МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«29» 08 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«29» 08 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни

«КРИПТОГРАФІЯ»

ступінь вищої освіти – **бакалавр**

галузь знань – **12 Інформаційні технології**

спеціальність – **125 Кібербезпека та захист інформації**

освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестри	Лекції (год.)	Лаб. занять (год.)	ІРС (год.)	Тренінг (год)	СРС (год)	Разом (год.)	Екзамен
Денна	3	5	46	44	5	12	73	180	5

29.08.2025

Тернопіль - 2025

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека та захист інформації, затвердженої Вченою радою ЗУНУ (протокол №10 від 23.06.2023 р.).

Робочу програму склав доктор технічних наук, професор, професор кафедри кібербезпеки Михайло КАСЯНЧУК

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол №1 від 26 серпня 2025 р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Гарант освітньо-професійної програми _____ Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Криптографія”

Дисципліна “Криптографія”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 6	галузь знань – 12 Інформаційні технології	**Статус дисципліни** обов’язкова **Мова навчання** українська
Кількість залікових модулів – 5	спеціальність – 125 Кібербезпека та захист інформації	Рік підготовки: *3* Семестр: *5*
Кількість змістових модулів – 3	ступінь вищої освіти – бакалавр	Лекції (год): *46* Лабораторні заняття (год): *44*
Загальна кількість годин – 180		Самостійна робота (год): 73 Тренінг (год) – 12 Індивідуальна робота (год): *5*
Тижневих годин – 12, з них аудиторних – 6		Вид підсумкового контролю – екзамен

2. Мета й завдання вивчення дисципліни “Криптографія”

2.1. Мета завдання дисципліни

Мета вивчення дисципліни “Криптографія” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного криптографічного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу “Криптографія» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи кібербезпеки», „Лінійна алгебра та аналітична геометрія”, «Дискретна математика», «Фізика», «Основи програмування»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни.

В результаті вивчення курсу „Криптографія” студенти повинні:

– засвоїти основні фундаментальні поняття і закони криптографічного захисту інформації для їх використання в сучасних системах;

– знати принципи побудови криптографічних алгоритмів, криптографічних стандартів та їх використання в задачах захисту інформації;

– використовувати основні математичний апарат та закони криптографії в професійній діяльності;

– вміти використовувати програмні засоби, які реалізують основні криптографічні функції;

– програмно реалізовувати криптографічні алгоритми вирішення типових задач захисту інформації;

– проектувати різного рівня криптографічні системи захисту;

– вміння використовувати методи та засоби криптографічного захисту даних.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Криптографія». Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Криптографія» та формуванні у студентів цілісної системи теоретичних знань з курсу «Криптографія».

Завдання проведення лабораторних занять

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення лабораторних занять полягає

у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

– вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

– здатність до пошуку, оброблення та аналізу інформації;

– здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

– здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);

– здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності;

– здатність виконувати оцінку якості криптографічного захисту інформації в інформаційно-телекомунікаційних системах.

2.4. Передумови для вивчення дисципліни

Вивчення курсу "Криптографія» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи кібербезпеки», «Вища математика», «Теорія інформації та кодування», «Дискретна математика», «Фізика», «Основи програмування»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.5. Результати навчання

– виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

– вирішувати завдання захисту програм та інформації, що обробляється в інформаційно телекомунікаційних системах програмно апаратними засобами та давати оцінку результативності якості прийнятих рішень;

– забезпечувати процеси захисту та функціонування інформаційно телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

– вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

– реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах;

– вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);

– впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;

– приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

– вирішувати задачі захисту інформації, що обробляється в інформаційно телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

– виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах;

– здійснювати загальну оцінку якості криптографічного захисту інформації в інформаційно-телекомунікаційних системах;

– забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

– підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах.

3. Програма навчальної дисципліни “Криптографія"

Змістовий модуль 1. Симетричні криптосистеми.

Тема 1. Вступ. Шифри перестановки.

