ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
КРИПТОАНАЛІЗ

Освітньо-професійна програма «Комп'ютерна інженерія»
першого (бакалаврського) рівня вищої освіти

Спеціальність 123 Комп'ютерна інженерія
Галузь знань 12 Інформаційні технології

Розглянуто на засіданні кафедри
Протокол №13 від 31 березня 2022 року

м. Кропивницький – 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	КРИПТОАНАЛІЗ
Рік викладання	2022-2023 навчальний рік
Викладач	Якименко Наталія Миколаївна, доцент, кандидат фізико-математичних наук, доцент кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/yakymenko-natalia/
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8.30 до 14.20 Мобільні телефони / Telegram надано у описі курсу «Криптоаналіз» на сайті дистанційної освіти ЦНТУ.
E-mail:	it-kntu@ukr.net
Консультації	Очні консультації згідно розкладу консультацій Онлайн консультації: засобами електронної пошти, мессенджерів (Viber / Telegram) у робочі дні
Курс у системі дистанційного навчання	http://moodle.kntu.kr.ua/course/view.php?id=672

2. Анотація до дисципліни

Дисципліна «Криптоаналіз» належить до переліку вибіркових навчальних дисциплін галузі знань 12 «Інформаційні технології».
Курс «Криптоаналіз» спрямований на формування навиків розшифровки кодованих повідомлень без вказівки ключа з метою:
1) зламу криптографічних систем безпеки, щоб отримати доступ до зашифрованих повідомлень, якщо втрачено ключ шифру;
2) визначення вразливостей в алгоритмах кодування для їх поліпшення;
3) вивчення або аналізу інформаційних систем для виявлення прихованих помилок.
Фактично після вивчення даного курсу студент отримує знання та навички «білого» хакера.

3. Мета і завдання дисципліни

Мета вивчення дисципліни:

1) формування компетентностей, необхідних для підготовки фахівців, здатних використовувати і впроваджувати технології інформаційної безпеки та кібербезпеки;
2) розвиток у студентів фахового стилю мислення;

3) надання глибоких та міцних знань про об’єкти інформатизації, технології забезпечення безпеки інформації, процеси управління інформаційною та кібербезпекою об’єктів, що підлягають захисту, необхідних для подальшого вивчення спеціальних дисциплін та для практичної інженерної діяльності;
4) вироблення у студентів вміння використовувати набуті знання при використанні і впровадженні технологій інформаційної та кібербезпеки;
5) закласти математичний та термінологічний фундамент в галузі криптології;
6) вироблення у студентів вміння правильно проводити аналіз загроз безпеці інформації;
7) вироблення у студентів вміння використовувати основні методи, механізми, алгоритми та протоколи криптографічного захисту інформації в інформаційно-комунікаційних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення загроз,
8) вироблення у студентів вміння проведення криптографічного аналізу з боку потенційних порушників.

Завдання вивчення дисципліни полягає в формуванні компетентностей, важливих для особистісного розвитку фахівців та їхньої конкурентоспроможності на сучасному ринку праці:

- Здатність до пошуку, оброблення та аналізу інформації;
- Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, поєднуючи із лабораторними роботами.

Формат очний (offline / Face to face)

Для заочної форми навчання:

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

5. Результати навчання

У результаті вивчення навчальної дисципліни «Криптоаналіз» студент матиме наступні програмні результати навчання:

- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

- аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно-телекомунікаційних системах;
- аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Рекомендації щодо семестру вивчення	6 семестр
Спеціальність	125 Кібербезпека
Кількість кредитів / годин	3 / 90
Кількість змістових модулів	2
Нормативна / вибіркова	Вибіркова
Лекції	28
Лабораторні	14
Самостійна робота	48
Вид підсумкового контролю: залік	-

7. Пререквізити

Ефективність засвоєння змісту дисципліни «Криптоаналіз» значно підвищиться, якщо студент попередньо опанував матеріал таких дисциплін: «Вища математика(Теорія ймовірності та математична статистика)», «Спеціальні розділи математики для інформаційної безпеки», «Основи криптографічного захисту інформації», «Технології програмування».

8. Технічне й програмне забезпечення/обладнання

Для викладання дисципліни «Криптоаналіз» застосовується матеріально-технічна база кафедри кібербезпеки та програмного забезпечення. Лекційні заняття проводяться в аудиторіях, обладнаних мультимедійним проектором. Лабораторні роботи виконуються у спеціалізованих комп’ютерних лабораторіях 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

Організація освітнього процесу.

