IEEE 802.1Qbh)

– Підтримка стандарту PCIe

– Робота у віртуалізованому і невіртуалізованомуй середовищу

– Підтримка Hypervisor Bypass

– Відказостійкість на апаратному рівні

– Висока продуктивність (2x 10Gb, >600K IOPS)

У стійкових серверах UCS використовуються найбільш затребувані мережні адаптери у вигляді карт PCIe, таких виробників, як QLogic, Broadcom, Emulex і Intel, а також віртуалізований PCIe адаптер Cisco VIC.

Програмний модуль UCS manager

UCS Manager – це убудований програмний модуль, за допомогою якого здійснюється керування всіма компонентами блейд-системи. Інтерфейс UCS Manager розділений на п'ять зон: адміністрування, устаткування, сервери, ЛВС і мережа зберігання. Під адмініструванням маються на увазі операції, вироблені за допомогою UCS Manager. Устаткування – це, як правило, задіяна в цей момент фізична основа UCS. Серверами в загальному випадку йменуються логічні сервери, створені й використовувані за допомогою UCS Manager. У зону ЛВС включається все, що ставиться до локальних мереж, а в зону мережі зберігання – усе, що стосується ресурсів зберігання.

Переваги Unified Computing System (UCS)

– **Убудоване керування системою**. Кожний з компонентів об'єднаної системи обчислень Cisco UCS поставляється з убудованим мікропрограмним забезпеченням, що дозволяє управляти роботою пристрою за допомогою Cisco UCS Manager. Адміністратори мережі, системи зберігання даних і серверів можуть працювати із графічним користувальницьким інтерфейсом або інтерфейсом командного рядка системи Cisco UCS Manager або, використовуючи документований набір функцій XML API, з існуючої корпоративної системи керування ЦОД. Рольова модель контролю спрощує рішення завдань керування, до яких повинні залучатися групи адміністраторів серверів, мережі й системи зберігання даних, дозволяючи обмежити область поширення спеціальної інформації рамками кожної групи. Це дозволять експертам по конкретних питаннях випливати звичайним робочим процедурам і інтегрувати всі дані про конфігурацію в рамках єдиної системи керування, а не в розрізнених системах, як це нерідко відбувається в сучасних ЦОД.

– **Впровадження застосунків з використанням сервісних профілів**. ПЗ UCS Manager реалізує концепцію керування на базі ролей і політик з використанням сервісних профілів і шаблонів. Інформація про параметри системи електроживлення, охолодження, фізичної безпеки, а також про стан устаткування, конфігурації мережного середовища й мережі зберігання даних утримується в сервісному профілі. Використання сервісних профілів дозволяє IT-персоналу ЦОД знизити час впровадження застосунків у ЦОД від днів до мінут.

– **Об'єднаний транспорт**. Розроблена CiscoSystems технологія консолідованої мережі (unifiedfabric) на базі наборів стандартів DataCenterBridging і FibreChanneloverEthernet (FCoE) дозволяє значно знизити витрати на елементи мережної інфраструктури (безліч мережних адаптерів, комутатори LAN, SAN, різні мережні кабелі й т.п.). Мережні модулі шасі дозволяють відмовитися від використання комутаторів у складі блейд-серверів шляхом транзиту всього трафіку від серверів через централізовану фабрику комутації, де трафік буде оброблятися й комутируватися по призначенню. Уніфікована фабрика комутації будується на базі технології 10-Gigabit Ethernet зі стандартними кабельними з'єднаннями. Тепер у випадку зміни типу підключення сервера до мережі немає необхідності в установці додаткових адаптерів і прокладці нових кабелів.

– **Підтримка технології віртуалізації (VN-Link)**. Технологія Cisco VN-Link розширює границю мережі до віртуальної машини. Ця технологія стирає розходження з керування мережною інфраструктурою для фізичних і віртуальних серверів. Тепер всі мережні з'єднання налаштуються й управляються централізовано, без виділення додаткового рівня комутації для віртуальних середовищ. Конфігурації портів вводу/виводу й мережних політиків можуть переміщатися між віртуальними серверами, що збільшує ефективність і зменшує складність їхньої експлуатації.

– **Віртуалізований адаптер Cisco VIC**. Віртуалізований адаптер Cisco VIC дозволяє одержати на одно-двопортовому конвергентному адаптері динамічно або статично до 58 віртуальних адаптерів, кожний їх яким представлений PCIe-Функцією. Таким чином, операційна система «бачить» кожний з віртуальних адаптерів як фізичний адаптер. Даним віртуальним адаптерам можна гарантувати смугу пропущення; невикористовувана в сучасний момент частина смуги пропущення будь-якого віртуального адаптера може бути динамічно розподілена між іншими віртуальними адаптерами, яким у той же момент потрібна більша смуга, чим їм гарантував системний адміністратор.

– **Технологія розширення пам'яті Cisco.** Технологія розширення пам'яті Cisco дозволяє збільшити в 4 рази кількість рознімань для установки модулів пам'яті DIMM (до 96) у порівнянні із класичними двопроцесорними серверами архітектури x86 при збереженні швидкості частоти 1866Мгц. Збільшення оперативної пам'яті дозволяє збільшити продуктивність роботи серверів, особливо при роботі у віртуальних середовищах.

– **Сучасна продуктивність**. У рішенні Cisco UCS використовуються блейд-сервера, побудовані на базі процесорів серії Intel Xeon E5 v2 і E7v2. Ці багатоядерні процесори інтелектуально й автоматично регулюють продуктивність серверів відповідно до вимог застосунків, збільшують продуктивність у необхідний момент і істотно заощаджують енергоспоживання в період простою. Для більше точного керування серверами всі параметри продуктивності й економії електроенергії можуть бути налаштовані вручну.

– **Енергетична ефективність**. Компоненти рішення Cisco UCS були спроектовані з урахуванням вимог по енергетичній ефективності. Спрощена архітектура системи дозволила скоротити кількість елементів, для яких необхідне електроживлення й охолодження зразкове на 50% у порівнянні із класичними середовищами блейд-серверів. Шасі блейд-серверів у рішенні Cisco UCS зроблено таким чином, щоб значно збільшити теплообмін з навколишнім середовищем. Рішення Cisco UCS використовує нові, більше ефективні блоки живлення для своїх компонентів.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування інфраструктурою ЦОД на основі технології Unified

