ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Рівень вищої освіти другий (магістерський)

Галузь знань Інформаційні технології

Розглянуто на засіданні кафедри
Протокол №17 від 29 червня 2022 року

м. Кропивницький – 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Інформаційна безпека в комп'ютерних мережах**
Рік викладання	2022-2023 навчальний рік
Розробники	Смірнова Тетяна Віталіївна, кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету Скрипник Дмитро Анатолійович, DevOps Engineer/DevSecOps Engineer (Security Engineer), MIF Projects Конопліцька-Слободенюк Оксана Костянтинівна, викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
Викладач	Лектор – Смірнова Тетяна Віталіївна, кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/2021/08/30/smirnova-tatiana/ https://www.scopus.com/authid/detail.uri?authorId=57219108044 https://scholar.google.com/citations?hl=ru&user=4t-bqj0AAAAJ https://orcid.org/0000-0001-6896-0612 Асистент –Конопліцька-Слободенюк Оксана Костянтинівна, викладач кафедри кібербезпеки та програмного забезпечення, http://kbpz.kntu.kr.ua/konoplickay-oksana/ https://scholar.google.com.ua/citations?user=I6VRWKcAAAAJ&hl=ru
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20} Мобільні телефони / Viber / Telegram надано у описі курсу «Інформаційна безпека в комп'ютерних мережах» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=617
E-mail:	У описі курсу «Інформаційна безпека в комп'ютерних мережах» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=617
Консультації	*Очні консультації* згідно розкладу консультацій Вівторок та Середа з 14^{20} до 15^{40} *Онлайн консультації* засобами електронної пошти, мессенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні

2. Анотація дисципліни

Курс «Інформаційна безпека в комп'ютерних мережах» призначений для набуття теоретичних знань та практичних навичок з питань забезпечення інформаційної безпеки в комп'ютерних мережах. Включає в себе набуття наступних теоретичних знань: загальні відомості про атаки на програмне забезпечення та дані у комп'ютерних системах та мережах; міжмережеві екрани (фаєрволи, брандмауери); віртуальні приватні мережі (VPN); технології тунелювання; архітектура безпеки для IP (IPSec); протокол SSL/TLS; безпека бездротових з'єднань; системи виявлення вторгнень (IDS-системи); системи протидії вторгненням (IPS-системи); реалізація мережевої безпеки у організаціях; безпека банківських електронних платіжних систем; електронна комерція: вимоги до безпеки; резервування інформації та компонентів інформаційних та комп'ютерних систем різного призначення; відновлення функціонування комп'ютерних систем та мереж після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; моніторинг процесів функціонування комп'ютерних систем та мереж; система візуалізації та управління подіями (SIEM); аналіз подій; проектування, створення, супровід КСЗІ комп'ютерних систем та мереж; оцінка захищеності

інформації в комп'ютерних системах та мережах; управління інформаційною та / або кібербезпекою комп'ютерних систем та мереж. Та набуття наступних практичних навичок й вмінь, які полягають у можливості програмно реалізовувати наступні проекти: Реалізація мережевого антивірусу; Реалізація міжмережевого екрану; Реалізація сніффера; Реалізація протоколу IPSec; Реалізація протоколу TLS/SSL; Реалізація системи виявлення вторгнень. Відповідно означене є предметом навчальної дисципліни «Інформаційна безпека в комп'ютерних мережах» як освітньої компоненти ОП «Комп'ютерні науки» другого (магістерського) рівня вищої освіти.

3. Мета і завдання дисципліни

Метою викладання дисципліни «Інформаційна безпека в комп'ютерних мережах» є формування у здобувачів вищої освіти ґрунтовних теоретичних знань, практичних умінь та навичок, необхідних для застосування в професійній діяльності у сфері забезпечення інформаційної безпеки в комп'ютерних мережах.

Основними **завданнями** вивчення дисципліни є формування наступних **компетенцій магістра з комп'ютерних наук**:

– СК05. Здатність розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.

– СК07. Здатність розробляти програмне забезпечення відповідно до сформульованих вимог з урахуванням наявних ресурсів та обмежень.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

5. Результати навчання

У результаті вивчення дисципліни студент повинен забезпечити наступні **програмні результати навчання**:

– РН9. Розробляти алгоритмічне та програмне забезпечення для аналізу даних (включно з великими).