Викладач і здобувачі повинні дотримуватися вимог Положення про організацію освітнього процесу ЦНТУ, Кодексу академічної доброчесності ЦНТУ, Положення про дотримання академічної доброчесності НПП та здобувачами вищої освіти, інших нормативних актів університету http://www.kntu.kr.ua/?view=univer&id=4 .

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

Відвідання 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

Недопустимими є: запізнення на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

10. Навчально - методична карта дисципліни

Тиждень, дата, години	Тема, основні питання	Форма діяльності (заняття) /формат	Матеріали	Література, інформаційні ресурси	Завдання, години	Вага оцінки	Термін виконання
Змістовий модуль 1. Основи криптоаналізу							
Тиждень 1 (за розкладом) 2 год.	Тема 1. Основи криптології, криптографії та криптоаналізу. Загальні відомості про класичну криптологію, криптографію та криптографічний аналіз. Історія розвитку криптології. Основні визначення, використовувані в криптології. Основи теорії засекреченого зв'язку К. Шеннона. Класифікація методів шифрування повідомлень. Криптографічний аналіз. Атака на зашифрований текст. Атака на відомий вхідний текст. Атака на обраний вхідний текст. Атака на обраний зашифрований текст.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,3 Допоміжна 1,2,3,6 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 1. Виконати завдання СРС №1. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 1 тижня. 2 год.	4	Навчальний тиждень 1

Тиждень 2 (за розкладом) 2 год.	Тема 2. Традиційні історичні шифри та атаки на них. Шифри підстановки та атаки на них. Шифри перестановки та атаки на них.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,3 Допоміжна 1,2,3,6 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 2. Виконати завдання СРС №2. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 2 тижня. 2 год.	4	Навчальний тиждень 2
Тиждень 1-2 (за розкладом) 2 год.	Тема 1-2. Традиційні історичні шифри та атаки на них. Лабораторна робота №1. Криптоаналіз шифрів стовпцевої перестановки та подвійної перестановки. Криптоаналіз шифрів простої заміни.	Лабораторна / Face to face	Методичні рекомендації до виконання лабораторних робіт	Базова 1,3 Інформаційні ресурси 1,2,3 Методичне забезпечення 1	Самостійно опрацювати теоретико-практичні питання до лабораторної роботи №1. 2 год.	4	За розкладом лабораторних занять
Тиждень 3 (за розкладом) 2 год.	Тема 3. Сучасні блокові шифри та складені шифри. Шифри підстановки та транспозиції. Блокові шифри як групові математичні перестановки. Розсіювання й перемішування. Раунди. Два класи складених шифрів. Атаки на блокові шифри. Диференціальний криптографічний аналіз. Лінійний криптографічний аналіз.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,3,8-11 Допоміжна 1,2,3,6 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 3. Виконати завдання СРС №3. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 3 тижня. 2 год.	4	Навчальний тиждень 3
Тиждень 4 (за розкладом) 2 год.	Тема 4. Потокові шифри. Загальні відомості про потокові шифри. Класифікація потокових шифрів. Криптографічна стійкість потокового шифру A5. Криптографічна стійкість потокового шифру RC4.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,3 Допоміжна 1,2,3,6 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 4. Виконати завдання СРС №4. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 4 тижня. 2 год.	4	Навчальний тиждень 4
Тиждень 3-4 (за розкладом) 2 год.	Тема 3-4. Сучасні блокові шифри та потокові шифри. Лабораторна робота №2. Криптоаналіз шифрів Цезаря. Криптоаналіз шифрів Віжінера.	Лабораторна / Face to face	Методичні рекомендації до виконання лабораторних робіт	Базова 1,3 Інформаційні ресурси 1,2,3 Методичне забезпечення 1	Самостійно опрацювати теоретико-практичні питання до лабораторної роботи №2. 3 год.	4	За розкладом лабораторних занять