Computing System. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем керування інфраструктурою ЦОД на основі технології Unified Computing System; Досліджена система керування інфраструктурою ЦОД на основі технології Unified Computing System; На основі отриманих результатів досліджень створена програмна реалізація системи керування інфраструктурою ЦОД на основі технології Unified Computing System. Розроблені під час виконання магістерської роботи алгоритми дозволяють успішно вирішувати завдання керування інфраструктурою ЦОД на основі технології Unified Computing System. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Босько В.В. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-12
2. Босько В.В. Разработка методики оценки среднего времени обслуживания информационных пакетов в телекоммуникационной сети / Смирнов А.А., Босько В.В., Мелешко Е.В. // Системи управління, навігації та зв'язку. – Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. – Вип. 2(10). – С.162-165.
3. Босько В.В. Разработка математической модели процесса динамического управления маршрутизацией данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ навігації і управління», 2009. – Вип. 3(11). – С.208-210.
4. Босько В.В. Разработка метода определения оптимального множества путей передачи информации в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник наукових праць. – Х.: ХУПС, 2009. – Вип. 3(21). – С.102-108.
5. В.В. Босько. Разработка метода прогнозирования поведения информационного потока в телекоммуникационной сети // Збірник наукових праць. Харківського університету Повітряних Сил: – Х.:ХУ ПС, – 2010.-Вип. 3 (25) .- С.126-130.
6. Босько В.В. Исследование особенностей построения современных телекоммуникационных систем и сетей / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы восьмой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2008. – С.54.
7. Босько В.В. Исследование влияния времени мониторинга телекоммуникационной сети на точность прогнозирования поведения трафика / Смирнов А.А., Босько В.В. // Перша міжнародна науково-практична конференція "Проблеми й перспективи розвитку IT-індустрії" м. Харків , 18-19 листопада 2009р. – С.198-200.
8. Босько В.В. Анализ математических моделей телекоммуникационной сети / Смирнов А.А., Босько В.В. // Проблемы информатики и моделирования. Материалы девятой международной научно-технической конференции 26-28 ноября. – Х.: НТУ "ХПИ", 2009. – С.52-5
9. Босько В.В. Метод повышения оперативности передачи данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Збірник тез доповідей науково-практичної конференції "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 24-25 березня. – Х.: АВВ МВС України, 2010. – С.54.
10. Босько В.В. Динамическое управление процессом маршрутизации данных в телекоммуникационной сети / Смирнов А.А., Босько В.В. // Тези доповідей Міжнародної науково-практичної конференції м. Вінниця, Україна 19-21 травня 2010 року. – Вінниця: ВНТУ, 2010. – С.231-232.
11. Можаєв О.О. Часова прозорість мережі, як характеристика, що визначає виконання необхідної якості обслуговування / О.О. Можаєв, О.Д. Анохіна, С.Ю. Гайдаров, С.Г. Семенов // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 11(39). – С.133-139.

УДК 004

С. Чачуна, магістр гр. КІ-20М-1,9
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УНІФІКОВАНИХ КОМУНІКАЦІЙ ЯК СЕРВІСУ UCAAS

У статті розроблено програмне забезпечення, яке призначено для системи уніфікованих комунікацій як сервісу UCaaS. Метою розробки є дослідження та програмна реалізація системи уніфікованих комунікацій як сервісу UCaaS.Об’єктом дослідження є процес уніфікованих комунікацій як сервісу UCaaS. Предметом дослідження є методи уніфікованих комунікацій як сервісу UCaaS. Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи уніфікованих комунікацій як сервісу UCaaS. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерна інженерія, уніфіковані комунікації як сервіс, UCaaS

Постановка проблеми. Уніфіковані комунікації як послуга (UCaaS) категорія «як сервіс» або «хмарні» механізми доставки для корпоративних комунікацій. Подібно платформи як сервіс (PaaS, де центр обробки даних ємність стає доступної для підприємства за моделлю споживання від постачальника послуг), з UCaaS, уніфіковані комунікації послуги можуть бути доступні із хмари для бізнесу від малого й середнього бізнесу на підприємство.

UCaaS є частиною глобальної індустрії тенденції хмарних сервісів, також відомих як цифрове перетворення.

Традиційно, підприємства придбали й розгорнули свою власну інфраструктуру зв'язку. Це, безумовно, найбільш економічним підходом, оскільки підприємства можуть розгортати свої власні комутатори PBX і уникнути витрат на окремі телефонні лінії для кожного співробітника. З появою IP і віртуалізації центрів обробки даних, економіка перемістилися назад на користь моделі постачальника послуг. Постачальник послуг інвестує у віртуалізованих центрах обробки даних, що усуває необхідність для підприємства, щоб зробити це, і пропонує більше гнучку модель споживання.

До хмари, постачальники послуг запропонували IP Centrex і Hosted послуги зв'язку. Вони були майже ідентичні можливостями UCaaS, за винятком того, що «віртуалізація» означає, що економіка UCaaS настільки більше переконливе виключення.

Основний довід для UCaaS є тим фактом, що вона дозволяє компанії перейти від капітальних вкладень (CAPEX) до моделі операційних витрат (OPEX). Крім того, він надає компаніям можливість більш швидко збільшити їхнє споживання (тобто споживати більше ліцензій), або зменшити їхнє споживання, без потреби в капіталі. З моделлю традиційних зв'язків, компанії повинні придбати здатність попереду попиту, і вони рідко одержують це зовсім правильно, а це значить, надлишкові потужності.

По-друге, що росте складність корпоративних уніфікованих комунікацій означає, що компанії повинні інвестувати не тільки капітал. Вони повинні вкладати усе більше й більше в їх IT-персонал для того, щоб мати можливість підтримувати цю зростаючу витонченість. Додавання нових функцій і відновлення не є тривіальними й у той час як зв'язку мають вирішальне значення для успіху бізнесу й продуктивності своїх співробітників, підтримка інфраструктури вимагає високого рівня знань, що продовжує рости. Компанії можуть

вхолосту більшу частину цієї складності для постачальників послуг з моделлю UCaaS, а також забезпечення того, щоб вони завжди мають самі останні версії й функції.

Історично зложилося так, корпоративні й державні організації , необхідні для підтримки свого постачальника каретки (тобто доступ до PSTN) у високо конкурентній позиції. Якщо вони дозволяють постачальникові послуг , щоб зафіксувати їх з розчином Centrex, то вони , можливо, не в змозі досягти найкращі ціни за перевезення. Тепер, коли каретка стає товаром і ліцензії UC стає преміум, існує набагато менше ризик для переходу до рішення SP UCaaS.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи уніфікованих комунікацій як сервісу UCaaS.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи уніфікованих комунікацій як сервісу UCaaS.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем уніфікованих комунікацій як сервісу UCaaS.
– Дослідження системи уніфікованих комунікацій як сервісу UCaaS.
– Програмна реалізація системи уніфікованих комунікацій як сервісу UCaaS.

Об'єктом дослідження є процес уніфікованих комунікацій як сервісу UCaaS.

Предметом дослідження є методи уніфікованих комунікацій як сервісу UCaaS.

Методи дослідження базуються на методах теорії інформації та кодування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Прийшов час приймати ключові рішення в області IT. Це й хвилюючий, і складний момент. За останні п'ять років загальна кількість і розмаїтість засобів зв'язку багаторазово збільшилося. Користувачі одержали доступ до каталогів з можливістю відстеження присутності, кілька видів синхронного й асинхронного обміну текстовими повідомленнями, а також IP-рішення для спільної роботи на основі передачі звуку, відео й даних. Функції надання й підтримки цих нових послуг перейшли від устаткування замовника до хмари й у деяких випадках знову повернулися до корпоративної платформи. Більше того, перехід на уніфіковані комунікації (UC) забезпечив користувачам консолідоване й зручне середовище, а для IT-відділів спростив підтримку й надання послуг зв'язку завдяки єдиній платформі.

