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

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«__30__» _____ 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«__30__» _____ 2025 р.

ЗАТВЕРДЖУЮ
Директор Навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
«__30__» _____ 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни

«КРИПТОГРАФІЧНІ ПРОТОКОЛИ ТА МЕТОДИ КРИПТОАНАЛІЗУ»

ступінь вищої освіти – магістр

галузь знань – F Інформаційні технології

спеціальність – F5 Кібербезпека та захист інформації

освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. заняття (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік/ екзамен. (семестр)
Денна	1	2	32	14	5	6	93	150	Екзамен (2)
Заочна	1	2	8	4	-	-	138	150	Екзамен (2)

Тернопіль - 2025

Робочу програму склали доктор технічних наук, професор, професор кафедри кібербезпеки Михайло КАСЯНЧУК та кандидат технічних наук, доцент, доцент кафедри кібербезпеки Степан ІВАСЬЄВ.

Робоча програма затверджена на засіданні кафедри кібербезпеки,
протокол №__3__ від __25.09.25__ р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Криптографічні протоколи та методи криптоаналізу”

Дисципліна “Криптографічні протоколи та методи криптоаналізу ”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	галузь знань – F Інформаційні технології	**Статус дисципліни** вибіркова **Мова навчання** українська
Кількість залікових модулів – 4	спеціальність – F5 Кібербезпека та захист інформації	Рік підготовки: Денна – 1 Заочна – 1 Семестр: Денна – 2 Заочна – 2
Кількість змістових модулів – 3	ступінь вищої освіти – магістр	Лекції (год): денна – 32; заочна – 8. Лабораторні заняття (год): денна – 14; заочна – 4.
Загальна кількість годин – 150		Самостійна робота (год): денна – 93; заочна – 138. Тренінг (год): денна – 6. Індивідуальна робота (год): денна – 5
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – екзамен.

2. Мета й завдання вивчення дисципліни “Криптографічні протоколи та методи криптоаналізу”

2.1. Мета завдання дисципліни

Мета вивчення дисципліни “Криптографічні протоколи та методи криптоаналізу” полягає у формуванні у майбутніх фахівців 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 “Криптографічні протоколи та методи криптоаналізу» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Цифрова криміналістика», «Аналіз шкідливого програмного забезпечення», «Моніторинг та управління інформаційною безпекою»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи здобувачів.

2.2. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є систематизація інформації щодо розроблення, впровадження та експлуатації криптографічних систем захисту інформації на об’єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик криптографічного захисту інформації.

У результаті вивчення навчальної дисципліни здобувач повинен:

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

– знати принципи побудови криптографічних протоколів 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 протоколи;

– програмно реалізовувати криптографічні протоколи вирішення типових задач захисту інформації;

– проектувати різного рівня криптографічні системи захисту з врахуванням методів криптоаналізу;

– вміння використовувати методи та засоби криптографічного захисту даних.

Мета проведення лекцій полягає у тому, щоб ознайомити здобувачів із головними питаннями курсу «Криптографічні протоколи та методи криптоаналізу». Завдання проведення лекцій полягає у: викладенні здобувачам у відповідності з програмою та робочим планом основних питань курсу «Криптографічні протоколи та методи криптоаналізу» та формуванні у здобувачів цілісної системи теоретичних знань з курсу «Криптографічні протоколи та методи криптоаналізу».

Мета проведення лабораторних занять полягає у тому, щоб виробити у здобувачів практичні навички використання теоретичного матеріалу. Завдання проведення лабораторних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

3. Програма навчальної дисципліни “Криптографічні протоколи та методи криптоаналізу"

Змістовий модуль 1. Криптографічні протоколи.

Тема 1. Сучасні симетричні та асиметричні криптосистеми.

Структура алгоритму DES. Функція шифрування алгоритму DES. Генерація підключів алгоритму DES. Режими роботи алгоритму DES. Структура алгоритму IDEA. Сімейство алгоритмів RC. Опис криптосистеми RSA. Генерування ключів. Шифрування та розшифрування. Генерування ключів криптосистеми Рабіна. Шифрування та розшифрування в криптосистемі Рабіна. Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля.

