

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ  
«ІРПІНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ  
БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»

Циклова комісія фундаментальних дисциплін та комп'ютерних технологій

ЗАТВЕРДЖУЮ

Заступник директора

з навчальної роботи

Викторія СОВА

2025 року



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Захист інформації в комп'ютерних системах»

(назва навчальної дисципліни)

галузь знань

**12 Інформаційні технології**

(шифр і назва галузі знань)

освітньо-професійна  
програма

**Комп'ютерна інженерія**

спеціальність

**123 Комп'ютерна інженерія**

відділення

**Інформаційних технологій**

(назва відділення)

Робоча програма

Захист інформації в комп'ютерних системах

(назва навчальної дисципліни)

для студентів  
за галуззю знань

12 Інформаційні технології

спеціальністю  
освітньо-професійна  
програма

123 Комп'ютерна інженерія

Комп'ютерна інженерія

«28» серпня 2025 року, - 12 с.

Розробник: **Вадим ПЕЧКУРОВ**, викладач першої кваліфікаційної категорії

Робоча програма затверджена на засіданні циклової комісії фундаментальних дисциплін та комп'ютерних технологій  
Протокол від «29» серпня 2025 року № 1

Голова циклової комісії фундаментальних дисциплін та комп'ютерних технологій



Е. Дібрівна

Схвалено методичною радою коледжу.  
Протокол від «29» серпня 2025 року № 1

Голова



Д. Костюк

## 1. Опис навчальної дисципліни

Найменування показників	Галузь знань, освітньо-професійна програма, освітньо-професійний ступінь	Характеристика навчальної дисципліни
		денна форма здобуття освіти
Кількість кредитів – 5	Галузь знань: 12 Інформаційні технології	Вибіркова
Модулів – 3	Спеціальність: 123 Комп'ютерна інженерія Освітньо-професійна програма: Комп'ютерна інженерія	Рік підготовки:
Загальна кількість годин – 150		4-й
		Семестр:
		7-й
		Лекції:
Тижневих годин для денної форми здобуття освіти: аудиторних – 7 самостійної роботи – 6	Освітньо-професійний ступінь: фаховий молодший бакалавр	36 год.
		Практичні:
		48 год.
		Лабораторні:
		–
		Самостійна робота:
		66 год.
		Вид контролю:
		Диференційований залік

**Примітка.** Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить: 84/66

## 2. Мета навчальної дисципліни

Мета дисципліни – ознайомлення студентів з сутністю, задачами, принципами та сучасними інформаційними технологіями захисту інформації в комп'ютерних системах (КС), методологічними та законодавчими основами організації, планування та впровадження систем захисту інформації, а також основним аспектам практичної діяльності по їх створенню, забезпеченню функціонування та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення загроз зі сторони потенційних порушників..

Перелік компетентностей студентів, що формуються в результаті засвоєння дисципліни:

### **Загальних компетентностей (ЗК):**

ЗК3. Здатність до абстрактного мислення, аналізу і синтезу;

ЗК4. Здатність застосовувати знання у практичних ситуаціях;

ЗК8. Здатність вчитися і оволодівати сучасними знаннями.

### **Спеціальних компетентностей (СК):**

СК3. Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями, прикладними та спеціалізованими комп'ютерно-інтегрованими середовищами для розробки, впровадження та обслуговування апаратних та програмних засобів комп'ютерної інженерії.

СК4. Здатність брати участь у розробці системного та прикладного програмного забезпечення засобів комп'ютерної інженерії з використанням ефективних алгоритмів, сучасних методів і мов програмування.

СК5. Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

СК9. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

СК10. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.

СК12. Здатність створювати, впроваджувати, адмініструвати бази даних і знань з використанням сучасних методів, технологій та систем керування базами даних.

СК13. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їх компонентів шляхом використання аналітичних методів і методів моделювання.