Хоча сам термін «хмара» став популярним у середині 2000-х рр., якийсь час хмарні технології служили потужним засобом для розгортання різноманітних корпоративних застосунків. Постачальники послуг довго надавали розміщені на хостингу сервіси аудіо-, відео- і веб-конференц-зв'язку із центрів обробки даних по всій земній кулі. Згодом розміщені в хостинг-середовищі застосунки електронної пошти й підвищення продуктивності були перенесені в хмару постачальника послуг, і надання засобів асинхронного зв'язку стало практично стандартним компонентом проектів спільної роботи через хмарне середовище. Завдяки UC підприємства одержали можливість впровадити комунікаційні технології нового покоління, а постачальники змогли надати принципово нові послуги з моделі as-a-Service (UCaaS – уніфіковані комунікації як послуга).

Тут потрібно враховувати два ключових факторів. По-перше, сучасні підприємства середнього й великого бізнесу хочуть замінити застарілі розрізнені комунікаційні платформи (такі, як офісні АТМ на базі технології TDM, автономні системи відеоконференц-зв'язку) уніфікованими й модернізованими рішеннями. По-друге, попит на хмарні технології зв'язку й спільної роботи стрімко росте, і згідно із прогнозами продовжить збільшуватися протягом наступних п'яти років. Потреби підприємств у рішеннях UCaaS принципово змінилися з появою, удосконалюванням і поширенням нових розробок. Тепер особи, відповідальні за прийняття рішень в області IT, задають інше питання: не «що» (які рішення доступні в хмарі), а «як» (як використовувати можливості хмари для підтримки передових рішень спільної роботи).

У цьому документі розглядається ряд тенденцій у корпоративному секторі, які ми спостерігали протягом останніх 12 місяців. Після короткого огляду ринку UCaaS і переваг, пропонованих сучасними постачальниками хмарних технологій, ми проаналізуємо основні корпоративні тенденції, які виявилися успішними в реальних сценаріях розгортання: визначення пріоритетів застосунків, методології, а також перешкоди й проблеми, про які варто знати. Справжній документ містить короткий огляд тенденцій і передових практик компаній, які першими впровадили нове покоління хмарних рішень для спільної роботи. Він послужить керівництвом для IT-відділів, що зробили вибір на користь таких рішень, але не знаючих, як діяти далі.

Методологія

Фахівці Wainhouse Research (WR) проаналізували тенденції ринку хмарних рішень для зв'язку й спільної роботи більш ніж за 10-літній період. Для своїх досліджень аналітики одержали дані більш ніж від 200 постачальників устаткування й послуг. Аналітики проводили регулярні опитування корпоративних користувачів і відповідальних осіб, щоб оцінити поточний рівень впровадження технологій спільної роботи. Аналітики також взаємодіють з багатьма замовниками в корпоративному секторі, надаючи рекомендації із планів розвитку UC і вибору технологій. У цілому, цими зусиллями створюється велика база об'єктивних і суб'єктивних ринкових даних.

Крім того, для цілей справжнього документа аналітики опитали кілька провідних постачальників послуг UCaaS, включаючи Orange, Vodafone, West IP Communications, KPN і Telstra. Вони представляють найбільш велику екосистему постачальників UCaaS, що сьогодні включає практично всіх мережних операторів першого рівня, ряд постачальників послуг для спільної роботи, системних інтеграторів, постачальників професійних послуг і інших учасників ринку. Ці цілеспрямовані опитування доповнили й підкріпили дані, які аналітики зібрали на сучасний момент, створивши докладне подання про підхід сучасного середнього й великого бізнесу до переносу комунікацій і спільної роботи в хмару.

Поточний стан ринку рішень для спільної роботи в хостинг-середовищу

В останні десять років аналітики спостерігали швидкий і наростаючий розвиток ринку рішень для спільної роботи, розташовуваних на хостингу. У цьому секторі споконвічно були представлені послуги аудіо-, відео- і веб-конференц-зв’язку. Але згодом значне поширення одержали передові сервіси UCaaS. Поява послуг UCaaS частково стало причиною того, що традиційні рішення для аудіо-, відеозв'язку й організації персональних веб-конференцій перестали служити основним джерелом прибутку. Протягом наступних п'яти років очікується досить помірний темп росту в секторі послуг аудіо- і веб- конференц-зв'язку, розташовуваних на хостингу, тоді як джерелом доходу в сегменті відео стають персональні рішення по обробці й передачі відеоданих. У цілому, фахівці очікують максимальний ріст у сегменті UCaaS, де прогнозується середньорічний темп росту 43 % протягом наступних п'яти років.

Як уже говорилося, розвиток ринку UCaaS відбувається за рахунок традиційних автономних сервісів аудіоконференцій. Багато підприємств приводять зниження витрат на розташовувані на хостингу сервіси аудіоконференцій як аргумент для обґрунтування планів розгортання UC і в результаті активно спонукують користувачів переходити на нові платформи UC. На сьогоднішній день рішення UC використовуються для проведення приблизно 9 % всіх аудіоконференцій. Аналітики прогнозують збільшення цього показника й припускають, що в 2021 році на технології UC буде доводитися більше 25 % глобального ринку послуг аудіоконференц-зв’язку.

Прихильники хмарних технологій – хто сьогодні приймає рішення

Може здатися саме собою що розуміє, що підтримка з боку вищого керівництва – ключова вимога для переходу на хмарні технології. І дійсно, ця точка зору часто підтверджувалася в ході опитування постачальників. Рішення перейти на хмарні технології вимагає сильної підтримки з боку вищого керівництва. Це гарантує погодженість бізнес-стратегії з напрямком проекту. У більшості випадків відповідальність за рішення по-

колишньому лягає на IT-директорів, однак фінансовий директор також, як правило, бере участь в обговоренні питань витрат.

Хоча в плануванні переносу спільної роботи в хмару ключову роль грають фінансовий і IT-директори, у проекті повинен брати участь більше широке коло фахівців. Конкретні підрозділи, які потрібно залучити до обговорення, залежать від характеристик кожного проекту міграції, але для всіх сценаріїв є один загальний момент: чим більше послуг уніфікується на базі хмари, тим більше підрозділів повинне брати участь на попередніх етапах проекту. Наприклад, за міграцію сервісів телефонії може відповідати переважно IT-відділ. Але в міру додавання програмних клієнтів, функцій миттєвого обміну повідомленнями, відеозв'язку на робочому місці, спільного використання даних і сервісів конференц-зв'язку число зацікавлених сторін росте. У більшості випадків перехід до хмари, як мінімум, вимагає участі IT-відділу, відділу кадрів, закупівель і юридичного відділу.

Для проектів переходу на хмарні технології, пов'язані із заміною офісної АТМ у короткий термін, головне питання звичайно полягає в економічних стимулах – і швидко зводиться до проблем IT. Однак, чим більше стратегічні питання розглядаються, тим важливіше стає залучити до участі в обговоренні всі підрозділи організації.

Ціннісна пропозиція: які вимоги компанії, що переходять на хмарні технології, пред'являють до постачальників хмарних комунікаційних послуг?