Тема 2. Поняття криптографічних протоколів. Їх опис.

Визначення криптографічного протоколу. Учасники протоколу. Вербальний опис. Математичний опис виконуваних операцій з вербальним описом дій учасників. Опис по кроках протоколу. Символічний опис. Опис у вигляді відображення послідовності дій.

Тема 3. Класифікація криптографічних протоколів.

Примітивні і прикладні криптографічні протоколи. Класифікація за кількістю учасників. Класифікація за кількістю переданих повідомлень. Класифікація за цільовим призначенням протоколу. За типом використовуваних криптографічних систем. За способом функціонування. Класифікація за надійністю.

Тема 4. Властивості, що визначають безпеку криптографічних протоколів.

Аутентифікація. Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення. Авторизація (довіреною третьою стороною). Властивості спільної генерації ключа. Конфіденційність. Анонімність. Захищеність від атак типу «відмова в обслуговуванні». Інваріантність відправника. Неможливість відмови від раніше вчинених дій. Безпечна тимчасова властивість.

Тема 5. Аналіз та моделювання криптографічних протоколів.

Моделювання і перевірка роботи протоколу з використанням мов опису і засобів перевірки, не розроблених для аналізу криптографічних протоколів. Створення експертних систем. Вироблення вимог до сімейства протоколів. Розробка формальних методів. Протоколи з посередником. Протоколи з арбітром. Самодостатні протоколи.

Тема 6. Протоколи електронного цифрового підпису.

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.

Змістовий модуль 2. Протоколи розподілу криптографічних ключів.

Тема 7. Протоколи, що ґрунтуються на симетричних криптосистемах.

Протокол Барроуза. Протокол Нідхема-Шредера. Протокол Kerberos. Протокол розподілу ключів по паралельних каналах.

Тема 8. Протоколи, що ґрунтуються на асиметричних криптосистемах.

Протокол обміну ключами Діффі-Хелмана. Триразовий протокол рукостискання. Протокол MQV (Менезес-Кью-Ванстоун).

Тема 9. Квантовий розподіл ключів.

Протокол BB84. Протокол B92. Протокол E91 (EPR). Протокол розподілу ключів, що ґрунтується на кодуванні через часові зсуви. Протокол на основі квантового прямого безпечного зв'язку. Протокол на основі методу довірених кур'єрів.

Тема 10. Протокол розподілу ключів за допомогою еліптичних кривих.

Протокол Діффі-Хелмана. Опис протоколу. Приклад застосування. Приклади програмної реалізації.

Змістовий модуль 3. Методи криптоаналізу.

Тема 11. Вступ до криптоаналізу. Криптоаналітичні атаки.

Вступ. Основні поняття криптоаналізу. Криптоаналіз шифру Цезаря. Типи криптостійких систем шифрування. Поняття про атаки на алгоритми шифрування та їх класифікація. Метод повного перебору. Моделі оцінки безпеки. Типи атак на алгоритми шифрування. Ідеальний шифр, принципи побудови та властивості. Безумовно стійкі та практично (обчислювально) стійкі шифри.

Тема 12. Атаки на протоколи.

Класи криптоаналітичних атак. Атаки на схеми зашифрування. Пасивні атаки. Активні атаки. Пасивні шахраї. Активні шахраї. Підміна. Повторне нав'язування повідомлення. Атака відображенням. Затримка передачі повідомлення. Комбінована атака. Атака з паралельними сеансами. Атака з використанням спеціально підібраних текстів. Атака «противник в середині». Атака з відомим сеансовим ключем. Атака з невідомим спільним ключем. Атака вичерпного пошуку та словникова атака. Атака на основі парадоксу днів народження. Атака на основі застосування таблиць передобчислень.

Тема 13. Криптоаналіз симетричних криптосистем.