Вступ. Задачі криптографії. Основні поняття та положення комп’ютерної криптографії. Принципи криптографічного захисту інформації. Криптоаналітичні атаки. Їх види. Шифр скитала. Шифруючі таблиці. Шифр магічних квадратів. Шифр Кардано.

Тема 2. Шифри простої заміни.

Шифр атбаш. Полібіанський квадрат. Шифр Цезаря. Шифр Цезаря з ключовим словом. Шифруючі таблиці Трисемуса.

Тема 3. Шифри складної заміни. Шифр одноразового блокноту.

Шифр Гронсфельда. Шифр Гронсфельда з ключовим словом. Шифр Віженера. Шифр Віженера з ключовим словом. Роторні шифрувальні машини. Роторна шифрувальна машина Enigma. Біграмний шифр Плейфейра. Подвійний квадрат Уїтстона. Шифр чотирьох квадратів. Шифр ADFGVX. Шифр одноразового блокноту.

Тема 4. Алгоритм DES.

Структура алгоритму DES. Його переваги та недоліки. Операції алгоритму DES. Функція шифрування алгоритму DES. Генерація підключів алгоритму DES.

Тема 5. Режими роботи алгоритму DES.

Електронна кодова книга, зчеплення блоків шифру, зворотній зв’язок по шифртексту, зворотній зв’язок по виходу. Галузі застосування алгоритму DES.

Тема 6. Алгоритми IDEA та ГОСТ28147–89.

Структура алгоритму IDEA. Його переваги та недоліки. Операції алгоритму IDEA. Генерація підключів алгоритму IDEA. Загальна структура алгоритму ГОСТ28147–89. Його переваги та недоліки. Операції алгоритму ГОСТ28147–89. Генерація підключів алгоритму IDEA. Режими роботи алгоритму ГОСТ28147–89: проста заміна, гамування, гамування із зворотним зв’язком, вироблення іміговставки. Галузі застосування алгоритмів IDEA та ГОСТ28147–89.

Тема 7. Український та світовий стандарти симетричного шифрування.

Український стандарт симетричного шифрування «Калина». Світовий стандарт симетричного шифрування AES (Rijndeal).

Тема 8. Сімейство алгоритмів RC.

RC-подібні алгоритми. Алгоритми RC 2, RC 4, RC 5, RC 6.

Змістовий модуль 2. Асиметричні криптосистеми та хеш-функції.

Тема 9. Арифметика асиметричних криптосистем.

Основні поняття. Алгоритм Евкліда, його наслідок, пошук оберненого елемента, китайська теорема про остачі. Функція Ейлера. Теореми Ейлера та Ферма.

Тема 10. Криптосистема RSA.

Опис криптосистеми RSA. Генерування ключів. Шифрування та розшифрування. Коректність, ефективність та надійність криптосистеми.

Тема 11. Криптосистема Рабіна.

Генерування ключів криптосистеми Рабіна. Шифрування та розшифрування в криптосистемі Рабіна. Коректність, ефективність та надійність криптосистеми.

Тема 12. Криптосистема Ель–Гамаля.

Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля. Коректність, ефективність та надійність криптосистеми.

Тема 13. Електронний цифровий підпис.

Поняття електронного цифрового підпису. Електронний цифровий підпис в системах RSA та Ель–Гамаля. Алгоритм DSA. Система Шнорра. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.

Тема 14. Шифрування із паролем.

Шифрування із паролем. Апаратні пристрої збереження ключів. Криптографічні акселератори. Біометрична ідентифікація.

Тема 15. Поняття хеш-функції. Застосування хеш-функцій.

Визначення функції хешування та вимоги до неї. Алгоритм функції хешування по ГОСТ Р 34.11-94. Аналіз алгоритму та особливостей його програмної реалізації. Геш-функції на основі ділення. Мультиплікативна схема гешування. Гешування рядків змінної довжини. Криптографічні хеш-функції. Геометричне гешування. Прискорення пошуку даних.