Тиждень 5 (за розкладом) 2 год.	Тема 5. Стандарт симетричного алгоритму блокового шифрування даних DATA ENCRIPTION STANDARD. Аналіз алгоритму. Уразливі місця. Уразливість ключа шифру. Безпека шифру. Атака “грубої сили”. Диференціальний криптографічний аналіз. Лінійний криптографічний аналіз.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,3,8 Допоміжна 1,2,3,6,14 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 5. Виконати завдання СРС №5. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 5 тижня. 2 год.	5	Навчальний тиждень 5
Тиждень 6 (за розкладом) 2 год.	Тема 6. Симетричний алгоритм блокового шифрування даних INTERNATIONAL DATA ENCRYPTION ALGORITHM Принципи побудови алгоритму. Структура алгоритму шифрування даних. Безпека шифру. Аналіз шифру IDEA. Уразливість ключа шифру.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,3 Допоміжна 1,2,3,6,14 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 6. Виконати завдання СРС №6. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 6 тижня. 2 год.	5	Навчальний тиждень 6
Тиждень 5-6 (за розкладом) 2 год.	Тема 5-6. Криптографічний аналіз симетричного алгоритму блокового шифрування даних. Лабораторна робота №3. Дослідження захисту комп’ютерних систем за допомогою симетричних криптографічних шифрів.	Лабораторна / Face to face	Методичні рекомендації до виконання лабораторних робіт	Базова 1,3,9 Інформаційні ресурси 1,2,3 Методичне забезпечення 1	Самостійно опрацювати теоретико-практичні питання до лабораторної роботи №3. 3 год.	4	За розкладом лабора-торних занять
Тиждень 7 (за розкладом) 2 год.	Тема 7. Стандарт симетричного алгоритму блокового шифрування даних ДСТУ ГОСТ 28147:2009. Принципи побудови алгоритму. Аналіз шифру. Криптографічна стійкість. Зауваження до архітектури. Вимоги до якості ключової інформації та джерела ключів. Нестандартне використання стандарту.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,3 Допоміжна 1,2,3,5,6 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 7. Виконати завдання СРС №7. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 7 тижня. 2 год.	4	Навчальний тиждень 7
Тиждень 8 (за розкладом) 2 год.	Тема 8. Методи криптоаналізу асиметричних криптосистем. Методи зламу криптографічних систем, заснованих на дискретному логарифмуванні. Метод “крок немовляти, крок велетня”. Алгоритм обчислення порядку.	Лекція / Face to face	Конспект лекцій / презентація	Базова 1,2,3 Допоміжна 1,2,3,5,6 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 8. Виконати завдання СРС №8. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 8 тижня. 2 год.	4	Навчальний тиждень 8

Тиждень 7-8 (за розкладом) 2 год.	Тема 7-8. Методи криптоаналізу асиметричних криптосистем.. Лабораторна робота №4. Дослідження захисту комп'ютерних систем за допомогою асиметричних криптографічних шифрів	Лабораторна / Face to face	Методичні рекомендації до виконання лабораторних робіт	Базова 1,3 Інформаційні ресурси 1,2,3 Методичне забезпечення 1	Самостійно опрацювати теоретико-практичні питання до лабораторної роботи №4. 3 год.	4	За розкладом лабора-торних занять
Максимальна кількість балів за змістовим модулем 1						50	
Змістовий модуль 2. Сучасні підходи до криптоаналізу							
Тиждень 9 (за розкладом) 2 год.	Тема 9. Методи та алгоритми криптоаналізу криптографічних перетворень в групі точок еліптичних кривих. Еліптичні криві над простим полем Галуа GF (p). Алгоритм обчислення точок еліптичної кривої. Приклад додавання точок еліптичної кривої. Алгоритм обчислення порядку точки еліптичної кривої. Алгоритм скалярного множення на еліптичній кривій.	Лекція / Face to face	Конспект лекцій / презентація	Базова 5,6,7 Допоміжна 4,5,14 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 9. Виконати завдання СРС №9. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 9 тижня. 2 год.	5	Навчальний тиждень 9
Тиждень 10 (за розкладом) 2 год.	Тема 10. Квантова криптографія та криптоаналіз. Що таке квантова криптографія? Протокол передачі з використанням квантової криптографії. Злам квантової системи. Квантово-оптична система Підключай та працюй (Plug & Play). Публічна інформація про квантовий криптоаналіз.	Лекція / Face to face	Конспект лекцій / презентація	Базова 5,6,7 Допоміжна 4,5 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 10. Виконати завдання СРС №10. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 10 тижня. 2 год.	5	Навчальний тиждень 10
Тиждень 9-10 (за розкладом) 2 год.	Тема 9-10. Методи та алгоритми криптоаналізу криптографічних перетворень в групі точок еліптичних кривих. Лабораторна робота №5. Криптоаналіз криптографічних перетворень в групі точок еліптичних кривих.	Лабораторна / Face to face	Методичні рекомендації до виконання лабораторних робіт	Базова 5,6,7 Допоміжна 4,5 Інформаційні ресурси 1,2,3 Методичне забезпечення 1	Самостійно опрацювати теоретико-практичні питання до лабораторної роботи №5. 3 год.	6	За розкладом лабора-торних занять