Універсальні методи криптоаналізу. Атака по ключам. Частотний аналіз. Методи криптоаналізу блочних шифрів. Методи криптоаналізу потокових шифрів. Криптоаналіз по побічним каналам. Стійкість сучасних стандартів симетричного шифрування. Криптоаналіз методом «зустрічі посередині».

Тема 14. Диференційний (різницевий) криптоаналіз.

Сутність диференційного криптоаналізу. Диференційні властивості підстановки блокового шифру DES. Механізм відновлення бітів ключа при знанні вхідних різниць підстановки. Операція додавання ключа. Різниці у цикловій функції блокового шифру DES. Складність диференційного криптоаналізу блокового шифру DES..

Тема 15. Криптоаналіз асиметричних криптосистем.

Криптоаналіз асиметричних криптосистем. Криптоаналіз геш-функцій. Рішення завдання факторизації. Рішення задачі дискретного логарифма. Квантові обчислення.

4. Структура залікового кредиту дисципліни “Криптографічні протоколи та методи криптоаналізу”

4.1 Структура залікового кредиту дисципліни “Криптографічні протоколи та методи криптоаналізу” для ДФН

	Кількість годин					
	Лекції	Лабораторні заняття	Самостійна робота	Індивідуальна робота	Тренінг	Контрольні заходи
Змістовий модуль 1. **Криптографічні протоколи.**						
Тема 1. Сучасні симетричні та асиметричні криптосистеми**.**	2	-	6	2	2	Поточне опитування
Тема 2. Поняття криптографічних протоколів. Їх опис.	2	-	6			
Тема 3. Класифікація криптографічних протоколів**.**	2	-	6			
Тема 4. Властивості, що визначають безпеку криптографічних протоколів**.**	2	-	6			
Тема 5. Аналіз та моделювання криптографічних протоколів.	2	2	6			
Тема 6. Протоколи електронного цифрового підпису.	2	2	6			
Змістовий модуль 2. **Протоколи розподілу криптографічних ключів**						
Тема 7. Протоколи, що ґрунтуються на симетричних криптосистемах.	2	-	6	1	2	Поточне опитування
Тема 8. Протоколи, що ґрунтуються на асиметричних криптосистемах**.**	3	2	6			
Тема 9. Квантовий розподіл ключів	2	-	6			
Тема 10. Протокол розподілу ключів за допомогою еліптичних кривих	2	2	6			
Змістовий модуль 3. **Методи криптоаналізу.**						
Тема 11. Вступ до криптоаналізу. Криптоаналітичні атаки**.**	2	-	7	2	2	Поточне опитування
Тема 12. Атаки на протоколи**.**	2	-	6			
Тема 13. Криптоаналіз симетричних криптосистем**.**	2	2	7			
Тема 14. Диференційний (різницевий) криптоаналіз**.**	2	2	6			
Тема 15. Криптоаналіз асиметричних криптосистем**.**	3	2	7			
Разом	32	14	96	5	6	

4.2 Структура залікового кредиту дисципліни "Криптографічні протоколи та методи криптоаналізу" для ЗФН

	Кількість годин			
	Лекції	Лабораторні заняття	Самостій-на робота	Контрольні заходи
Тема 1. Сучасні симетричні та асиметричні криптосистеми**.** Поняття криптографічних протоколів. Їх опис. Класифікація криптографічних протоколів**.** Властивості, що визначають безпеку криптографічних протоколів**.**	2	1	34	Поточне опитування
Тема 2. Аналіз та моделювання криптографічних протоколів. Протоколи електронного цифрового підпису. Протоколи, що ґрунтуються на симетричних криптосистемах. Протоколи, що ґрунтуються на асиметричних криптосистемах**.**	2	1	35	
Тема 3. Квантовий розподіл ключів. Протокол розподілу ключів за допомогою еліптичних кривих. Вступ до криптоаналізу. Криптоаналітичні атаки**.** Атаки на протоколи**.**	2	1	34	
Тема 4. Криптоаналіз симетричних криптосистем**.** Диференційний (різницевий) криптоаналіз. Криптоаналіз асиметричних криптосистем.	2	1	35	
Разом	8	4	138	

5. Тематика лабораторних робіт.