Тема 16. Хеш-функції типу MD та SHA. Український стандарт хешування.

Хеш-функція MD (MD-2, MD-4, MD-5). Сімейство хеш-функцій SHA (SHA-1, SHA-2, SHA-3, SHA-256). Український стандарт хешування ДСТУ 7564:2014 «Купина».

Тема 17. Генерація ЕЦП на основі хеш-функцій.

Процедура вироблення та перевірки електронного підпису по ДСТУ 4145-2002. Генерація загальних параметрів, секретного та відкритого ключів. Особливості програмної реалізації процедури. Алгоритм DSA.

Змістовий модуль 3. Еліптична та квантова криптографія, елементи стеганографії.

Тема 18. Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих.

Еліптичні криві над кінцевими полями. Еліптичні криві над полями непарної характеристики. Теорема Хассе. Еліптичні криві над полями характеристики 2. Проективні координати. Швидка редукція (NIST-криві). Еліптичні криві, рекомендовані NIST. Розмір ключа.

Тема 19. ЕЦП на основі еліптичних кривих

Особливості ЕЦП на основі еліптичних кривих. Вибір параметрів. Генерування ключів ECDSA. Переваги ECDSA перед DSA. Практична реалізація.

Тема 20. Криптографічні протоколи

Визначення криптографічного протоколу. Перелік вимог до криптографічного протоколу. Аналіз атак на криптографічні протоколи. Використання симетричного та несиметричного шифрування в криптографічних протоколах.

Тема 21. Приклади сучасних комп'ютерних криптографічних систем.

Характеристики протоколу SSL компанії Netscape Communication Corporation для захисту інформаційного обміну в середовищі Інтернет. Ієрархія ключів, блок-схема розсилки ключів абонентам мережі, блок-схема забезпечення цифрового підпису даних в мережі.

Тема 22. Елементи стеганографії.

Комп'ютерна стеганографія. Методи вкладення інформації у файли мультимедіа. Методи приховування інформації в зображеннях. Методи приховування інформації в аудіо сигналах.

Тема 23. Квантова криптографія

Поняття квантової криптографії. Квантовий розподіл ключів. Способи та пристрої генерації та передачі одиночних фотонів. Фазове та часове кодування. Основні напрямки розвитку та проблеми квантової криптографії. Порівняльний аналіз протоколів квантової криптографії.

4. Структура залікового кредиту дисципліни “Криптографія”

	Кількість годин					
	Лекції	Лабораторні заняття	Самостійна робота	Індивідуальна робота	Тренінг	Контрольні заходи
Змістовий модуль 1. **Симетричні криптосистеми.**						
Тема 1. Вступ. Шифри перестановки.	2	-	3	2	4	Поточне опитування
Тема 2. Шифри простої заміни.	2	2	2			
Тема 3. Шифри складної заміни. Шифр одноразового блокноту.	2	2	3			
Тема 4. Алгоритм DES.	2	2	3			
Тема 5. Режими роботи алгоритму DES.	2	2	4			

Тема 6. Алгоритми IDEA та ГОСТ28147–89.	2	2	2			
Тема 7. Український та світовий стандарти симетричного шифрування.	2	2	3			
Тема 8. Сімейство алгоритмів RC.	2	2	2			
Змістовий модуль 2. **Асиметричні криптосистеми та хеш-функції**						
Тема 9. Арифметика асиметричних криптосистем.	2	2	4	2	4	Поточне опитування
Тема 10. Криптосистема RSA.	2	2	4			
Тема 11. Криптосистема Рабіна..	2	2	3			
Тема 12. Криптосистема Ель–Гамаля.	2	2	3			
Тема 13. Електронний цифровий підпис.	2	2	6			
Тема 14. Шифрування із паролем.	2	2	2			
Тема 15. Поняття хеш-функції. Застосування хеш-функцій	2	2	4			
Тема 16. Хеш-функції типу MD та SHA. Український стандарт хешування	2	2	6			
Тема 17. Генерація ЕЦП на основі хеш-функцій	2	2	2			
Змістовий модуль 3. **Еліптична та квантова криптографія, елементи стеганографії.**						
Тема 18. Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих.	2	2	3	1	4	Поточне опитування
Тема 19. ЕЦП на основі еліптичних кривих.	2	2	3			
Тема 20. Криптографічні протоколи.	2	2	3			
Тема 21. Приклади сучасних комп'ютерних криптографічних систем.	2	2	3			
Тема 22. Стеганографія.	2	2	2			
Тема 23. Квантова криптографія	2	2	3			
Разом	46	44	73	5	12	