– РН10. Проектувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Денна форма навчання	Заочна форма навчання
	Кількість годин	Кількість годин
Рекомендації щодо семестру вивчення	2 семестр	2 семестр
Спеціальність	122 «Комп'ютерні науки»	122 «Комп'ютерні науки»
Кількість кредитів / годин	4/120	4/120
Кількість змістових модулів	2	2
Нормативна / вибіркова	вибіркова	вибіркова
лекції	36	4
лабораторні	18	2
самостійна робота	66	114
Вид підсумкового контролю : залік	0	0

7. Пререквізити

Враховуючи послідовність накопичення знань та інформації, дисципліна вивчається після викладання наступних дисциплін: «Теорія захисту інформації», «Проектування комп'ютерних систем та мереж».

8. Технічне і програмне забезпечення / обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти.

9. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

10. Навчально-методична карта дисципліни

Тиждень, дата, академічні години	**Тема, основні питання** *(розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)*	**Форма діяльності (заняття) /формат**	**Матеріали**	**Література, інформаційні ресурси**	**Самостійна робота Завдання, обсяг годин**	**Вага оцінки**	**Термін виконання**
Змістовний модуль 1. Дослідження атак на комп'ютерні мережі, VPN, IPSec та SSL/TLS, безпека бездротових з'єднань, IDS–системи							
Тиж.1 (за розкладом) (2 год.)	**Тема 1. Атаки на програмне забезпечення та засоби протидії атакам** Загальні відомості про атаки на програмне забезпечення та дані у комп'ютерних системах та мережах. Моделі атак. Етапи реалізації атак. DDoS – комп'ютерні атаки. Технології їхнього виявлення. Захист. Варіанти реакцій на виявлену атаку.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації атак на програмне забезпечення та дані у комп'ютерних системах та мережах. (2 год.)	4 бали	Самостійна робота до 2 тижня включно
Тиж.2 (за розкладом) (2 год.)	**Тема 1. Атаки на програмне забезпечення та засоби протидії атакам** Міжмережеві екрани (фаєрволи, брандмауери). Технології міжмережевих екранів. Стани TCP-з'єднання. Класифікація міжмережевих екранів. Фільтрування пакетів. Пакетні фільтри з аналізом стану.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до протидії атакам на програмне забезпечення та дані у комп'ютерних системах та мережах.. (2 год.)	4 бали	Самостійна робота до 2 тижня включно
Тиж.1,2 (за розкладом) (2 год.)	**Тема 1. Атаки на програмне забезпечення та засоби протидії атакам** Реалізація мережевого антивірусу. Ч.1.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати мережевий антивірус. (3 год.)	4 бали	Самостійна робота до 2 тижня включно

Тиж.3 (за розкладом) (2 год.)	**Тема 2. Віртуальні приватні мережі** Віртуальні приватні мережі (VPN). Визначення віртуальних приватних мереж. Розгортання користувальницьких віртуальних приватних мереж. Розгортання вузлових мереж VPN. Поняття стандартних технологій функціонування VPN. Сервер VPN. Алгоритми шифрування. Система автентифікації. Протокол VPN. Типи систем VPN	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації VPN (2 год.)	4 бали	Самостійна робота до 4 тижня включно
Тиж.4 (за розкладом) (2 год.)	**Тема 2. Віртуальні приватні мережі** Технології тунелювання. Протокол GRE. Протоколи канального рівня. Протокол Point-to-Point Protocol (PPP). Діаграма станів. Встановлення каналу. Автентифікація. Протокол автентифікації Challenge-Handshake (CHAP). Розширення Microsoft PPP CHAP. Конфігурування LCP. Протокол шифрування MPPE Microsoft. Протокол конфігурування IP – IPCP.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до технологій тунелювання. (2 год.)	4 бали	Самостійна робота до 4 тижня включно
Тиж.3,4 (за розкладом) (2 год.)	**Тема 1. Атаки на програмне забезпечення та засоби протидії атакам** Реалізація мережевого антивірусу. Ч.2.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати мережевий антивірус. (3 год.)	4 бали	Самостійна робота до 4 тижня включно