Тиждень 11 (за розкладом) 2 год.	Тема 11. Методи стеганоаналізу для графічних файлів. Практична стійкість стеганосистем. Методи стеганоаналізу контейнерів-зображень. Сигнатурні і схемні методи аналізу. Метод візуального аналізу графічних файлів. Метод візуального аналізу бітових зрізів. Метод аналізу гістограм, побудованих за частотами елементів зображення.	Лекція / Face to face	Конспект лекцій / презентація	Базова 5 Допоміжна 5, 15-17 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 11. Виконати завдання СРС №11. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 11 тижня. 2 год.	5	Навчальний тиждень 11
Тиждень 12 (за розкладом) 2 год.	Тема 12. Оцінки практичної стійкості модифікацій нових стандартів блокового шифрування відносно цілочисельного різницевого криптоаналізу. Побудова оцінок практичної стійкості ГОСТ-подібного алгоритму. Побудова оцінок практичної стійкості «Калина»-подібних алгоритмів.	Лекція / Face to face	Конспект лекцій / презентація	Базова 5 Допоміжна 5 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 12. Виконати завдання СРС №12. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 12 тижня. 2 год.	5	Навчальний тиждень 12
Тиждень 11-12 (за розкладом) 2 год.	Тема 11-12. Методи стеганоаналізу для графічних файлів. Лабораторна робота №6. Дослідження захисту комп'ютерних систем за допомогою «Калина»-подібних алгоритмів.	Лабораторна / Face to face	Методичні рекомендації до виконання лабораторних робіт	Базова 5 Допоміжна 5 Інформаційні ресурси 1,2,3 Методичне забезпечення 1	Самостійно опрацювати теоретико-практичні питання до лабораторної роботи №6. 3 год.	6	За розкладом лабора-торних занять
Тиждень 13 (за розкладом) 2 год.	Тема 13. Критерії оцінки стійкості криптографічних систем захисту. Абсолютно стійкі алгоритми шифрування, практично стійкі або обчислювально стійкі системи захисту інформації. Критерії оцінки стійкості. Розкриття системи засекреченого зв'язку або АШ. Узагальнена класифікація атак на криптографічні СЗІ.	Лекція / Face to face	Конспект лекцій / презентація	Базова 5,8-11 Допоміжна 5 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 13. Виконати завдання СРС №13. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 13 тижня. 2 год.	6	Навчальний тиждень 13
Тиждень 14 (за розкладом) 2 год.	Тема 14. Методи активного криптоаналізу.	Лекція / Face to face	Конспект лекцій / презентація	Базова 5 Допоміжна 5,15-17 Інформаційні ресурси 1,2,3 Методичне забезпечення 2	Самостійно опрацювати теоретичний матеріал теми 14. Виконати завдання СРС №14. Підготувати повідомлення(презентацію) на тему, вказану за варіантом для 14 тижня. 2 год.	6	Навчальний тиждень 14

Тиждень 13-14 (за розкладом) 2 год..	Лабораторна робота №7. Дослідження захисту комп'ютерних систем за допомогою ГОСТ-подібного алгоритму.	Лабораторна / Face to face	Методичні рекомендації до виконання лабораторних робіт	Базова 5 Допоміжна 5 Інформаційні ресурси 1,2,3 Методичне забезпечення 1	Самостійно опрацювати теоретико-практичні питання до лабораторної роботи №7. 3 год.	6	За розкладом лабора-торних занять
Максимальна кількість балів за змістовим модулем 2						50	

11. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю студентів, усне опитування, письмовий контроль, тестовий контроль. Форма підсумкового контролю: залік.

Контроль знань і умінь здобувачів (поточний і підсумковий) здійснюється згідно з кредитною трансферно-накопичувальною системою організації освітнього процесу в ЦНТУ. Рейтинг студента із засвоєння дисципліни визначається за 100 бальною шкалою. Він складається з рейтингу з поточної навчальної роботи впродовж семестру, для оцінювання якої призначається 100 балів(по 50 балів за кожен змістовий модуль)..