5. Тематика лабораторних робіт.

Лабораторна робота № 1

Тема: Реалізація шифрів простої заміни.
Мета: Реалізувати шифри простої заміни.

Лабораторне заняття №2

Тема: Реалізація шифрів складної заміни.
Мета: Реалізувати шифри складної заміни.

Лабораторна робота № 3

Тема: Реалізація біграмних шифрів.
Мета: Реалізувати біграмні шифри.

Лабораторна робота № 4

Тема: Реалізація шифру одноразового блокноту.

Мета: Запрограмувати процес шифрування та дешифрування за допомогою шифру одноразового блокноту.

Лабораторна робота № 5

Тема: Вивчення стандарту шифрування даних DES.

Мета: Засвоїти методику побудови симетричних алгоритмів шифрування даних.

Лабораторна робота № 6

Тема: Реалізація стандарту шифрування даних DES.

Мета: Реалізація стандарту шифрування даних DES

Лабораторна робота № 7

Тема: Вивчення та реалізація режимів шифрування даних стандартом DES.

Мета: Вивчити та реалізувати режими шифрування даних стандартом DES.

Лабораторна робота № 8

Тема: Алгоритм IDEA.

Мета: Вивчити та дослідити алгоритм IDEA.

Лабораторна робота № 9

Тема: Вивчення українського та світового стандарту симетричного шифрування.

Мета: Вивчити український та світовий стандарт симетричного шифрування.

Лабораторна робота №10

Тема: Сімейство алгоритмів RC.

Мета: Вивчення та дослідження сімейства алгоритмів RC

Лабораторна робота № 11

Тема: Український та світовий стандарти симетричного шифрування..

Мета: Вивчення та дослідження українського та світового стандартів симетричного шифрування.

Лабораторна робота №12

Тема: Арифметика асиметричних криптосистем.

Мета: Вивчення та дослідження арифметики асиметричних криптосистем.

Лабораторна робота №13

Тема: Реалізація афінних шифрів.

Мета: Запрограмувати процес шифрування та дешифрування в афінних шифрах.

Лабораторна робота № 14

Тема: Вивчення процедури шифрування та дешифрування в криптосистемі RSA.

Мета: Засвоїти методику та отримати практичні навики побудови засобів захисту інформації на основі криптосистеми RSA.

Лабораторна робота № 15

Тема: Реалізація процедури шифрування та дешифрування в криптосистемі RSA.

Мета: Запрограмувати процедури шифрування та дешифрування в криптосистемі RSA.

Лабораторна робота № 16

Тема: Реалізація схеми шифрування Ель-Гамаля.

Мета: Запрограмувати схему шифрування Ель-Гамаля

Лабораторна робота № 17

Тема: Вивчення та дослідження особливостей побудови електронного цифрового підпису на основі алгоритму RSA.

Мета: Засвоїти методику та отримати практичні навики побудови електронних підписів на прикладі ЕЦП на основі алгоритму RSA

Лабораторна робота № 18

Тема: Реалізація електронного цифрового підпису на основі алгоритму RSA.

Мета: Запрограмувати алгоритм електронного цифрового підпису на основі алгоритму RSA.

Лабораторна робота № 19

Тема: Поняття хеш-функції. Генерування та види хеш-функцій.

Мета: Вивчити та дослідити поняття хеш-функції, її види та методи генерування.