5.1 Тематика лабораторних робіт для ДФН.

Лабораторна робота №1

Тема: Розподіл ключів. Протокол Діффі-Хеллмана.

Мета роботи:

- Ознайомитися з принципами розподілу симетричних ключів у відкритих мережах.
- Дослідити роботу протоколу Діффі-Хеллмана.
- Реалізувати обмін ключами за допомогою алгоритму Діффі-Хеллмана.
- Перевірити, що обидві сторони отримують однаковий спільний секрет.

Лабораторна робота № 2

Тема: Протокол Нідхема-Шредера (Needham-Schroeder Protocol).

Мета роботи:

- Ознайомитися з принципами автентифікації у розподілених системах.
- Вивчити симетричний протокол автентифікації Нідхема-Шредера.
- Реалізувати протокол для встановлення сесійного ключа між двома сторонами.
- Проаналізувати можливі вразливості та способи їх усунення.

Лабораторна робота №3

Тема: Протокол сліпого підпису.

Мета роботи:

- ознайомитися з протоколом сліпого підпису в групі точок еліптичної кривої над простим полем GF(p) на базі алгоритму цифрового підпису ЕльГамаля**.**

Лабораторна робота № 4

Тема: Протокол колективного підпису**.**

Мета роботи:

- Вивчити принципи роботи протоколу колективного (групового) цифрового підпису.
- Реалізувати базову модель протоколу колективного підпису в обраному середовищі програмування.

- Перевірити, як кілька учасників можуть колективно створити підпис, який можна перевірити як єдиний, але який залежить від участі всіх підписантів.

Лабораторна робота № 5

Тема: Криптоаналіз шифру Віжінера.

Мета роботи:

- Застосування методів частотного аналізу до шифру Віжінера.

Лабораторна робота №6

Тема: Методи криптоаналізу асиметричних криптоперетворень в групі точок еліптичних кривих**.**

Мета роботи:

- Розглянути методи криптоаналізу та дослідити крипто стійкість асиметричних криптоперетворень в групі точок еліптичних кривих

Лабораторна робота № 7

Тема: Криптоаналіз за побічними каналами (Side-Channel Analysis).

Мета роботи:

- Ознайомитися з основами криптоаналізу за побічними каналами.
- Зрозуміти, які типи побічної інформації можуть бути використані для зламу криптографічних алгоритмів.
- Провести моделювання або аналіз атаки за побічним каналом (наприклад, по часу виконання або енергоспоживанню).
- Сформувати уявлення про методи захисту від таких атак.

5.2 Тематика лабораторних робіт для ЗФН.

Лабораторна робота №1

Тема: Тема: Розподіл ключів. Протокол Діффі-Хеллмана. Протокол Нідхема-Шредера (Needham-Schroeder Protocol).

Мета роботи:

- Ознайомитися з принципами розподілу симетричних ключів у відкритих мережах.
- Дослідити роботу протоколу Діффі-Хеллмана.
- Реалізувати обмін ключами за допомогою алгоритму Діффі-Хеллмана.
- Перевірити, що обидві сторони отримують однаковий спільний секрет.
- Ознайомитися з принципами автентифікації у розподілених системах.
- Вивчити симетричний протокол автентифікації Нідхема-Шредера.
- Реалізувати протокол для встановлення сесійного ключа між двома сторонами.
- Проаналізувати можливі вразливості та способи їх усунення.

Лабораторна робота № 2

Тема: Протокол сліпого підпису. **Протокол колективного підпису.**

Мета роботи:

- ознайомитися з протоколом сліпого підпису в групі точок еліптичної кривої над простим полем GF(p) на базі алгоритму цифрового підпису ЕльГамаля**.**
- Вивчити принципи роботи протоколу колективного (групового) цифрового підпису.
- Реалізувати базову модель протоколу колективного підпису в обраному середовищі програмування.
- Перевірити, як кілька учасників можуть колективно створити підпис, який можна перевірити як єдиний, але який залежить від участі всіх підписантів.

