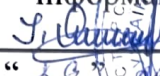


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

Декан факультету комп'ютерних
інформаційних технологій

Ігор ЯКИМЕНКО
"29" 2025 р.

ЗАТВЕРДЖУЮ

Директор навчально-наукового
інституту новітніх освітніх
технологій

Святослав ПИТЕЛЬ
"29" 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної
роботи

Віктор ОСТРОВЕРХОВ
"29" 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Захист інформації в комп'ютерних системах і мережах»

ступінь вищої освіти – бакалавр

галузь знань – 12 “Інформаційні технології”

спеціальність – 123 “Комп'ютерна інженерія”

освітньо-професійна програма – „Комп'ютерна інженерія”

Кафедра комп'ютерної інженерії

Форма навчання	Курс	Семестр	Лекції (год.)	Лабораторні (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Екз. (сем.)
Денна	3	6	46	30	5	10	59	150	6
Заочна	3	6	8	4	-	-	138	150	6

29.01.2025

Тернопіль – ЗУНУ
2025

Робоча програма складена на основі освітньо – професійної програми підготовки бакалавра галузі знань 12 “Інформаційні технології” напряму підготовки 123 “Комп’ютерна інженерія”, затвердженої Вченою радою ЗУНУ (протокол № 10 від 23 червня 2023 р.).

Робочу програму склала к.т.н., доцент, зав.кафедри КІ

Леся ДУБЧАК

Робоча програма затверджена на засіданні кафедри комп’ютерної інженерії, протокол №1 від 26 серпня 2025 р.

Завідувач кафедри



Леся ДУБЧАК

Гарант ОП «Комп’ютерна інженерія»



Леся ДУБЧАК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ"

1. Опис дисципліни "Захист інформації в комп'ютерних системах і мережах"

Дисципліна – «Захист інформації в комп'ютерних системах»	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів – 5	галузь знань – 12 „Інформаційні технології”	Статус дисципліни – обов’язкова Мова навчання – українська
Кількість залікових модулів: 5	Спеціальність – 123 „Комп’ютерна інженерія”	Рік підготовки: <i>Денна</i> - 3, <i>Заочна</i> – 3 Семестр: <i>Денна</i> – 6 <i>Заочна</i> – 6
Кількість змістових модулів – 4	Ступінь вищої освіти - бакалавр	Лекції: <i>Денна</i> - 46 год., <i>Заочна</i> – 8 год. Лабораторні заняття: <i>Денна</i> - 30 год. <i>Заочна</i> – 4 год.
Загальна кількість годин – <i>Денна</i> – 150 год., <i>Заочна</i> - 150 год.		Самостійна робота: <i>Денна</i> – 59 год. <i>Заочна</i> – 138 год. Тренінг – 10 год. Індивідуальна робота: <i>Денна</i> – 6 год.
Тижневих годин: <i>Денна</i> : 6 семестр: 10 год., з них аудиторних – 5 год.		Вид підсумкового контролю <i>Денна</i> : 6 семестр – екзамен <i>Заочна</i> : 6 семестр – екзамен

2. Мета й завдання вивчення дисципліни "Захист інформації в комп'ютерних системах і мережах"

2.1. Мета вивчення дисципліни

Програма та тематичний план дисципліни орієнтовані на отримання студентами навиків та знань щодо захисту інформації.

Студенти вивчають основи використання прикладного програмного забезпечення, яке використовується при захисті інформації, включаючи ознайомлення з вірусами та антивірусними програмами, методи ідентифікації та аутентифікації особи.

2.2 Завдання вивчення дисципліни

Завдання курсу полягає в ознайомленні студентів з основами побудови та використання систем захисту інформації в комп'ютерних системах, а також прищеплення практичних навиків роботи з існуючими сучасними системами захисту інформації, зокрема, криптографічними.