Шкала оцінювання: національна та ЄКТС

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

Критерії оцінювання знань і вмінь здобувачів визначені Положенням про організацію освітнього процесу в ЦНТУ (стор. 32-33) http://www.kntu.kr.ua/doc/doc/The_provisions_of_company_profile.pdf

Розподіл балів, які отримують студенти при вивченні дисципліни «Криптоаналіз»:

ЗМ1				ЗМ2			Сума
Т1-2	Т3-4	Т5-6	Т7-8	Т9-10	Т11-12	Т13-14	
12	12	14	12	16	16	18	100

Примітка: ЗМ1,ЗМ2-змістовний модуль; Т1, Т2,.. ,,Т14 - тема програми.

12. Рекомендована література

Базова

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 878 с.
2. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
3. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.
4. Бессалов А., Телиженко А. Криптосистемы на эллиптических кривых. – К.: «Політехніка», 2004. – 224 с.
5. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк // Захист інформації. — 2010. — № 1. — С. 77–89.
6. Юдін О.К. Захист інформації в мережах передачі даних : Підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. — К. : Видавництво «DIRECTLINE», 2009. — 714 с.
7. Атаки в квантових системах захисту інформації / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Вісник інженерної академії України. — 2010. — № 2. — С. 109–115
8. Смірнова Т. В., Якименко Н. М., Смірнов С. А., Поліщук Л. І., Смірнов О. А. Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах .
9. 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»)**
10. 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»**)

11. 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»)**

Допоміжна

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 868 с.
2. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Електронний конспект лекцій. Харків, ХНУРЕ, 2012 р.
3. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
4. Есин В. И., Кузнєцов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.
5. Matt Walker. Certified Ethical Hacker Practice Exams. McGraw Hill. 2022. 352 с.
6. Shannon C. Communication Theory of Secrecy Systems, Bell Systems Technical Journal, 1949. — Vol. 28. — P. 656–715.
7. Nishant Bhajaria. Data Privacy. Manning. 2022. 805 с.
8. Tanuj Kumar Jhamb. Cracking C Programming Interview. BPB Online. 2022. 384 с.
9. Богуш В.М. , Мухачов В.А. Криптографічні застосування елементарної теорії чисел: Навч. посібник – К.: ДУІКТ, 2006. – 126 с.
10. Клесов О.І. Елементарна теорія чисел та елементи криптографії: Підручник. – Київ: ТВіМС, 2016. – 393 с.
11. Математичні основи криптоаналізу: навч. посіб. / С. О. Сушко, Г. В. Кузнецов, Л. Я. Фомичова, А. В. Корабльов ; – Дніпропетровськ: НГУ, 2010. - 465 с.
12. Кравець О. Підвищення ефективності крипто аналізу сучасних потокових шифрів / О. Кравець, С. Лупенко, А. Луцків // Вісник Національного університету "Львівська політехніка". – 2012. – № 741 : Автоматика, вимірювання та керування. – С. 240–245
13. Криптоаналіз. Криптографічні протоколи : навч. посіб. для студ. спец. 123 «комп'ютерна інженерія» / уклад. : О. М. Гапак – Ужгород : ПП "АУТДОР-ШАРК", 2021. – 93 с
14. Massimo Bertaccini. Cryptography Algorithms. Packt Publishing. 2022. 358 с.
15. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 с.
16. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 с.
17. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 с.

Інформаційні ресурси

1. http://www.nbuv.gov.ua/eb/ep.html - Національна бібліотека України імені В.І.Вернадського
2. http://dspace.nbuv.gov.ua/ - Наукова електронна бібліотека періодичних видань НАН України
3. Дистанційна освіта ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=672

Методичне забезпечення

1. Методичні рекомендації до лабораторних занять з дисципліни “ Криптоаналіз ” освітньо-професійної програми першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека денної та заочної форми навчання. / Укладач: Н.М.Якименко – Кропивницький: ЦНТУ, 2022 – 50 с.
2. Методичні рекомендації до самостійної роботи з дисципліни “ Криптоаналіз ” освітньо-професійної програми першого (бакалаврського) рівня вищої освіти зі спеціальності 125 Кібербезпека денної та заочної форми навчання. / Укладач: Н.М.Якименко – Кропивницький: ЦНТУ, 2022 – 12 с.