Незалежно від кола зацікавлених осіб, у більшості випадків планування переходу на хмарні рішення починається з обговорення переваг. Це звичайно припускає аналіз економічної цінності переходу на хмарне середовище й часто більше велике дослідження можливостей перетворення бізнесу, пов'язаних з новою платформою UCaaS. Кожний постачальник адаптує ціннісну пропозицію у відповідності зі своєю спеціалізацією й існуючими лінійками продуктів. Наприклад, більшість мережних операторів позиціонують свої пропозиції UCaaS у рамках більше комплексного рішення для передачі голосу й мережної взаємодії. Таким чином, можна виділити ціннісні пропозиції, найцікавіші для осіб, що приймають рішення на підприємствах:

– Поліпшені моделі витрат: з кожним проектом переходу на хмарні технології зв'язаний елемент витрат, і багато підприємств розраховують знизити сукупну вартість володіння (TCO) у результаті переносу сервісів спільної роботи в хмару. У ході обговорення витрат розглядаються можливості економії в короткостроковій і середньостроковій перспективі, у тому числі рішення, відновлення яких кожні 2-3 роки зажадає багато часу й фінансових витрат. Сукупна вартість володіння UC стає каменем спотикання для багатьох осіб, що приймають рішення. Сьогодні увага організацій зміщається від економії за рахунок продуктивності (яку важко оцінити кількісно) до зниження постійних витрат, пов'язаних з кадровим забезпеченням, модернізацією, навчанням, електроживленням, устаткуванням, зв'язком і обслуговуванням. Гарний партнер по хмарних сервісах може внести додатковий вклад в обговорення цих питань, створивши об'єктивну модель TCO, що відповідає бізнес-стратегії компанії. Вражають фінансові обмеження, з якими доводиться мати справу багатьом IT-керівникам. Недавно старший віце-президент по IT в успішній транснаціональній компанії зі штатом 50 000 чоловік помітив: «Протягом останніх п'яти років у нас був капітальний бюджет з нульовою базою й без приросту». Керівник свідомо вибирав об'єкти фінансування, і він не самотній у цьому. Невеликі річні капітальні бюджети, як правило, стимулюють потреба в моделях витрат на основі співвідношення експлуатаційних і капітальних витрат, які допомагають ефективно розподіляти засобу на кілька років. Усе більше підприємств готові прийняти модель розрахунку TCO з нульовим прибутком, якщо це дасть їм можливість перетворити капітальні витрати в експлуатаційні в результаті переносу спільної роботи в хмару. Очікування повинні бути адекватними – хмарне середовище не гарантує зниження TCO. Економія залежить від розміру організації, набору послуг і специфіки підприємства. Стандартна модель UCaaS також дозволяє оплачувати тільки ті ресурси, які потрібні в даний конкретний момент. Необхідність у розширенні платформи для підтримки прогнозованого росту бізнесу в 3-5-літній перспективі

або прив'язка організації до корпоративної ліцензійної угоди строком у кілька років – от над чим варто думати в процесі розгортання рішення на території замовника, оскільки більшість постачальників UCaaS пропонують гнучкі моделі з оплатою в міру споживання послуг. Можливість швидкого масштабування сервісів шляхом додавання й видалення ліцензій у міру необхідності – ключова перевага UCaaS.

– Спрощення середовища: перехід на хмарні технології, як правило, містить елемент консолідації постачальників. Провідні постачальники UCaaS пропонують різноманітні асортименти послуг, у тому числі мережні підключення, керовані й мобільні послуги, а також різноманітні застосунки на базі хостингу. Аналітики спостерігали дуже небагато випадків міграції окремих застосунків, оскільки середні й великі підприємства прагнуть домогтися ефективності за рахунок консолідації й скорочення числа постачальників, з якими доводиться мати справа їх IT-відділам. Постачальники хмарних послуг інвестували значні засоби у свої платформи UCaaS, щоб надати замовникам масштабоване, продуктивне й надійне середовище. Як добре відомо кожному фахівцеві, відповідальному за рішення в області IT, повноцінне середовище UC – комплексний проект, для якого потрібні різні елементи телефонії, відео й конференц-зв'язку. Можливість використовувати вже існуючу спеціалізовану платформу – ключова перевага UCaaS. Більше того, можливість прискорити планування й розгортання й оперативно додавати користувачів і функції найчастіше є найважливішим аргументом на користь моделі UCaaS.

– Можливості підтримки актуалізації: тут мова йде про здатність постачальника постійно підтримувати актуальний стан розміщених у хостинг-середовищі застосунків. Це особливо привабливий довід в обговоренні UC, оскільки постачальники платформ усе швидше надають нові версії й додаткові функції. Уважається, що постачальники послуг краще впораються з коротким циклом відновлення, чим виділена група IT-фахівців на підприємстві. Таким чином, постачальники послуг UCaaS повинні використовувати гнучку модель, щоб можна було розгортати нові функції в темпі, прийнятному для кожного окремого корпоративного замовника.

– Безпека: постачальники хмарних послуг перетворили безпеку – традиційний предмет турботи середніх і великих підприємств – у конкурентну перевагу. Кожний постачальник UCaaS забезпечує той або інший рівень безпеки, що відповідає потребам середньостатистичної організації середнього або великого бізнесу. Безсумнівно, не маючи солідної репутації в плані забезпечення безпеки, ці постачальники швидко б стали банкрутами. Деякі постачальники зволіли перевести проблему безпеки в іншу площину й використовувати її як можливість виділитися серед конкурентів. Серед можливих варіантів – спеціалізовані сертифікати, що відповідають галузевим або державним вимогам, або розміщення центрів обробки даних у стратегічних пунктах для відповідності регіональним стандартам.

– Інновації: деякі постачальники послуг UCaaS розвивають унікальну здатність брати участь у стратегічних проектах перетворення бізнесу. У процесі роботи з корпоративними замовниками ці постачальники нагромадили великий досвід у виборі підходящих для них рішень. Здатність UC перетворювати бізнес-комунікації стала досить привабливою метою, до якої прагне більшість підприємств. Результатом співробітництва з гарним партнером по послугах UCaaS може стати такий стратегічний проект перетворень.

Конкуренція на ринку UCaaS росте. Тому постачальники прагнуть виділити свої послуги серед конкурентів, опираючись на власні унікальні переваги. От кілька прикладів.

– Мобільність. Постачальники, що спеціалізуються на мобільних послугах, домоглися тісної інтеграції між застосунками UC, розміщеними на хостингу, і своїм мобільним середовищем. Наприклад, можливість одержати єдиний номер для передачі голосових викликів на мобільний пристрій, настільний телефон і клієнт UC залучає багатьох корпоративних користувачів.

– Контакт-центр. Якщо перехід від голосових сервісів TDM на уніфіковані комунікації на базі IP лякає своєю складністю, можна обговорити подібний проект стосовно

до контакт-центрів. Росте число постачальників послуг UCaaS, що спеціалізуються на наданні сервісів і підтримці контакт-центра в хостинг-середовищу й розширювальним своїм пропозиціям UCaaS у цьому напрямку. Залежно від розміру й складності корпоративного контакт-центра підтримка постачальника UCaaS може стати винятково коштовної.

– Інтеграція. Можливість інтегрувати комунікації в бізнес-процеси або існуючі рішення для керування робочими потоками довго була заповітною метою галузі UC. Складності й проектні вимоги, пов'язані з такою інтеграцією, часто відлякують багато організацій. Усе більше постачальників UCaaS створюють центри компетенції в області інтеграції, надаючи що налаштовуються API-Інтерфейси, готові можливості інтеграції зі стандартними системами CRM і засобами підвищення продуктивності (наприклад, SalesForce.com) і при необхідності професійні послуги для особливих проектів інтеграції.

Розробка структурної схеми

Визначення пріоритетів застосунків – які застосунки переважно використовуються в хмарному середовищі?