Тиж.5 (за розкладом) (2 год.)	**Тема 3. IPSec та SSL/TLS** Архітектура безпеки для IP (IPSec). Призначення сімейства протоколів IPSec. Протоколи захисту трафіку й поняття безпечної асоціації. Поняття домену IPSec. Визначення умов, при яких виконується. Можливі топології IPSec. Ступінь деталізації керування трафіком. Протокол ESP	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити існуюче застосування IPSec. (2 год.)	4 бали	Самостійна робота до 6 тижня включно
Тиж.6 (за розкладом) (2 год.)	**Тема 3. IPSec та SSL/TLS** Протокол SSL/TLS. Протокол Запису. Стан з'єднання. Обчислення ключів. HMAC і псевдовипадкова функція. Протокол Рукостискання. Протокол зміни шифрування. Перевірка цілісності за допомогою сертифіката клієнта. Додавання додаткових можливостей до протоколу. Переговори про максимальну довжину фрагмента.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити існуюче застосування SSL/TLS. (2 год.)	4 бали	Самостійна робота до 6 тижня включно
Тиж.5,6 (за розкладом) (2 год.)	**Тема 1. Атаки на програмне забезпечення та засоби протидії атакам** Реалізація міжмережевого екрану	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати міжмережевий екран (3 год.)	4 бали	Самостійна робота до 8 тижня включно

Тиж.7 (за розкладом) (2 год.)	**Тема 4. Безпека бездротових з'єднань та системи виявлення вторгненнь.** Безпека бездротових з'єднань. Сучасні бездротові технології. Стандартні архітектури. Безпека передачі даних. WPA і WPA2. Протокол 802.1X: контроль доступу в мережу за портами. Питання безпеки бездротових з'єднань. Виявлення WLAN. Прослуховування. Активні атаки. Безпека точки доступу. Безпека передачі даних. Безпека робочої станції. Безпека сайту.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до безпеки бездротових з'єднань (2 год.)	4 бали	Самостійна робота до 8 тижня включно
Тиж.8 (за розкладом) (2 год.)	**Тема 4. Безпека бездротових з'єднань та системи виявлення вторгненнь.** Системи виявлення вторгнень (IDS-системи). Визначення типів систем виявлення вторгнень. HIDS. NIDS. Установка IDS. Керування IDS. Дослідження підозрілих подій. Розгортання мережевої IDS	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації IDS -систем (2 год.)	4 бали	Самостійна робота до 8 тижня включно
Тиж.7,8 (за розкладом) (2 год.)	**Тема 1. Атаки на програмне забезпечення та засоби протидії атакам** Реалізація сніффера. Ч.1.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати сніффер. (3 год.)	6 балів	Самостійна робота до 8 тижня включно
Максимальна кількість балів за змістовим модулем 1						50 балів	

Змістовний модуль 2. Системи протидії вторгненням та реалізація мережевої безпеки у організаціях, безпека банківських електронних платіжних систем, електронна комерція: вимоги до безпеки, резервування та відновлення інформації та компонентів інформаційних та комп'ютерних систем різного призначення, моніторинг процесів функціонування та проектування, створення, супровід КСЗІ комп'ютерних систем та мереж, оцінка захищеності інформації та управління інформаційною та / або кібербезпекою комп'ютерних систем та мереж							
Тиж.9 (за розкладом) (2 год.)	**Тема 5 Системи протидії вторгненням та реалізація мережевої безпеки у організаціях** Системи протидії вторгненням (IPS-системи). Запобігання вторгнень. Механізми ухвалення рішення IPS. Механізми керування IPS: віддалені й централізовані. Можливість інтеграції IPS з іншими системами. Проблеми, пов'язані з виявленням вторгнень. Ключові тенденції розвитку систем виявлення вторгнень	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації IPS-систем (2 год.)	3 бали	Самостійна робота до 10 тижня включно
Тиж.10 (за розкладом) (2 год.)	**Тема 5 Системи протидії вторгненням та реалізація мережевої безпеки у організаціях** Реалізація мережевої безпеки у організаціях. Адміністративна безпека. Політики й процедури. Навчання співробітників. Плани виходу із критичних ситуацій. Обробка інцидентів. Плани проектів безпеки. Захист від шкідливого коду. Автентифікація. Аудит. Фізична безпека. ISO 17799.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації мережевої безпеки у організаціях (2 год.)	3 бали	Самостійна робота до 10 тижня включно