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

K11. Здатність застосовувати законодавчу та нормативно- правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії

K14. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

K20. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та ін их методів і засобів захисту інформації

2.4 Передумови для вивчення дисципліни

Зазначена дисципліна включена до циклу дисциплін професійної підготовки за переліком програми. У структурно-логічній схемі навчання зазначена дисципліна розміщена на IV-му курсі. Вивчення курсу "Захист інформації в комп'ютерних системах і мережах" передбачає наявність систематичних та ґрунтовних знань із дисциплін «Комп'ютерні системи», «Системи обробки розподілених баз даних», «Паралельні та розподілені комп'ютерні системи», цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи.

2.5. Результати навчання.

В результаті вивчення дисципліни студенти повинні:

ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПРН4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

ПРН6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

ПРН9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

3. Програма навчальної дисципліни

"Захист інформації в комп'ютерних системах і мережах"

Змістовий модуль 1. Основи систем захисту інформації у КС Тема

1. Вступ. Поняття захисту інформації.

Інформаційна безпека комп'ютерних систем. Вразливість комп'ютерних систем. Канали витоку інформації, атака та вторгнення в КС. Класифікація загроз безпеці інформації та інформаційним системам. Перехват, переривання. Модифікація та фальсифікація. Радіотехнічне, організаційне, комунікаційне, програмно-технічне.

Література: 1-3.

Тема 2. Політика безпеки інформації. Законодавча база захисту інформації в Україні.

Політика безпеки. Нормативно-правове та організаційне забезпечення безпеки. Комунікаційно-технічне забезпечення. Програмне забезпечення. Література: 2, 6, 8, 11.

Змістовий модуль 2. Управління доступом та розмежування прав доступу до інформації

Тема 3. Зміст етапів ідентифікації, авторизації та автентифікації користувачів.

Етапи ідентифікації, авторизації та автентифікації користувачів Прості паролі. Способи формування та реєстрації паролів. «Слабкі» паролі.

Характеристики парольного захисту.

Література: 1, 2, 12.

Тема 4. Модифікації системи паролів. Механізми розширення прав доступу.

Паролі одноразові, ідентифікатори, секретні функції, процедури «рукостискання». Списки доступу, мандатні списки. Механізми розширення прав доступу. Принцип мінімальних привілей.

Література: 1-3.

Змістовий модуль 3. Атаки на системи захисту інформації та методи захисту від них.

Тема 5. Основні типи атак та методи захисту від них.

Модель системи захисту Adept-50. Типи об'єктів та категорій. Модель простору безпеки Хартсона. Домени повноважень користувачів.

Література: 2, 5, 13, 14.

Тема 6. Канали витоку інформації. Сучасні атаки на реалізацію та відповідні методи протидії.

Модель системи захисту Бела і Лападули. Матриця прав доступу. Потоки запитів суб'єктів до об'єктів. Модель моніторингу безпеки. Лічильники небезпечних подій. Вектор індикації аномалій в діях користувачів.

Література: 2, 17.

Змістовий модуль 4. Захист інформації в комп'ютерних системах.

Тема 7. Найпростіші шифри.

Перестановки та підстановки. Шифри «Скітала», Полібія, Цезаря. Шифри Плейфера, Уїтстона. Шифрувальні таблиці. Роторні машини. Маскування. Шифр Вернама.

Література: 1, 3, 12, 14.

Тема 8. Симетричні криптоалгоритми.

Система Люцифер. Стандарт DES. Функція шифрування та управління ключами. Режими ECB,CBC,OFB,CFB.

Література: 1, 6, 9, 12.

Тема 9. Асиметричні криптоалгоритми.

Алгоритм асиметричного шифрування інформації. Алгоритм Діффі-Хелмана. Алгоритм Ель-Гамала.

Література: 1, 6, 12.

Тема 10. Електронний цифровий підпис.

Алгоритми цифрового підпису Blowfish, RC-5, CAST-128. Хеш-згортка
омлень. Алгоритми MD-5, SHA, ГОСТ 34.11-94.

Література: 4, 12.

Змістовий модуль 5. Захист інформації в комп'ютерних мережах.

Тема 11. Захист інформації в комп'ютерних та Wi-Fi мережах. Захист
нього зв'язку.

Особливості Wi-Fi мереж. Основні атаки в Wi-Fi мережах та методи ту від них. Захист мобільного зв'язку.