Вибираючи серед застосунків потенційних кандидатів для переносу в хмару й упорядковуючи їх по пріоритеті, у першу чергу варто поставити запитання: «Які застосунки вже використовуються в хмарі?» По нашім досвіді, більшість середніх і великих підприємств користуються сервісами аудіо- і веб-конференц-зв’язку на базі хостингу. Хоча ця обставина може вплинути на вибір постачальника (замовника цікавить, чи можна консолідувати додаткові послуги з існуючими сервісами конференц-зв'язку, розміщеними в середовищі постачальника), воно навряд чи вплине на розподіл застосунків по пріоритетах. Всі постачальники, опитані в ході нашого дослідження, пояснювали, що комбінація й пріоритетний порядок застосунків, обраних для переносу в хмару, унікальні для кожного підприємства й найчастіше залежать від розміру організації і її стратегічних стимулів. Основні шляхи переходу на середовище UCaaS можна звести до двох типів: орієнтованим на передачу голосу або на миттєвий обмін повідомленнями. Провідні постачальники не тільки надають послуги, але й допомагають організації визначити її унікальні стимули й фактори успіху для переходу на хмарні технології.

Передача голосу й телефонія

Загальновизнано, що голосовий зв'язок, зокрема телефонія, – найважливіша послуга для бізнесу. Хоча аналітики впевнені, що з розвитком мобільних можливостей діапазон прийнятної якості голосового зв'язку росте, простої як і раніше неприпустимі, особливо коли мова йде про взаємодію між організаціями, між компаніями й споживачами й між вищими керівниками.

Рішення UCaaS з підтримкою телефонії – самий звидкозростаючий сегмент серед застосунків UC, розміщених на хостингу. Попит на такі рішення стимулює потреба в заміні великого числа застарілих офісних АТМ на базі TDM і VoIP, підтримка яких поступово припиняється. Не секрет, що більшість постачальників послуг UCaaS побудували свої хостинг-рішення на основі існуючої інфраструктури передачі голосу й пов'язаних з нею сервісів. Наприклад, мережні оператори, що надають послуги UCaaS, пропонують розширені рішення для передачі голосу в комбінації зі шлюзами, магістралями VoIP, підключеннями до телефонної мережі, що комутирується, загального користування й т.п. З іншого боку, постачальники послуг для спільної роботи надають глобальні мережі передачі голосу разом з міжнародними послугами в складі сервісів аудіоконференц-зв'язку, розташовуваних на хостингу. У кожному із цих випадків постачальники розглядають хостинг-послуги VoIP як логічне продовження своєї лінійки продуктів, а отже, і як можливість використовувати існуючу інфраструктуру.

Як згадувалося вище, перенос голосового зв'язку в хмару часто розглядається як тактичний проект, необхідність якого обумовлена старінням інфраструктури офісної АТМ (PBX). Такі проекти швидко переходять у фазу планування, як тільки ухвалене рішення про вибір постачальника. Функції, що входять у розміщене на хостингу рішення для передачі голосу, аналогічні тим, які передбачаються в рішеннях, розгорнутих на встаткуванні

замовника: одержання тонального сигналу, перенос номерів DID, пакети LD і ILD, плани внутримережних викликів і т.п.

Після телефонії наступні по пріоритеті застосунки, які найчастіше призначаються для переносу або консолідації, включають аудіо-, відео- і веб-конференц-зв'язок, підтримку мобільності й функції контакт-центра. Плануючи перехід на хмарне середовище, можна також розглядати розміщення на хостингу застосунків для миттєвого обміну повідомленнями й контролю присутності. Однак більшість постачальників заявляють, що багато організацій уже впровадили корпоративні системи миттєвого обміну повідомлення. У таких випадках обговорюють уже не хостинг, а інтеграцію, тобто ставиться питання, наскільки нове, розміщене на хостингу рішення для телефонії інтегрується з існуючою системою миттєвого обміну повідомленнями, розгорнутої в організації?

Особлива увага варто приділяти зростаючому попиту на розміщені в хостинг-середовищу рішення для контакт-центра на базі IP. На таких рішеннях спеціалізуються трохи постачальників, які швидко помітили, що усе більше підприємств починають планування переносу в хостинг-середовище з застосунків для контакт-центра. Здавалося б, це суперечить здоровому глузду, адже інфраструктура контакт-центра завжди складніше, ніж корпоративна телефонія. Однак постачальники розташовуваних на хостингу сервісів контакт-центра прийшли до виводу, що для замовників подібна складність стимулює потребу в рішенні для контакт-центра нового покоління операторського класу. Існуючі застарілі офісні АТМ на базі технології TDM не просто передають функції системам корпоративного телефонного зв'язку. Є безліч контакт-центрів зі стабільно працюючими, але застарілими офісними АТМ на базі TDM. Таким користувачам непросто перейти на нові IP-рішення, розміщені на території підприємства або в хостинг-середі. Постачальник хостинг-послуг з досвідом розгортання рішень для контакт-центрів у спеціалізованому хмарному середовищі може вирішити безліч проблем, з якими зштовхнулася б організація, впроваджуючи аналогічне рішення на своєму встаткуванні.

Миттєвий обмін повідомленнями

У той час як передача голосу звичайно вважається складним, але критично важливим бізнес-застосунком, миттєвий обмін повідомленнями розглядається практично як протилежне рішення: простої в розгортанні, масове й не настільки критичне для бізнесу. Підприємства, що використовують розміщену на хостингу систему миттєвого обміну повідомленнями протягом останніх двох років, у більшості випадків перенесли сервіси електронної пошти й (або) керування вмістом у хмару, щоб попередньо оцінити нову технологію.

Трохи постачальників UCaaS відзначають чітке розходження між проектами, орієнтованими на передачу голосу, і проектами на основі вимог миттєвого обміну повідомленнями. Зокрема, коли мова йде про розміщені на хостингу рішеннях для миттєвого обміну повідомленнями, звичайно плануються пробні розгортання, тоді як міграція систем голосового зв'язку більше проектно-орієнтований. Однак після розгортання вихідного розміщеного в хостинг-середовищу застосунку наступні застосунки стають більше погоджені й однаковими, коли підприємства звертаються до сервісів аудіо-, веб- і відеоконференц-зв'язку, підтримки мобільності, контакт-центра й т.п.

Вихід за рамки передачі голосу й миттєвого обміну повідомленнями: конференц-зв'язок і спільна робота

Коли за допомогою платформи UCaaS закладена основа для передачі голосу й миттєвого обміну повідомленнями, перенос сервісів спільної роботи з використанням аудіо-, відео- і веб-технологій часто планується з урахуванням вимог економії витрат. Хоча такий підхід не унікальний для хмари (багато проектів розгортання UC на території замовника включають консолідацію інфраструктури конференц-зв'язку), дуже часто він стає продовженням обговорення розміщених рішень для передачі голосу або миттєвого обміну повідомленнями.