Лабораторна робота №3

Тема: Криптоаналіз шифру Віжінера. Методи криптоаналізу асиметричних криптоперетворень в групі точок еліптичних кривих.

Мета роботи:

- Застосування методів частотного аналізу до шифру Віжінера.
- Розглянути методи криптоаналізу та дослідити крипто стійкість асиметричних криптоперетворень в групі точок еліптичних кривих.

.

Лабораторна робота №4

Тема: Криптоаналіз за побічними каналами (Side-Channel Analysis).

Мета роботи:

- Ознайомитися з основами криптоаналізу за побічними каналами.
- Зрозуміти, які типи побічної інформації можуть бути використані для зламу криптографічних алгоритмів.
- Провести моделювання або аналіз атаки за побічним каналом (наприклад, по часу виконання або енергоспоживанню).
- Сформувати уявлення про методи захисту від таких атак.

6. Тематика самостійної роботи студентів

На самостійну роботу кожному студенту пропонується написання і представлення реферату на запропоновану або самостійно вибрану тему. Орієнтовна тематика рефератів:

1. Протокол доведення з нульовим пізнанням.
2. Протокол обміну ключами.
3. Протокол для проблеми криптографів, що обідають.
4. Протокол Діффі - Геллмана на еліптичних кривих.
5. Протокол Signal.
6. Протоколи таємного голосування.
7. Протокол CCMP.
8. Протокол HOTP.
9. Протокол HTTPS.
10. Протокол Kerberos.
11. Протокол KMIP.
12. Протокол MIKEY.
13. Протокол OCRA.
14. Протокол Off-the-Record Messaging.
15. Протокол OMEMO.
16. Протокол SCRAM.
17. Протокол SDES.
18. Протокол SSL.
19. Протокол Subresource Integrity.
20. Протокол Transport Layer Security.
21. Протокол Wi-Fi Protected Setup.
22. Протокол ZRTP.
23. Генератори випадкових та псевдовипадкових послідовностей. Статистичні тести.
24. Криптографічно безпечні генератори псевдовипадкових послідовностей.
25. Випадкові числа. Генератори випадкових чисел.
26. Генератори псевдовипадкових послідовностей.
27. Використання стандартних функцій мов програмування високого рівня. Конгруентний генератор псевдовипадкових чисел.
28. Лінійні регістри зі зворотним зв'язком (LFSR). Модифіковані LFSR.
29. Криптографічно стійкі датчики випадкових чисел.
30. Системно-теоретичний підхід отримання випадкових чисел.
31. Складнісно-теоретичний підхід отримання випадкових чисел.
32. Інформаційно-теоретичний підхід отримання випадкових чисел.
33. Рандомізований підхід отримання випадкових чисел.
34. Генератори справжніх випадкових чисел. Відхилення та кореляції.
35. Розподіл випадковості за допомогою односторонньої хеш-функції.

36. Статистичні тести для псевдовипадкових чисел.
37. Метод криптоаналізу «метод зустрічі посередині».
38. Поліграмний шифр Хілла і дослідження методів його криптоаналізу.
39. Аналіз криптографічної стійкості AES.
40. Лінійний криптоаналіз.
41. Сутність та вимоги до протоколів автентифікації.
42. Аналіз методів криптографічного аналізу криптоперетворень в циклічних групах та підгрупах.
43. Аналіз відомих вразливостей банків та нанесених втрат.
44. Порівняльний аналіз стійкості асиметричних крипто перетворень.
45. Вимоги до засобів генерування та застосування ключів та ключової інформації.
46. Класифікація та оцінка стійкості криптоперетворень в групі точок еліптичних кривих.
47. Порівняльний аналіз методів криптографічного аналізу симетричних шифрів.
48. Сутність та вразливості симетричних крипто перетворень.
49. Аналіз вразливостей блокових шифрів.
50. Класифікація та оцінка вразливості відомих методів криптоаналізу відносно блокових симетричних шифрів.
51. Порівняльний аналіз методів криптоаналізу симетричних шифрів.
52. Вимоги до криптостійкості блокових шифрів.