СК15. Здатність аналізувати, оптимізувати та моделювати складність архітектури комп'ютерних систем і мереж із застосуванням сучасних принципів побудови математичного, програмного, лінгвістичного, технічного та інформаційного забезпечення;

СК16. Знання та розуміння математичних моделей інформаційної безпеки та методів оцінювання захищеності комп'ютерних мережевих систем;

### **3. Передумови вивчення навчальної дисципліни**

Дана навчальна дисципліна базується на раніше здобутих результатах навчання таких дисциплін як: «Архітектура комп'ютерів» та «Програмування».

### **4. Очікувані результати навчання**

#### **Програмні результати навчання (РН):**

РН2. Знати і розуміти теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп'ютерної інженерії;

РН3. Знати сучасні методи та технології для розв'язання прикладних задач комп'ютерної інженерії.

РН6. Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп'ютерної інженерії.

РН7. Застосовувати знання для формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

РН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності.

РН9. Розробляти, тестувати, впроваджувати, експлуатувати програмне забезпечення для вбудованих і розподілених систем;

РН11. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності;

РН12. Вміти розробляти, тестувати, впроваджувати, експлуатувати програмне забезпечення для вбудованих і розподілених систем;

РН14. Вміти ефективно працювати як індивідуально, так і у складі команди при вирішенні технічних та організаційних задач у професійній діяльності;

РН15. Вміти ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів комп'ютерної інженерії;

### **5. Критерії оцінювання**

Критерії оцінювання знань студентів наведено в додатку до робочої програми навчальної дисципліни.

### **6. Засоби оцінювання**

Контрольні заходи включають поточний, модульний та підсумковий контроль знань студента.

Поточний контроль здійснюється шляхом оцінювання лабораторних робіт та у процесі здійснення самостійної роботи у таких формах: експрес-опитування, тести, задачі, захист звітів з лабораторної роботи, робота в Інтернет тощо.

Модульний контроль проводиться з метою оцінки результатів навчання студентів на визначених його етапах.

Підсумковий контроль проводиться з метою оцінки результатів навчання на завершальному етапі.

## **7. Програма навчальної дисципліни**

### **Модуль 1. Основні поняття та законодавча база**

#### **Тема 1. Основні поняття захисту інформації та загрози безпеки в комп'ютерних системах (КС)**

Поняття інформації та інформаційних систем. Типи інформації. Поняття захисту інформації. Види інформаційної небезпеки. Програмні засоби захисту.

#### **Тема 2. Правові та організаційні методи захисту інформації в КС. Основи побудови комплексів захисту в КС**

Правове регулювання в галузі безпеки інформації. Політика держави в області безпеки інформаційних технологій. Законодавча база. Організаційні методи захисту інформації. Комплекси захисту в КС.

#### **Тема 3. Вразливості та загрози безпеки інформації в КС**

Поняття вразливості КС. Класифікація вразливостей. Фундаментальні недоліки в дизайні ОС. Шкідливе програмне забезпечення.

### **Модуль 2. Типові загрози та методи захисту у різних середовищах**

#### **Тема 4. Вірусологія. Комп'ютерні віруси та механізми боротьби з ними**

Поняття комп'ютерного вірусу. Механізми «зараження» та фази розвитку. Відомі віруси та принципи їх дій.

#### **Тема 5. Захист інформації в КС від випадкових загроз**

Дублювання інформації. Підвищення надійності та відмовостійкості КС. Блокування помилкових операцій. Оптимізація взаємодії користувачів і обслуговуючого персоналу з КС. Мінімізація збитку від аварій і стихійних лих.

#### **Тема 6. Захист операційних систем персональних комп'ютерів та мобільних гаджетів**

Ідентифікація, встановлення достовірності. Методи паролювання. Поняття антивірусу. Антивірусне ПЗ.

#### **Тема 7. Захист інформації дата-центрів, офісних та промислових СУБД**

Організація безпечного зберігання інформації у ЦОД. Поняття бази даних та основні методи захисту інформації в ній. Моделі безпеки БД. Процедури ідентифікації, аутентифікації і авторизації в СУБД

### **Модуль 3. Фізичні та перспективні методи та засоби захисту**

#### **Тема 8. Методи і засоби захисту інформації в КС від традиційного шпигунства і диверсій**

Система охорони об'єкта КС. Інженерні конструкції та засоби спостереження. Підсистема доступу на об'єкт. Організація робіт з конфіденційними інформаційними ресурсами на об'єктах КС. Протидія спостереженню в оптичному діапазоні та підслуховуванню. Захист від зловмисних дій обслуговуючого персоналу і користувачів.