З погляду можливостей кожна платформа UCaaS надає в тій або іншій формі загальний доступ до робочого стола й застосунків. З організацією аудіоконференцій можуть бути зв'язані додаткові витрати (зокрема, з викликами ТфОП), але економія, що досягається за рахунок використання платформи UCaaS замість традиційних розташовуваних на хостингу сервісів аудіоконференц-зв'язку, часто занадто переконлива, щоб відмовитися від переносу цих сервісів на хостинг-платформу UC. Відеоконференц-зв'язок – звичайно найбільш складний додаток у стеці UC, і тому іноді його перенос виконується в останню чергу. Крім більше докладного аналізу можливостей локальних і глобальних мереж відеоконференц-зв'язок часто вимагає інтеграції між настільними клієнтами UC і встановленими стаціонарними системами відеозв'язку.

Не кожна платформа UCaaS надає всі необхідні споживачам функції спільної роботи з використанням аудіо-, відео- і веб-комунікацій. Варто зрозуміти основні потреби й впровадити рішення (в ідеалі від постачальника послуг UCaaS), інакше користувачі можуть заповнити відсутні засоби власними неконтрольованими застосунками.

Методології міграції в хмарне середовище

Як і визначення пріоритетів застосунків, методологія їхнього переносу в хмару унікальна для кожного підприємства. Однак є кілька загальних підходів, які в основному залежать від набору використовуваних застосунків, що існує інфраструктури й стратегічних стимулів конкретної організації:

– Пробні розгортання в порівнянні зі структурованими міграціями. Пробні міграції, як правило, проводяться в рамках підрозділів. При цьому група IT-фахівців випробовує нові, розміщені на хостингу послуги до того, як підприємство ухвалить рішення щодо більше масштабному розгортанні. Структуровані міграції використовують методологічний підхід: спочатку вибирають користувачів, які будуть одержувати нові, розміщені на хостингу послуги, а наступне розгортання розглядають як завдання планування проекту. Більшість середніх і великих підприємств, що використовують структуровану міграцію, у невеликому масштабі проводять пробне розгортання сервісів для перевірки рішення. Як уже згадувалося, більшість постачальників відзначають, що міграції розміщених на хостингу систем миттєвого обміну повідомленнями звичайно починаються як пробне розгортання, а міграції рішень для передачі голосу проводяться по структурованому алгоритмі.

– Порівняння гібридної й оптової моделей. Всі постачальники, опитані в ході нашого дослідження, підтвердили, що в середніх і великих організаціях дуже рідко проводиться повний перенос сервісів у хмару. Навпаки, підприємства використовують методологічний підхід до міграції, створюючи гібридне середовище, що поєднує існуючі сервіси, розгорнуті на власній платформі, і нові послуги, надавані постачальником через хмару.

– Міграція, заснована на амортизації. Найпоширеніший підхід до переносу сервісів голосового зв'язку в хмару – визначення пріоритетності заміни застарілих офісних АТМ. У багатьох середніх і великих організаціях уже є сукупність різних офісних АТМ: обслуговування одних користувачів як і раніше здійснюється через застарілі, але працездатні комутатори TDM, а обслуговування інших – за допомогою нових рішень VoIP. Стандартний підхід припускає першочергову міграцію на об'єктах із застарілою й непідтримуваною інфраструктурою й в останню – на об'єктах, де встаткування поки не застаріло.

– Стратегічна міграція. Віддалена робота, загальне офісне середовище й гнучка організація робочого простору – все це поступово стає звичайним явищем, особливо в Європі. Подібні тенденції часто пов'язані із зусиллями компаній по скороченню займаних площ. Підприємства, що переходять на передову платформу UCaaS з метою одержати гнучкі комунікаційні можливості з відстеженням присутності, часто проводять міграцію на об'єктах, де планується скорочення виробничих площ.

– Традиційна міграція. Традиційна міграція сервісів VoIP нерідко починається з невеликих філій, щоб перевірити рішення VoIP. Потім у найкоротший термін проводиться міграція на основних площадках, щоб домогтися максимальної економії в порівнянні з

рішеннями на основі TDM. Ці оптимальні прийоми також застосовуються прямо до переносу в хмару.

Переконаєтеся, що у вашого постачальника є рішення для потреб гібридного розгортання – воно може включати інтеграцію з існуючими застарілими офісними АТМ або системами миттєвого обміну повідомленнями.

Перешкоди й проблеми – про що варто знати

Перехід на хмарні технології нерідко сполучений із численними труднощами й перешкодами. Деякі з них унікальні й не піддаються прогнозуванню, інші більше поширені й очевидні. Нижче перераховані найбільш загальні проблеми міграції в хмару, відмічувані постачальниками послуг і підприємствами:

– Помилки в політиках. Є чи в організації формальна політика аутсорсингу? Чи прийняті найважливіші правила, що визначають, де можуть зберігатися дані організації й співробітників і хто може одержувати до них доступ? Які політики діють відносно даних замовників? Чи можна архівувати документацію контакт-центра в хмарі або вона повинна зберігатися в корпоративному центрі обробки даних? Якісь із цих політик добре відомі, інші можуть бути невизначеними. Найкраще на ранніх етапах задіяти в плануванні переходу до хмарних технологій юридичний відділ і фахівців з кадрів.

– Внутрішній краудсорсинг. Цей термін означає прямий зв'язок між тривалістю проекту й кількістю осіб, що приймають рішення. Перенос офісної АТМ у хмару повинен проводитися з урахуванням тактичних міркувань і цілей проекту, тому в цьому випадку необхідно тільки участь фахівців з телефонії й мереж. Однак перехід від традиційних послуг передачі голосу до сервісів UC може, крім цих фахівців, зажадати участі персоналу служби підтримки настільних систем, відділу кадрів і декількох інших підрозділів. У персоналу може бути обґрунтоване або необґрунтоване упередження відносно платформи, рішення, функціональних вимог, інтерфейсу й постачальника. Процес ухвалення рішення тим складніше, чим більше осіб у ньому бере участь. Саме тому важливо по можливості відокремити збір вимог від вибору платформи. Щоб успішно перебороти опір, важливо заручатися підтримкою проекту з боку вищого керівництва.

– Проблеми безпеки. Кожний постачальник послуг зв'язку й спільної роботи в хостинг-середовищу забезпечує той або інший рівень безпеки. Аналітики рекомендуємо запитувати в постачальника відомості про діючим у його компанії політиках і практиках забезпечення безпеки. Як правило, комбінація часток VPN-мереж на базі IP і логічно сегментованих застосунків відповідає вимогам безпеки більшості організацій. Також варто враховувати прийняті в компанії постачальника політики керування доступом персоналу до даних, архівування даних, географічного розміщення систем зберігання й центрів обробки даних, а також сертифікації в області безпеки для конкретних галузевих вертикалей і державних установ.

– Зміни у взаємодії з користувачами. Перенос послуг зв'язку й спільної роботи в хмару може зажадати змін у взаємодії з користувачами. Це може передбачати зміни існуючого плану нумерації, розміщення термінального встаткування, номерів для конференц-зв'язку й PIN-кодів, номерів настільних телефонів і ін. Із запровадженням у дію нових сервісів, імовірно, з'являться й нові програмні клієнти. Варто обов'язково обговорити всі передбачувані зміни й ретельно проаналізувати їхнього наслідки: до яких змін користувачі зможуть пристосуватися й, саме головне, що потрібно залишити колишнім? Варто заручатися підтримкою ключових підрозділів, які будуть використовувати нове рішення UCaaS.