Тиж.9,10 (за розкладом) (2 год.)	**Тема 1. Атаки на програмне забезпечення та засоби протидії атакам** Реалізація сніффера. Ч.2.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати сніффер. (3 год.)	3 бали	Самостійна робота до 10 тижня включно
Тиж.11 (за розкладом) (2 год.)	**Тема 6. Безпека банківських електронних платіжних систем. Електронна комерція: вимоги до безпеки.** Безпека банківських електронних платіжних систем. Безпека електронних платіжних систем. Види банківських карт. Персоналізація**.** Авторизація**.** Крадіжки грошей із пластикових карт із використанням банкоматів.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації безпеки банківських електронних платіжних систем (2 год.)	3 бали	Самостійна робота до 12 тижня включно
Тиж.12 (за розкладом) (2 год.)	**Тема 6. Безпека банківських електронних платіжних систем. Електронна комерція: вимоги до безпеки.** Електронна комерція: вимоги до безпеки. Служби електронної комерції. Продаж товарів. Питання взаємин "компанія-клієнт". Питання взаємин "компанія-компанія". Збитки внаслідок простою. Реалізація безпеки клієнтської сторони. Реалізація безпеки серверної частини. Реалізація безпеки застосунків. Сканування уразливостей. Розробка архітектури сайту електронної комерції.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації безпеки електронної комерції (2 год.)	3 бали	Самостійна робота до 12 тижня включно

Тиж.11,12 (за розкладом) (2 год.)	**Тема 3. IPSec та SSL/TLS** Реалізація протоколу IPSec.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати протокол IPSec. (3 год.)	3 бали	Самостійна робота до 12 тижня включно
Тиж.13 (за розкладом) (2 год.)	**Тема 7. Резервування та відновлення інформації та компонентів інформаційних та комп'ютерних систем різного призначення.** Резервування інформації та компонентів інформаційних та комп'ютерних систем різного призначення.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до резервування інформації та компонентів інформаційних та комп'ютерних систем різного призначення (2 год.)	3 бали	Самостійна робота до 14 тижня включно
Тиж.14 (за розкладом) (2 год.)	**Тема 7. Резервування та відновлення інформації та компонентів інформаційних та комп'ютерних систем різного призначення.** Відновлення функціонування комп'ютерних систем та мереж після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до відновлення функціонування комп'ютерних систем та мереж після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження (2 год.)	3 бали	Самостійна робота до 14 тижня включно
Тиж.13,14 (за розкладом) (2 год.)	**Тема 3. IPSec та SSL/TLS** Реалізація протоколу SSL/TLS	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати протокол SSL/TLS (3 год.)	3 бали	Самостійна робота до 14 тижня включно

Тиж.15 (за розкладом) (2 год.)	**Тема 8. Моніторинг процесів функціонування та проектування, створення, супровід КСЗІ комп'ютерних систем та мереж** Моніторинг процесів функціонування комп'ютерних систем та мереж. Система візуалізації та управління подіями (SIEM). Аналіз подій	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до моніторингу процесів функціонування комп'ютерних систем та мереж (2 год.)	3 бали	Самостійна робота до 16 тижня включно
Тиж.16 (за розкладом) (2 год.)	**Тема 8. Моніторинг процесів функціонування та проектування, створення, супровід КСЗІ комп'ютерних систем та мереж** Проектування, створення, супровід КСЗІ комп'ютерних систем та мереж.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до проектування, створення, супроводу КСЗІ комп'ютерних систем та мереж (2 год.)	3 бали	Самостійна робота до 16 тижня включно
Тиж.15,16 (за розкладом) (2 год.)	**Тема 5 Системи протидії вторгненням та реалізація мережевої безпеки у організаціях** Реалізація системи виявлення та протидії вторгненням. Ч.1.	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати систему виявлення вторгнень. (3 год.)	3 бали	Самостійна робота до 16 тижня включно
Тиж.17 (за розкладом) (2 год.)	**Тема 9. Оцінка захищеності інформації та управління інформаційною та / або кібербезпекою комп'ютерних систем та мереж** Оцінка захищеності інформації в комп'ютерних системах та мережах.	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації безпеки електронної комерції (2 год.)	3 бали	Самостійна робота до 18 тижня включно

Тиж.18 (за розкладом) (2 год.)	**Тема 9. Оцінка захищеності інформації та управління інформаційною та / або кібербезпекою комп'ютерних систем та мереж** Управління інформаційною та / або кібербезпекою комп'ютерних систем та мереж	Лекція / *Face to face*	Презентація	[1-16] [31]	Самостійно опрацювати матеріал: Дослідити сучасні підходи до реалізації безпеки електронної комерції (2 год.)	3 бали	Самостійна робота до 18 тижня включно
Тиж.17,18 (за розкладом) (2 год.)	**Тема 5 Системи протидії вторгненням та реалізація мережевої безпеки у організаціях** Реалізація системи виявлення та протидії вторгненням. Ч2	Лабораторна робота / *Face to face*	Методичні рекомендації	[29, 30, 31]	Самостійно опрацювати матеріал: Реалізувати систему протидії вторгненням. (6 год.)	8 балів	Самостійна робота до 18 тижня включно
Максимальна кількість балів за змістовим модулем 2						50 балів	
Максимальна кількість балів за залік						0 балів	

11. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: залік.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Інформаційна безпека в комп'ютерних мережах» здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних робіт), для оцінювання якої призначається 100 балів, та заліку, максимальна оцінка за який складає 0 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Інформаційна безпека в комп'ютерних мережах»

Поточний контроль та самостійна робота																													
Змістовий модуль 1												Змістовий модуль 2															Залік	Сума
Т1			Т2			Т3			Т4			Т5			Т6			Т7			Т8			Т9				
Л1	Л2	ЛР1	Л3	Л4	ЛР1	Л5	Л6	ЛР2	Л7	Л8	ЛР3	Л9	Л10	ЛР3	Л11	Л12	ЛР4	Л13	Л14	ЛР5	Л15	Л16	ЛР6	Л17	Л18	ЛР6		
4	4	4	4	4	4	4	4	4	4	4	6	3	3	3	3	3	3	3	3	3	3	3	3	3	3	8		
50												50															0	100

Примітка: Т1, Т2,…,Т7 – тема, Л – теоретичні (лекційні) заняття, ЛР – лабораторні заняття

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
90-100	A	відмінно
82-89	B	добре
74-81	C	
64-73	D	задовільно
60-63	E	
35-59	FX	незадовільно з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, лабораторні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті:

оцінку «відмінно» (90-100 балів, A) – заслуговує студент, який:

– всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;

– вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у нестандартних ситуаціях;

– засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою;

– засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває;

– вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію;

– самостійно визначає окремі цілі власної навчальної діяльності, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

оцінку « добре» (82-89 балів, B) – заслуговує студент, який:

– повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях;

– має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування;

– під час відповіді допустив деякі неточності, які самостійно виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, C) – заслуговує студент, який:

– в загальному роботу виконав, але відповідає на заліку з певною кількістю помилок;

– вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати на практиці, контролювати власну діяльність;

– опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) – заслуговує студент, який:

– знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

– виконує завдання, але при рішенні допускає значну кількість помилок;
– ознайомлений з основною літературою, яка рекомендована програмою;
– допускає на заняттях чи заліку помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

оцінку «задовільно» (60-63 бали, E) – заслуговує студент, який:

– володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) – виставляється студенту, який:

– виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінку «незадовільно» (35 балів, F) – виставляється студенту, який:

– володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім;
– допускає грубі помилки при виконанні завдань, передбачених програмою;
– не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

12. Рекомендована література

Базова

1. Смірнова Т.В., Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с. Режим доступу: http://dspace.kntu.kr.ua/jspui/handle/122456789/9799
2. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
3. Смірнов О.А., Кавун С.В., Доренський О.П., Вялкова В.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 151 с.
4. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
5. Смірнов О.А., Кавун С.В., Столбов В.Ф., Мелешко Є.В. Основи інформаційної безпеки. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. С.В. Кавуна. Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5760. – Кіровоград: КНТУ 2012. – 442 с.
6. Смірнов О.А., Віхрова Л.Г., Осадчий С.І., Ковтун В.Ю., Мелешко Є.В. Основи захисту інформації. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.050201 «Системна інженерія». За ред. О.А. Смірнова Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки України від 16.12.2010 року № 1/11-11486. – Кіровоград: КНТУ 2011. – 322 с.

7. Смірнов О.А., Кузнецов О.О., Євсеєв С.П., Мелешко Є.В., Король О.Г. Методи та алгоритми симетричної криптографії. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.О. Кузнецова**.** Гриф "Навчальний посібник" надано у відповідності з листом Міністерства освіти і науки, молоді та спорту України від 26.04.2012 року № 1/11-5762. – Кіровоград: КНТУ 2012. – 315 с.
8. Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
9. Остапов С. Е. Технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
10. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 13: Захист інформації в системах електронного урядування / [О.М. Хоша ба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.
11. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 с.
12. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 с.
13. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 с.
14. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 с.
15. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 с.
16. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 с.