7. Організація та проведення тренінгу з дисципліни «Криптографічні протоколи та методи криптоаналізу»

Тематика тренінгу: застосування і практична реалізація криптографічних протоколів для захисту інформаційних потоків та методів крипоаналізу.

Цей тренінг охоплює ключові аспекти криптографічних протоколів та методів криптоаналізу, поєднуючи теоретичні знання з практичними навичками. Здобувачі отримають практичні навички роботи з різноманітними програмними середовищами та апаратним забезпеченням.

Мета тренінгу: забезпечити здобувачів комплексними теоретичними знаннями та практичними навичками в галузі реалізації криптографічних протоколів та методів криптоаналізу, підготувавши їх до ефективної фахової діяльності у сучасному цифровому середовищі.

Орієнтовний перелік завдань для тренінгу:

1. Криптографічні атаки по стороннім каналам.
2. Криптографічні вразливості: недостатній аналіз розробленого алгоритму, застосування застарілих перетворень та некоректне застосування перетворень.
3. Атака розширення довжини на конструкцію Меркля-Дамгарда.
4. Застосування слабкого протоколу управління ключами.
5. Рекомендації щодо застосування криптографічних протоколів.
6. Криптографія на основі ідентифікаторів.
7. Інфраструктура відкритих ключів. Центр сертифікації ключів. Кореневий центр сертифікації.
8. Кроссертифікація. Сертифікат X.509 v3.
9. Список відкликаних сертифікатів. Причини відкликання сертифікату.
10. Протокол OCSP (Online Certificate Status Protocol).
11. Аутентифікація при розсилці за багатьма адресами або встановлення з'єднання зі службою підписки / повідомлення.
12. Методи бінарного відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії та властивості.
13. Вимоги, методи та засоби оцінки нерозрізнюваності, необоротності та непередбачуваності псевдовипадкових чисел (бітів).
14. Визначення та вимоги до випадкових послідовностей чисел(бітів).
15. Поняття та вимоги до псевдовипадкової послідовності.
16. Порівняльний аналіз властивостей випадкових та псевдовипадкових послідовностей.
17. Оцінка необоротності генераторів псевдовипадкових чисел.
18. Методи та механізми автентифікації і імітозахисту в радіосистемах, критерії та показники оцінки властивостей.

19. Модель загроз порушення справжності (автентичності).
20. Модель взаємної недовіри та взаємного захисту.
21. Особливості автентифікації в радіосистемах.
22. Критерії та показники оцінки якості імітозахисту.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення здобувачів із запропонованими завданнями тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі здобувачів.

Практична частина реалізується шляхом виконання одного вибраного завдання тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

8. Методи навчання.

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

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни "Криптографічні протоколи та методи криптоаналізу" використовуються наступні методи оцінювання навчальної роботи здобувачів:

– 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 здобувачами 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 здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, 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 "Криптографічні протоколи та методи криптоаналізу" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне з оцінок, отриманих за виконання та захист лабораторних робіт.	Підсумкова письмова робота за темами №1-15.	Оцінка за виконання та представлення одного вибраного завдання тренінгу	Оцінка за виконаний і представлений реферат на вибрану тему.	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне 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	Мультимедійний проектор та проєкційний екран	1 -15
2	Персональні комп'ютери	1 -15
3	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1 -15
4	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 -15
5	Наявність доступу до мережі Інтернет	1 -15
6	CrypTool, openssl, CyberChef, Scilab.	1-15

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. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// 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.
15. Симетрична система з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування/ В.М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова, В.А. Анікін// Вісник Хмельницького національного університету. Технічні науки. 2020. № 6. С. 33-39