Література: 6, 7, 14.

Тема 12. Internet-банкінг, POS-термінали, банкомати. Методи захисту сових даних.

Поняття інтернет-банкінгу. Апаратні засоби здійснення платежів та методи істуту. Захист особистих фінансових даних.

атура: 4, 12.

4. Структура залікового кредиту дисципліни "Захист інформації в комп'ютерних системах мережах"

(денна форма навчання)

	Кількість годин					
	Лекції	Лабораторні заняття	Самостійна робота	Індивідуальна робота	Тренінг	Контрольні заходи
Змістовий модуль 1						
Тема 1. Вступ. Поняття захисту інформації.	2		6		2	опитування
Тема 2. Політика безпеки інформації. Законодавча база захисту інформації в Україні	2	4	3			опитування
Змістовий модуль 2						

Тема 3. Зміст етапів ідентифікації, авторизації та автентифікації користувачів..	2	4	5		2	опитування
Тема 4. Модифікації системи паролів. Механізми розширення прав доступу.	2	4	5			опитування
Змістовий модуль 3						
Тема 5. Основні типи атак та методи захисту від них	2	4	5	4	6	опитування
Тема 6. Канали витоку інформації. Сучасні атаки на реалізацію та відповідні методи протидії	4	4	5			опитування
Тема 7. Захист інформації в комп'ютерних системах..	4	2	5			опитування
Тема 8. Симетричні криптоалгоритми.	4	2	5			опитування
Тема 9. Асиметричні криптоалгоритми.	4	2	5			опитування
Тема 10. Електронний цифровий підпис.	4	2	5			опитування
Змістовий модуль 4						
Тема 11. Захист інформації в комп'ютерних та Wi-Fi мережах. Захист мобільного зв'язку.	8	2	5	1	4	опитування

Тема 12. Internet-банкінг, POS-термінали, банкомати. Методи захисту фінансових даних.	8		5			опитування
Разом	46	30	59	5	10	

(заочна форма навчання)

	Кількість годин		
	Лекції	Лабораторні заняття	Самостійна робота
Змістовий модуль 1			
Тема 1. Вступ. Поняття захисту інформації.			10
Тема 2. Політика безпеки інформації. Законодавча база захисту інформації в Україні	1	1	10
Змістовий модуль 2			
Тема 3. Зміст етапів ідентифікації, авторизації та автентифікації користувачів..		1	10
Тема 4. Модифікації системи паролів. Механізми розширення прав доступу.	1		10
Змістовий модуль 3			
Тема 5. Основні типи атак та методи захисту від них	1		10
Тема 6. Канали витоку інформації.			10

Тема 7. Захист інформації в комп'ютерних системах..	1		10
Тема 8. Симетричні криптоалгоритми.	1	1	10
Тема 9. Асиметричні криптоалгоритми.	1	1	10
Тема 10. Електронний цифровий підпис.	1		10
Змістовий модуль 4			
Тема 11. Захист інформації в комп'ютерних та Wi-Fi мережах. Захист мобільного зв'язку.	1		15
Тема 12. Internet-банкінг, POS-термінали, банкомати. Методи захисту фінансових даних.			18
Разом	8	4	138

5. Тематика лабораторних занять

Лабораторна робота №1.

Тема: Шифрування файлів та папок засобами Secure IT.

Мета: Вивчити засіб захисту інформації Secure IT.

Питання для обговорення:

1. Методи шифрування
2. Парольний захист.
3. Процедура дешифрування.

Література: 4, 9, 12.

Лабораторна робота №2.

Тема: Захист текстових документів в Microsoft Word.

Мета: Навчитися захищати документ засобами Microsoft Word.

Питання для обговорення:

1. Методи захисту.
2. Простий пароль.
3. Модифікація прав доступу.

Література: 2, 13.

Лабораторна робота №3.

Тема: Захист інформації засобами ОС Windows.

Мета: Навчитися захищати інформацію засобами ОС Windows.

Питання для обговорення: 1.

Технологія BitLocker.