Лабораторна робота № 20

Тема: Хеш-функції типу SHA. Український стандарт хешування. Генерація ЕЦП на основі хеш-функцій.

Мета: Вивчити та дослідити хеш-функції типу SHA, український стандарт хешування, генерацію ЕЦП на основі хеш-функцій.

Лабораторна робота № 21

Тема: Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих. ЕЦП на основі еліптичних кривих.

Мета: Вивчення поняття еліптичної криптографії. Вивчення та дослідження методів реалізації шифрування на еліптичних кривих. Вивчення та дослідження ЕЦП на основі еліптичних кривих.

Лабораторна робота № 22

Тема: Криптографічні протоколи обміну ключем, жеребу по телефону, розподілу таємниці. Приклади сучасних комп'ютерних криптографічних систем.

Мета: Вивчення та дослідження криптографічних протоколів обміну ключем, жеребу по телефону, розподілу таємниці. Вивчення та дослідження прикладів сучасних комп'ютерних криптографічних систем.

6. Самостійна робота

Для самостійної роботи кожному студенту пропонується програмна або програмна-апаратна реалізація запропонованого чи вибраного самостійно криптографічного застосунку.

Орієнтовна тематика:

1. Реалізація представлення тексту у цифровій формі та шифру одноразового блокноту.
2. Реалізація схеми режиму шифрування DES-ECB.
3. Реалізація схеми режиму шифрування DES-CBC.
4. Реалізація схеми режиму шифрування DES-CPB.
5. Реалізація схеми режиму шифрування DES-OFB.
6. Реалізація потрійного DES.
7. Реалізація афінних шифрів.
8. Реалізація методу генерування простих чисел.
9. Реалізація методу генерування псевдопростих чисел.
10. Реалізація методу обчислення функції Ейлера
11. Реалізація алгоритму шифрування RSA.
12. Реалізація алгоритму шифрування Ель-Гамаля.
13. Дослідження стійкості криптографічних алгоритмів.
14. Алгоритм шифрування на основі задачі про укладку портфеля.
15. Реалізація алгоритму шифрування на основі еліптичних кривих.
16. Реалізація хеш-функції MD5.
17. Реалізація протоколу обміну ключами.
18. Реалізація протоколів аутентифікації.
19. Реалізація протоколу ідентифікації/аутентифікації на основі шифрування з відкритим ключем.
20. Реалізація ЕЦП на базі алгоритму RSA.
21. Реалізація ЕЦП на базі алгоритму Ель-Гамаля.
22. Реалізація ЕЦП на базі алгоритму DSA.

7. Організація та проведення тренінгу з дисципліни «Криптографія»

Тематика тренінгу: застосування і практична реалізація криптографічних застосунків.

Мета тренінгу: забезпечити студентів комплексними теоретичними знаннями та практичними навичками в галузі реалізації криптографічного захисту інформації, підготувавши їх до ефективної фахової діяльності у сучасному цифровому середовищі.

Цей тренінг охоплює ключові аспекти криптографічного захисту інформації, поєднуючи теоретичні знання з практичними навичками. Студенти повинні підготувати і представити презентацію по темі своєї самостійної роботи.

8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни “Криптографія” використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумковий модульний контроль за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– оцінювання тренінгів;
– оцінювання результатів самостійної роботи;
– підсумковий екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни "Криптографія" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за виконання та захист лабораторних робіт №1-11.	Підсумкова письмова робота за темами №1-12.	Оцінка за даний модуль визначається як середнє арифметичне за виконання та захист лабораторних робіт №12-22.	Підсумкова письмова робота за темами №13-23.	Визначається як середнє арифметичне з оцінок за представлення та захист реалізованого криптографіч-ного застосунку.	Оцінка за реалізацію криптогра-фічного застосунку	1. Теоре-тичні пи-тання: 2 питання по 30 балів - max 60 балів. 2. Практич-не завдання - max 40 балів

Поточне оцінювання під час заняття:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності;

1–59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань. Підсумкова оцінка за поточне опитування кожного модуля визначається як середнє арифметичне оцінок, отриманих під час занять в межах кожного модуля.