#### **Тема 9. Методи і засоби захисту від електромагнітного випромінювання і наведень**

Поняття ЕМВ та ЕМІ. Пасивні методи захисту від побічних електромагнітних випромінювань і наведень. Активні методи захисту від ПЕМВН.

#### **Тема 10. Перспективні напрями розвитку засобів захисту інформації**

Квантова криптографія. Штучний інтелект. Blockchain. AR та VR у тренінгу кадрів.

#### **Тема 11. Криптографічні методи і засоби захисту інформації**

Загальні відомості про криптографію. Класифікація методів криптографічного перетворення інформації. Шифрування та стиснення інформації.

#### **Тема 12. Штучний інтелект в засобах захисту інформації**

Обмеження класичних систем ШІ. Можливості генеративних моделей. Генеративний ШІ в

руках хакерів. Проблеми згенерованого коду.

### Тема 13. Нейронні мережі в засобах захисту інформації

Передумови застосування штучних нейронних мереж. Нейронні мережі, що самонавчаються. Ймовірнісні нейронні мережі. Класичні асоціативні нейронні мережі. Принципи розробки модельного програмного комплексу.

## 8. Структура навчальної дисципліни

Назви модулів і тем	Кількість годин					
	Усього	у тому числі				
		л	п	лаб	інд	с.р.
<b>Модуль 1. Основні поняття та законодавча база</b>						
Тема 1. Основні поняття захисту інформації та загрози безпеки в комп'ютерних системах (КС)	9	2	2			5
Тема 2. Правові та організаційні методи захисту інформації в КС. Основи побудови комплексів захисту в КС	10	2	4			4
Тема 3. Вразливості та загрози безпеки інформації в КС	10	4	3			3
Модульна контрольна робота №1	1		1			
Разом за модулем 1	30	8	10			12
<b>Модуль 2. Типові загрози та методи захисту у різних середовищах</b>						
Тема 4. Вірусологія. Комп'ютерні віруси та механізми боротьби з ними	15	4	4			7
Тема 5. Захист інформації в КС від випадкових загроз	15	4	4			7
Тема 6. Захист операційних систем персональних комп'ютерів та мобільних гаджетів	15	4	4			7
Тема 7. Захист інформації дата-центрів, офісних та промислових СУБД	14	4	3			7
Модульна контрольна робота №2	1		1			
Разом за модулем 2	60	16	16			28
<b>Модуль 3. Фізичні та перспективні методи та засоби захисту</b>						
Тема 8. Методи і засоби захисту інформації в КС від традиційного шпигунства і диверсій	10	2	4			4
Тема 9. Методи і засоби захисту від електромагнітного випромінювання і наведень	10	2	4			4
Тема 10. Перспективні напрями розвитку засобів захисту інформації	10	2	4			4
Тема 11. Криптографічні методи і засоби захисту інформації	10	2	4			4
Тема 12. Штучний інтелект в засобах захисту інформації	10	2	4			4
Тема 13. Нейронні мережі в засобах захисту інформації	9	2	1			6
Модульна контрольна робота №3	1		1			
Разом за модулем 3	60	12	22			26
Усього годин	150	36	48			66

### 9. Теми семінарських занять

№ з/п	Назва теми та зміст семінарських занять	Кількість годин
1	Не передбачено навчальним планом	