2. Технологія AppLocker.

3. Батьківський контроль.

Література: 2, 5, 13.

Лабораторна робота №4.

Тема: Захист інформації за допомогою антивірусних програм.

Мета: Вивчити можливості сучасних антивірусних програм.

Питання для обговорення:

1. Антивірусні програми.

2. Функції мережевого екрана.

3. Журнал активності.

Література: 14, 17.

Лабораторна робота №5.

Тема: Розробка та дослідження засобів ідентифікації користувачів в комп'ютерних системах.

Мета: Навчитися здійснювати ідентифікацію користувачів комп'ютерних систем.

Питання для обговорення:

1. Процедура ідентифікації.

2. Методи ідентифікації.

3. Рівні захисту КС.

Література: 9, 13-15.

Лабораторна робота №6.

Тема: Розробка та дослідження засобів аутентифікації користувачів в комп'ютерних системах.

Мета: Навчитися здійснювати аутентифікацію користувачів комп'ютерних систем.

Питання для обговорення:

1. Процедура аутентифікації.
2. Методи аутентифікації.
3. Процедура авторизації.

Література: 9, 13-15.

Лабораторна робота №7.

Тема: Дослідження засобів створення та використання електронних цифрових підписів користувачів в комп'ютерних системах.

Мета: Навчитися створювати та застосовувати електронний підпис користувачів комп'ютерних систем.

Питання для обговорення:

1. Процедура аутентифікації.
2. Методи аутентифікації.
3. Процедура авторизації.

Література: 9, 13-15.

8 Організація та проведення тренінгу з дисципліни «Захист інформації в комп'ютерних системах»

№	Вид роботи	Порядок проведення тренінгу п/п
1	Огляд сучасних засобів захисту – розгляд сучасних програмних та інформації комп'ютерної системи апаратних засобів захисту інформації, що відповідають ДСТУ;	– вибір засобу захисту відповідно до політики безпеки
2	Розгляд процесу розробки – постановка завдання; політики безпеки – вибір методів захисту інформації, відповідно до ТЗ;	– опис апаратних та програмних засобів захисту інформації; – аналіз стійкості розробленої системи захисту
3	Розробка політики безпеки згідно – розробка та аналіз ТЗ; індивідуального завдання –	– опис вибраних апаратних та програмних засобів захисту інформації;

вибір методів захисту інформації;	– аналіз стійкості розробленої системи захисту
-----------------------------------	--

7. Самостійна робота студентів

(денна форма навчання)

№ п/п	Тематика	Завдання
1	Законодавчі аспекти захисту інформації.	Розробка концепції політики безпеки згідно предметної області
2	Основні загрози безпеки інформації. Забезпечення безпеки інформації в комп'ютерних системах і мережах.	
3	Проблема ідентифікації користувача та механізми підтвердження його істинності.	Розробка системи ідентифікації користувача системи
4	Основні поняття і концепції ідентифікації та електронного цифрового підпису.	
5	Проблема ідентифікації користувача та механізми підтвердження його істинності.	
6	Основні поняття і концепції ідентифікації та електронного цифрового підпису.	
7	Взаємна перевірка істинності користувачів.	
8	Біометрична ідентифікація особи.	
9	Електронний цифровий підпис.	
10	Вітчизняні стандарти електронного цифрового підпису.	
11	Особливості функціонування міжмережевих екранів.	Розробка моделі захисту даних в мережі
12	Основні компоненти міжмережевих екранів.	
13	Фільтруючі маршрутизатори.	

(заочна форма навчання)

№ п/п	Тематика
-------	----------

1	Законодавчі аспекти захисту інформації.
2	Основні загрози безпеки інформації. Забезпечення безпеки інформації в комп'ютерних системах і мережах.
3	Проблема ідентифікації користувача та механізми підтвердження його істинності.
4	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
5	Проблема ідентифікації користувача та механізми підтвердження його істинності.
6	Основні поняття і концепції ідентифікації та електронного цифрового підпису.
7	Взаємна перевірка істинності користувачів.
8	Біометрична ідентифікація особи.
9	Електронний цифровий підпис.
10	Вітчизняні стандарти електронного цифрового підпису.