Тренінг:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його використовує під час розв'язування задач тренінгу;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при розв'язуванні окремих задач тренінгу не вистачає достатньої глибини та аргументації його використання, допускаються при цьому окремі несуттєві неточності та незначні помилки;

65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при розв'язування задач тренінгу, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому суттєві неточності та помилки;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його використовує, частково розв'язуючи задачі тренінгу, допускаючи при цьому суттєві неточності;

1–59 – не володіє навчальним матеріалом, не розв'язує задачі тренінгу, не бере участі у колективних завданнях підчас проведення тренінгу.

Самостійна робота:

90–100 балів – зміст та захист реферату свідчить про високий рівень опанування навчального матеріалу, реферат містить елементи самостійного дослідження, студент на високому рівні виявляє творчий підхід до виконання завдань;

75–89 балів – зміст та захист реферату загалом свідчить про належний рівень опанування навчального матеріалу, можуть бути несуттєві недопрацювання, студент належно виявляє творчий підхід до виконання завдань;

60–74 балів – поставлені завдання виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабко обґрунтованими, свідчать про недостатній рівень опанування навчального матеріалу; студент припускається значних помилок у виконанні завдань, в окремих моментах виявляє творчий підхід до виконання завдань;

1–59 балів – завдання практично не виконані; відсутні авторські напрацювання; грубі помилки у вирішенні завдань роботи, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до виконання завдань.

Модульна робота, екзамен – види контролю, при яких засвоєння студентом теоретичного та практичного матеріалу оцінюється від 0 до 100 балів як сума балів за виконані завдання. Екзаменаційний білет складається з двох теоретичних питань, за кожне з яких можна отримати від 0 до 30 балів, що в підсумку дає максимально 60 балів, та однієї практичної задачі, за яку можна отримати від 0 до 40 балів. За теоретичне питання студент отримує 15–30 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст завдання, і 1–14 балів – якщо в цілому володіє навчальним матеріалом, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст завдання, допускаючи при цьому суттєві неточності, відповіді на запитання нечіткі. За практичну задачу студент отримує 25–40 балів, якщо у повному обсязі володіє навчальним матеріалом, правильно розв'язує практичну задачу і інтерпретує отримані результати, демонструє самостійність виконання; 10–24 балів – у достатньому обсязі володіє навчальним матеріалом, правильно розв'язує практичну задачу, але на додаткові контрольні запитання відсутня повна відповідь, допускає несуттєві неточності та фрагментарно (без аргументації) інтерпретує отримані результати, демонструє самостійність виконання; 1–9 балів – не в повному обсязі володіє матеріалом, фрагментарно розв'язує практичне завдання, допускає суттєві неточності, поверхнево його викладає, недостатньо розкриває зміст поставлених питань.

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

12. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Електронний варіант лекцій	1 -21
2	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1 - 21
3	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-21

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
2. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
3. Stallings, W., & Brown, L. Computer Security: Principles and Practice (4th ed.). Pearson. 2022. 384 p.
4. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
5. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
6. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
7. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160/
8. Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
9. Асиметричні алгоритми шифрування у системі залишкових класів / Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138.
10. Ya.M.Nykolaychuk, M.M.Kasianchuk, I.Z.Yakymenko. Symmetric Cryptoalgorithms in the Residue Number System/ // Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
11. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
12. Nykolaychuk Ya.M., Yakymenko I.Z., Vozna N.Ya., and Kasianchuk M.M. Residue Number System Asymmetric Cryptoalgorithms. Cybernetics and Systems Analysis. 2022, Vol. 58, No. 4, P.611-618.

13. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах/ М. М. Касянчук, М. П. Карпінський, С. В. Казмірчук. Захист інформації, №2, т.21, 2019. С.65-73.

14. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання/ М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко. Informatics & Mathematical Methods in Simulation, №11, 2021. С. 47-57.