– Питання контролю. IT-відділи може хвилювати втрата контролю над ключовими каналами зв'язку. Важливо розібратися, чи обґрунтоване це занепокоєння (чи може постачальник забезпечити такий же рівень обслуговування кінцевих користувачів, як IT-відділ? чи Збереже IT-відділ у своїх руках необхідні засоби адміністративного контролю?) або мова йде про суб'єктивні переживання IT-фахівців із приводу своєї цінності й можливого звільнення? Щоб зняти ці побоювання, деякі постачальники послуг UCaaS надають

корпоративним ІТ- фахівцям такий рівень контролю, що вони вважають за необхідне, у тому числі над наданням ресурсів кінцевим користувачам, груповими політиками й підтримкою. Якщо організацію хвилюють питання якості й стійкості, їй варто вибрати постачальника, що буде дотримувати угод про рівень обслуговування на основі системи штрафів.

– Вимоги інтеграції. Чи йде мова про сервіси UC, розташовуваних на хостингу або на території замовника, створення гібридного середовища вимагає інтеграції різноманітних комунікаційних рішень від декількох постачальників. Крім того, переваги UC максимальні, коли нові послуги зв'язку прозоро інтегруються в існуючі робочі потоки й бізнес-процеси. Іноді ці вимоги нелегко виконати, особливо у випадку сучасних складних комунікаційних послуг, таких як відеоконференц-зв'язок і функції контакт-центра.

– Неправильне розуміння суті хмарних технологій. Часто подання про те, що таке хмарне середовище для зв'язку й спільної роботи, невірні. Деякі вважають, що кожна хмара припускає автоматизоване надання ПЗ як послуги (SaaS), інші впевнені, що це корисна модель із оплатою тільки використовуваних сервісів. Переговори з постачальником хмарних послуг варто починати із чіткого формулювання поточних потреб і стимулів організації. Необхідно зрозуміти, що пропонує постачальник, і разом з ним виробити оптимальне рішення UCaaS.

Вибір постачальника хмарних послуг – якими якостями повинен володіти підходящий постачальник

За останні роки кількість і розмаїтість постачальників хмарних послуг зв'язку й спільної роботи значно збільшилося. Багато мережних операторів, постачальники сервісів конференц-зв'язки, системні інтегратори й постачальники інфраструктури офісних АТМ додали пропозиції UCaaS у свої портфелі послуг. Тому підбор постачальника хмарного середовища варто починати серед надійних партнерів, з якими організація вже співробітничає, щоб використовувати переваги консолідації послуг, що супроводжує економії й сталих довірчих взаємин. Не варто вивчати обстановку, використовуючи запити пропозицій або інші формальні процедури постачання. Нижче перераховані якості, які можуть відігравати ключову роль у виборі підходящого постачальника UCaaS:

– Досвід. Зростаючі перспективи одержання прибутку, пов'язані з ринком рішень UCaaS, залучають безліч компаній, що мають добрі наміри, але безпринципних у досягненні мети. Шукайте постачальника із солідною репутацією й фінансовою стійкістю. Жодна організація не хоче виявитися в ситуації, коли буде потрібно ще одна міграція через те, що постачальник послуг UCaaS відмовився від подальшого співробітництва. Усе більше постачальників надає що налаштовуються API-Інтерфейси й професійні послуги для підтримки особливих проектів інтеграції. Варто довідатися про ці можливості на ранніх етапах обговорення UCaaS.

– Географія присутності. Середні й великі підприємства часто мають представництва в багатьох країнах, тому їм потрібний постачальник з відповідною географією присутності. Коли мова заходить про розташовувані на хостингу сервісах голосового зв'язку, далеко не всі постачальники пропонують послуги телефонії на всіх великих ринках. У таких випадках постачальники часто співробітничають один з одним, щоб надавати необхідні послуги передачі голосу в міжнародному масштабі. Варто зрозуміти, чи відповідає подібне партнерство потребам вашої компанії, яке його потенційний вплив на угоди про рівень обслуговування, моделі витрат і строки усунення неполадок.

– Основні області спеціалізації. Як показує дослідження WR, сьогодні, коли розташовувані на хостингу послуги UC широко використовуються в галузях, що обслуговуються різними постачальниками, кожний постачальник позиціонує свої унікальні переваги, опираючись на існуючі області спеціалізації. Можна виділити наступні важливі категорії постачальників:

1. Мережні оператори. Платформа UCaaS часто інтегрована в рішення MPLS і сервіси голосового зв'язку. Це може забезпечити перевагу з погляду вартості, коли такі послуги надаються у вигляді пакета.

2. Мобільні оператори. Обговорення пропозицій UCaaS може починатися з мобільних можливостей. Замовники зацікавлені у використанні мобільного номера для виклику клієнта UC з комп'ютера.

Постачальники послуг для спільної роботи. Тісна інтеграція з існуючої розміщеним на хостингу рішенням для аудіоконференц-зв'язку дозволяє організаціям у зручному для себе темпі перейти на нову технологію сполучення-конференц-зв'язку на базі UCaaS.

4. Системні інтегратори. Багато системних інтеграторів, які часто є надійними партнерами для аутсорсингу в області IT, включають у свої пропозиції керованих послуг розгортання сервісів UCaaS з розміщенням на хостингу.

5 Сполучення різних спеціалізацій. Деякі постачальники спеціалізуються в декількох зазначених дисциплінах, у те час як інші ефективно співробітничають один з одним у плані надання більше універсальних рішень.

Всебічні знання. Для успішної міграції на платформу UCaaS потрібен великий досвід у різних технологіях і дисциплінах, включаючи планування, надання ресурсів, передачу голосу, організацію мережі, спільну роботу, сервіси для настільних систем, підтримку й освоєння нових рішень користувачами. Важливо знайти постачальника із глибокими знаннями в цих різноманітних областях.

– Глобальне мислення. Впровадження рішення UCaaS варто розглядати не тільки як можливість поліпшити структуру витрат організації на зв'язок. UCaaS дозволяє докорінно змінити способи взаємодії співробітників. Успішний постачальник має досвід роботи з багатьма підприємствами й повинен добре розуміти, які рішення підійдуть замовникові, а які немає. Кращі постачальники послуг UCaaS усвідомлюють, що UC – це не просто заміна системи телефонного зв'язку, і можуть підтвердити свою здатність допомогти замовникові перетворити існуючий бізнес-процеси за допомогою технологій UC. Треба визнати, що більшість IT-відділів і бізнес-підрозділів не можуть домогтися успіхів у перетворенні бізнесу власними силами.

Кількість і розмаїтість постачальників послуг UCaaS росте приголомшливими темпами. Мережні оператори, мобільні оператори, системні інтегратори, постачальники послуг конференц-зв'язку – всі учасники ринку прагнуть підвищити цінність своїх ключових пропозицій і домогтися сукупного ефекту в сполученні з існуючими областями спеціалізації, включивши у свої портфелі послуг нові сервіси UCaaS. У результаті дослідження аналітики виявили наступні загальні для середніх і великих підприємств фактори, що стимулюють перехід на платформу UCaaS і її розвиток:

– Старіння офісних АТМ. Коли виникає необхідність заміни застарілих офісних АТМ, IT-керівники використовують цю можливість для створення й обґрунтування більше великого плану впровадження технологій UC шляхом додавання функцій у традиційні автономні системи телефонії.