8. Засоби оцінювання та методи демонстрування результатів навчання

У навчальному процесі застосовуються: лекції, в тому числі з використанням мультимедіапроектора та інших ТЗН; практичні заняття; індивідуальні заняття, самостійна робота студента, робота в Інтернет.

У процесі вивчення дисципліни "Захист інформації в комп'ютерних системах" використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточні опитування;
- модульне тестування та опитування;
- презентації результатів виконання завдань та досліджень;
- оцінювання результатів виконання завдань тренінгу;
- оцінювання результатів самостійної роботи студентів;
- екзамен.

10. Критерії, форми поточного та підсумкового контролю

В процесі вивчення дисципліни "Захист інформації в комп'ютерних системах" використовуються наступні методи оцінювання навчальної роботи студента:

- поточне тестування та опитування;
- підсумкове тестування по кожному змістовому модулю;

- підсумкова оцінка за виконання завдань тренінгу;
- оцінювання наскрізного проекту у результаті самостійної роботи;
- підсумковий екзамен.

Підсумковий бал (за 100-бальною шкалою) з дисципліни "Захист інформації в комп'ютерних систем" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

6 семестр

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 1	Тренінги	Самостійна робота	Екзамен
Середнє арифметичне за 3 лабораторних роботи	Тестові завдання	Середнє арифметичне за 4 лабораторних роботи	Письмова робота: 2 теоретичних питання, 1 задача, тестові завдання	Виконання 3 завдань	Виконання наскрізного проекту із 3 завдань	2 теоретичних питання 2 по 25 балів = 50 балів, Задача = 50 балів

Оцінка за поточне опитування визначається як середнє арифметичне з оцінок, отриманих за виконання та захист лабораторних робіт:

90–100 балів – студент у повному обсязі володіє навчальним матеріалом, необхідним для виконання лабораторної роботи, вільно та аргументовано розкриває зміст виконаних завдань, дає правильні відповіді на теоретичні питання, звіт про виконання лабораторної роботи оформлено згідно вимог;

75–89 балів – студент достатньо володіє навчальним матеріалом, необхідним для виконання лабораторної роботи, аргументовано розкриває зміст виконаних завдань, але допускає окремі несуттєві неточності та незначні помилки, звіт про виконання лабораторної роботи оформлено згідно вимог;

65–74 бали – студент в цілому володіє навчальним матеріалом, необхідним для виконання лабораторної роботи, викладає основний зміст виконаних завдань, допускаючи при цьому окремі суттєві неточності та помилки, звіт про виконання лабораторної роботи оформлено з порушеннями вимог;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, необхідним для виконання лабораторної роботи, фрагментарно виконує завдання, допускаючи при цьому суттєві неточності, звіт про виконання лабораторної роботи оформлено з порушеннями вимог;

1–59 балів – не володіє навчальним матеріалом, необхідним для виконання лабораторної роботи, завдання здебільшого не виконані, звіт про

виконання лабораторної роботи оформлено з порушеннями вимог або не представлено.

Оцінка за тренінг визначається як середнє арифметичне з оцінок, отриманих за виконання завдань тренінгу:

90–100 балів – у повному обсязі володіє навчальним матеріалом, самостійно та аргументовано його використовує під час виконання завдань тренінгу, виявляє творчий підхід до виконання завдань;

75–89 балів – достатньо повно володіє навчальним матеріалом, але при виконанні окремих завдань тренінгу не вистачає достатньої аргументації його використання, допускаються при цьому окремі несуттєві неточності та незначні помилки, загалом виявляє ініціативу та творчий підхід до виконання завдань;

65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при виконанні завдань тренінгу, але без глибокого всебічного аналізу та обґрунтування, допускаючи при цьому суттєві неточності та помилки, в окремих моментах виявляє творчий підхід до виконання завдань;

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно його використовує, завдання тренінгу виконує, допускаючи при цьому суттєві неточності, не виявляє творчого підходу до виконання завдань;

1–59 – не володіє навчальним матеріалом, не розкриває зміст завдань тренінгу, не бере участі у колективних завданнях під час проведення тренінгу.