Допоміжна

17. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399. **(Scopus).** Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85133613188&origin=resultslist&sort=plf-f&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1
18. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184. **(Scopus).** Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85118101973&origin=AuthorNamesList&txGid=9fba77a9424db54ff3b099e4400c22bb
19. Smirnova, T., Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., «Biometric authentication using convolutional neural networks». Lecture Notes in Networks and SystemsVolume 152, 2021, Pages 85-98. (Scopus). Режим доступу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85090914783&origin=resultslist
20. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., «Метод розрахунку критичності галузевих інформаційно-телекомунікаційних систем». *Наукоємні технології* № 2(54), 2022. С. 94-104. Режим доступу: https://jrnl.nau.edu.ua/index.php/SBT/article/view/16757 **(Фахове видання. Категорія «Б»)**
21. Смірнова Т.В., Гнатюк С.О., Юдін О.Ю., Сидоренко В.М., Жаксигулова Д.Д., «Експериментальне дослідження моделі розрахунку кількісного критерію оцінювання захищеності інформаційно-телекомунікаційних систем критичної інфраструктури держави» *Кібербезпека: освіта, наука, техніка*. № 4(16). 2022. С. 6-18. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/359/298 **(Фахове видання. Категорія «Б»)**

22. Смірнова Т.В., Якименко Н.М., Смірнов О.А., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022. Режим доступу: http://journals.khnu.km.ua/vestnik/?cat=65 **(Фахове видання. Категорія «Б»)**
23. Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., Смірнов О.А. «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89. Режим доступу: http://journals.nupp.edu.ua/sunz/article/view/2449/1918 **(Фахове видання. Категорія «Б»)**
24. Смірнова Т.В., Якименко Н.М., Улічев О.С., Конопліцька-Слободенюк О.К., Смірнов С.А., «Дослідження лінійних перетворень запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Кібербезпека: освіта, наука, техніка*. № 3(15). С. 85-92. 2022. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/337 **(Фахове видання. Категорія «Б»)**
25. Смірнова Т.В., Бурмак Ю.А., Улічев О.С., Усік П.С., Доренський О.П., «Стійка функція шифрування удосконаленого модуля криптографічного захисту інформації в інформаційно-комунікаційних системах» *Кібербезпека: освіта, наука, техніка*. № 1(13). С. 183-201. 2021. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/346 **(Фахове видання. Категорія «Б»)**
26. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Бурмак Ю.А., Оспанова Д.М., «Удосконалений модуль криптографічного захисту інформації в сучасних інформаційно-комунікаційних системах та мережах». *Кібербезпека: освіта, наука, техніка*. № 2(14). С. 176-185. 2021. Режим доступу: https://csecurity.kubg.edu.ua/index.php/journal/article/view/329 **(Фахове видання. Категорія «Б»)**
27. Смірнова Т.В., Смірнов О.А., Смірнов С.А., Поліщук Л.І., Конопліцька-Слободенюк О.К. Метод формування антивірусного захисту даних з використанням безпечної маршрутизації метаданих. Кібербезпека: освіта, наука, техніка. – Том 3 № 3. – Київ: КУ ім. Бориса Грінченка. – 2019. – С. 63-87. https://doi.org/10.28925/2663-4023.2019.3.6387 Режим доступу: http://nbuv.gov.ua/UJRN/cest_2019_3_7 **(Фахове видання).**
28. Смірнова Т.В., Смірнов О.А., Смірнов С.А., Поліщук Л.І., Конопліцька-Слободенюк О.К.,. GERT-моделі технології хмарного антивірусного захисту. Кібербезпека: освіта, наука, техніка. – Том 2 № 2. – Київ: КУ ім.. Бориса Грінченка. – 2018. – С. 7-30. https://doi.org/10.28925/2663-4023.2018.2.730 Режим доступу: http://nbuv.gov.ua/UJRN/cest_2018_2_3 **(Фахове видання).**

Методичне забезпечення

29. Смірнова Т.В., Буравченко К.О., Смірнов О.А., Конопліцька-Слободянюк О.К., Смірнов С.А. «Інформаційна безпека в комп'ютерних мережах». Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 69 с.
30. Смірнова Т.В., Буравченко К.О., Смірнов О.А., Конопліцька-Слободянюк О.К., Смірнов С.А. «Інформаційна безпека в комп'ютерних мережах». Методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 69 с.

Інформаційні ресурси

31. Курс «Інформаційна безпека в комп'ютерних мережах» на сервері дистанційної освіта ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=617
32. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/

33. Онлайн-курси Coursera. – URL: https://www.coursera.org
34. Академія Cisco. – URL: https://www.netacad.com
35. Он-лайн ресурс з інформаційних технологій. – URL:https://habr.com
36. Он-лайн ресурс з інформаційних технологій. – URL:https://dou.ua/
37. Пошукова система. – URL:https://www.google.com/
38. Он-лайн ресурс перегляду відеоуроків.– URL:https://www.youtube.com