– Розвиток пропозицій UCaaS. Якщо говорити про компанії Orange, Vodafone, West IP Communications, KPN, Telstra і інших великих галузевих гравцях, ясно, що ці постачальники послуг активно працюють над удосконалюванням своїх пропозицій UCaaS. Хоча ці технології ще перебувають на початковому етапі впровадження, згадані постачальники значно поліпшили свої рішення за останні 3 роки.

– Відкритість IT. Хмарні рішення й сервіси UCaaS у багатьох випадках стають природним продовженням стратегічних планів впровадження UC. Багато в чому це пов'язане зі зростаючою доступністю зрілих пропозицій. Ситуацію резюмує наступне висловлення одного IT-керівника: «Я хочу, щоб IT-відділ займався взаєминами з постачальниками, а не підтримкою користувачів». Всі частіше хмара розглядається як стратегічний компонент майбутніх проектів в області UC.

– Фінансові стимули. Можливість за допомогою хмарних технологій скоротити сукупну вартість володіння, змінити співвідношення капітальних і експлуатаційних витрат на користь останніх, усунути необхідність інвестицій у ресурси й (або) забезпечити

підтримку моделей з оплатою залежно від числа користувачів досить актуальна сьогодні для багатьох IT-організацій, що вирішують проблеми фінансування ключових рішень.

– Цінність хмари. Крім більше вигідної фінансової моделі підприємства прагнуть одержувати новітні можливості з постійною актуалізацією й визволити ресурси підтримки й навчання.

– Визнання з боку користувачів. Швидке освоєння нових технологій користувачами – ключова перевага успішного партнерства з постачальником хмарного середовища. Використання існуючого середовища постачальника, його досвіду, оптимальних методик і вдосконалених програм навчання й обміну знаннями в остаточному підсумку прискорює освоєння нових технологій користувачами. А це, у свою чергу, допомагає підприємству швидко досягти цільових фінансових показників і перетворити бізнес.

Перенос спільної роботи в хмару – не завжди дуже складний процес. Логічно почати з первісної оцінки потреб. Які будуть визначальні стимули для організації протягом наступних 3-5 років? Чи зв'язані вони переважно з витратами? Які стратегічні ініціативи, швидше за все, створять потреба в новому поколінні комунікаційних рішень? Яким образом ваші співробітники взаємодіють сьогодні? Які їхні переваги й чого не вистачає? Чи буде процес міграції вашого середовища орієнтований на передачу голосу або миттєвий обмін повідомленнями?

Наступний крок – оцінка технологій. Які базові технології використовуються в мережі, засобах передачі голосу й настільних систем вашої організації? Які постачальники підтримують ці технології? Який ваш план амортизації? Хмара дозволяє впровадити зовсім нові рішення, але вони повинні бути сумісні з існуючою інфраструктурою.

Подумайте про постачальників, з якими у вас уже встановлені довірчі ділові відносини. Можливо, що існують партнери розширили свої пропозиції, щоб надати вам потрібне рішення. Мережні оператори першого рівня (наприклад, Orange, KPN, Telstra), мобільні оператори (наприклад, Vodafone) і провідні постачальники сервісів для спільної роботи з розміщенням на хостингу (наприклад, West IP Communications/InterCall) за останні два роки вивели на ринок кращі у своєму класі послуги UCaaS.

Завжди розумно розширити свої можливості вибору, провівши формальну процедуру запиту пропозицій. Запросите у своїх поточних партнерів відомості про інших постачальників послуг UCaaS. Можливо, вони порекомендують постачальників, що надають кращу підтримку їхніх рішень.

У цілому аналітики вважають, що послуги UCaaS надають відмінні можливості для бізнесу сучасних середніх і великих підприємств за рахунок прискорення розгортання рішень UC і скорочення витрат. В ідеалі потрібно знайти партнера, що орієнтується на тривалу перспективу й зможе допомогти домогтися реального перетворення бізнесу. Ефективне партнерство відкриє шлях до цих можливостей, і не тільки.

На рисунку 1 зображена структура схема системи, з якої видно, які саме сервіси об’єднує UCaaS.

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів уніфікованих комунікацій як сервісу UCaaS. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем уніфікованих комунікацій як сервісу UCaaS; Досліджена система уніфікованих комунікацій як сервісу UCaaS; На основі отриманих результатів досліджень створена програмна реалізація системи уніфікованих комунікацій як сервісу UCaaS. Розроблені під час виконання магістерської роботи алгоритми дозволяють успішно вирішувати завдання уніфікованих комунікацій як сервісу UCaaS. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Дрєєв О.М. Метод прогнозування завантаженості серверу телекомунікаційної мережі / О.М. Дрєєв, О.А. Смірнов, Є.В. Мелешко, О.В. Коваленко // Системи обробки інформації. Випуск 3(101) Том 2. – Х.: ХУПС. – 2012. – С. 181-188.
2. Дрєєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дрєєв, О.П. Доренський // Збірник наукових праць "Системи обробки інформації". – Випуск 8(115). – Х.: ХУПС – 2013. – С. 234-239.
3. Дреев А.Н. Сравнение битовых плотностей при использовании различных методов кодирования информации / А.Н. Дреев, А.А. Смирнов // Системи обробки інформації, 2014, випуск 2 (118), том 2 – Харків: ХУПС – 2014. С 64-66.
4. Дреев А.Н. Повышение вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности / А.Н. Дреев, А.А. Смирнов //«Безпека інформації» Том 21, №1 2015 р. – Київ: НАУ – 2015. – С. 22-28.
5. Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Збірник тез доповідей. Академія внутрішніх військ МВС України

"Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку" 20-21 березня 2013р. – Харків: АВВ. – 2013. С. – 18-19

6. Дреев А.Н. Повышение оперативности доставки данных повышенной востребованности в телекоммуникационных системах и сетях / А.Н. Дреев, А.А. Смирнов, Е.В. Мелешко // Проблеми і перспективи розвитку ІТ-індустрії 25-26 квітня 2013 р. Системи обробки інформації. – Випуск 3 (110). Том 2. – Харків: ХУПС. – 2013. С. – 199.
7. Дрєєв О.М. Середньостатистичний та найімовірніший час доставки багатопакетного повідомлення в телекомунікаційній системі або мережі / О.М. Дрєєв, О.А. Смірнов // V Всеукраїнська науково-практична конференція "Інформатика та системні науки" ІСН – 2014, 13-15 березня 2014 року, м. Полтава – С. 92
8. Дрєєв О.М. Визначення оптимального розміру блоку при бітовому арифметичному кодуванні / О.М. Дрєєв, Г.М. Дрєєва // Збірник тез доповідей Комбінаторні конфігурації та їх застосування, 11-12 квітня 2014 р. – Кіровоград – С. 44
9. Дреев А.Н. Экстраполяция квазипериодических процессов с аддитивными помехами / А.Н. Дреев, А.А. Смирнов // П'ята Міжнародна науково-практична конференція "Інформаційні технології та моделювання в економіці" 15-16 травня 2014 р. – Черкаси – С. 59
10. Дреев А.Н. Статистическая модель передачи многопакетного сообщения в телекоммуникационной системе или сети / А.Н. Дреев, А.А. Смирнов // «Компьютерное моделирование в наукоемких технологиях (КМНТ-2014)» Харьков, 28-31 мая 2014 года – С. 137-140

ЗМІСТ