Оцінка за самостійну роботу визначається як середнє арифметичне з оцінок, отриманих за розроблене технічне завдання, його оформлення та обґрунтування:

90–100 балів – виконані завдання самостійної роботи повністю відповідають встановленим вимогам, містять елементи самостійного дослідження, свідчать про високий рівень опанування навчального матеріалу, студент на високому рівні виявляє творчий підхід до виконання завдань;

75–89 балів – виконані завдання самостійної роботи в основному відповідають встановленим вимогам, свідчать про належний рівень опанування навчального матеріалу, студент виявляє творчий підхід до виконання завдань, але є деякі несуттєві недопрацювання за окремими завданнями;

60–74 балів – поставлені завдання виконані на недостатньому рівні, свідчать про недостатній рівень опанування навчального матеріалу; студент припускається значних помилок при виконанні завдань, лише в окремих моментах виявляє творчий підхід до виконання завдань;

1–59 балів – завдання практично не виконані; допущені грубі помилки при вирішенні завдань, що свідчить про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до виконання завдань.

Модульна контрольна робота складається із 25 тестів, за правильну відповідь на кожен із яких студент може отримати 4 бали.

Екзамен – вид контролю, при якому засвоєння студентом теоретичного та практичного матеріалу оцінюється від 0 до 100 балів як сума балів за виконані завдання.

Екзаменаційний білет складається із:

- двох теоретичних питань, за відповідь на кожне із яких студент може отримати максимум 50 балів, що в підсумку становить максимально 100 балів:

25–35 балів – у повному обсязі володіє навчальним матеріалом, всебічно та аргументовано його викладає, дає правильні відповіді на додаткові запитання;

15–24 бали - достатньо володіє навчальним матеріалом, але при висвітленні деяких питань не вистачає глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки;

1–14 балів – в цілому володіє навчальним матеріалом, але не в повному обсязі, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичного питання, допускаючи при цьому суттєві неточності, відповіді на додаткові запитання нечіткі;

- практичного завдання, за виконання якого студент може отримати максимум 30 балів:

25–30 балів – у повному обсязі володіє навчальним матеріалом, правильно виконує практичне завдання та аналізує отримані результати, демонструє самостійність виконання;

10–24 балів – у достатньому обсязі володіє навчальним матеріалом, правильно виконує практичне завдання, допускає неточності та/або фрагментарно (без аргументації) інтерпретує отримані результати, демонструє самостійність виконання, але на додаткові запитання відсутня повна відповідь;

1–9 балів – не в повному обсязі володіє навчальним матеріалом, фрагментарно виконує практичне завдання, допускає суттєві неточності, поверхнево відповідає на додаткові запитання.

Шкала оцінювання:

За шкалою університету	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)

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

№	Найменування	Номер теми
1.	Антивірусні програми, фаєрволи	5, 6
2.	Операційні системи	3, 4, 6
3.	Secure IT	8, 9
4.	Java, C++, Python Trial Version	10-12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах. Ужгород: УжНУ, 2021 184 с.
2. Гребенюк А.М. Управління інформаційною безпекою: конс. лекцій. ДніпроЖ: ДДУВС, 2019. 68 с.
3. Державна служба спеціального зв'язку та захисту інформації України: вебсайт. URL: <https://cip.gov.ua/ua/news> (дата звернення 25.08.2022).
4. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. К.: Вид-во DIRECTLINE, 2019. 714 с.
5. Binance academy: веб-сайт. URL: <https://academy.binance.com/uk> (дата звернення 22. 08. 2022).
6. Остапов С.Е. Кібербезпека: сучасні технології захисту / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – К.:Новий світ-2000, 2020. – 678 с. 17. Хорошко В. О. Проектування комплексних систем захисту інформації./ В.О. Хорошко. – Львів: Видавництво Львівської політехніки, 2020. – 317 с.
7. Massimo Bertaccini, Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption , Packt Publishing, 2022. – 325 p.