### 10. Теми практичних занять

№ з/п	Назва теми та зміст практичних занять	Кількість годин
1	Тема 1. Основні поняття захисту інформації та загрози безпеки в комп'ютерних системах (КС) 1. Дослідження основних компонентів захисту інформації в ОС сімейства Windows.	2
2	Тема 2. Правові та організаційні методи захисту інформації в КС. 1. Основи побудови комплексів захисту в КС	4
3	Тема 3. Вразливості та загрози безпеки інформації в КС 1. Дослідження методів пошуку вразливостей та загроз у КС. Модульна контрольна робота №1	3 1
4	Тема 4. Вірусологія. Комп'ютерні віруси та механізми боротьби з ними 1. Дослідження процесів захисту інформації від комп'ютерних вірусів та принципів впливу окремих вірусів на КС.	4
5	Тема 5. Захист інформації в КС від випадкових загроз 1. Дослідження методів захисту КС від випадкових загроз.	4
6	Тема 6. Захист операційних систем персональних комп'ютерів та мобільних гаджетів 1. Дослідження та налагодження програмних засобів захисту інформації у різних ОС.	4
7	Тема 7. Захист інформації дата-центрів, офісних та промислових СУБД 1. Дослідження архітектури та принципів захисту інформації дата-центрів. 2. Модульна контрольна робота №2	3 1
8	Тема 8. Методи і засоби захисту інформації в КС від традиційного шпигунства і диверсій 1. Налаштування та дослідження параметрів адресації робочих станцій на базі ОС Windows та Linux.	4
9	Тема 9. Методи і засоби захисту від електромагнітного випромінювання і наведень 1. Налаштування та дослідження базових засобів захисту мережевої ОС Cisco IOS та мережевого обладнання Cisco.	4
10	Тема 10. Перспективні напрями розвитку засобів захисту інформації 1. Дослідження процесів та методів захисту інформації від кібер. атак.	4
11	Тема 11. Криптографічні методи і засоби захисту інформації. 1. Дослідження технологій симетричного та асиметричного шифрування та їх уразливості.	4
12	Тема 12. Штучний інтелект в засобах захисту інформації 1. Дослідження технологій симетричного та асиметричного шифрування та їх уразливості.	4
13	Тема 13. Нейронні мережі в засобах захисту інформації 1. Дослідження технологій аутентифікації та ідентифікації в розподілених комп'ютерних системах. 2. Модульна контрольна робота №3	1 1
	Разом:	48

### 11. Теми лабораторних занять

№ з/п	Назва теми та зміст лабораторних занять	Кількість годин
1	Назва теми та зміст лабораторних занять	

### 12. Самостійна робота

№ з/п	Назва теми та зміст самостійної роботи	Кількість годин
1	Тема 1. Основні поняття захисту інформації та загрози безпеки в комп'ютерних системах (КС). 1. Види інформаційної небезпеки. 2. Програмні засоби захисту.	5
2	Тема 2. Правові та організаційні методи захисту інформації в КС. Основи побудови комплексів захисту в КС. 1. Організаційні методи захисту інформації. 2. Комплекси захисту в КС.	4
3	Тема 3. Розпізнавання атак та вразливостей комп'ютерних систем. 1. Фундаментальні недоліки в дизайні ОС. 2. Шкідливе програмне забезпечення.	3
4	Тема 4. Вірусологія. Комп'ютерні віруси та механізми боротьби з ними. 1. Відомі віруси та принципи їх дій.	7
5	Тема 5. Захист інформації в КС від випадкових загроз. 1. Оптимізація взаємодії користувачів і обслуговуючого персоналу з КС. 2. Мінімізація збитку від аварій і стихійних лих.	7
6	Тема 6. Захист операційних систем персональних комп'ютерів та мобільних гаджетів. 1. Поняття антивірусу. Антивірусне ПЗ.	7
7	Тема 7. Захист інформації дата-центрів, офісних та промислових систем управління базами даних. 1. Процедури ідентифікації, аутентифікації і авторизації в СУБД.	7
8	Тема 8. Методи і засоби захисту інформації в КС від традиційного шпигунства і диверсій. 1. Протидія спостереженню в оптичному діапазоні та підслуховуванню. 2. Захист від зловмисних дій обслуговуючого персоналу і користувачів.	4
9	Тема 9. Методи і засоби захисту від електромагнітного випромінювання і наведень. 1. Активні методи захисту від ПЕМВН.	4
10	Тема 10. Перспективні напрями розвитку засобів захисту інформації.	4
11	Тема 11. Криптографічні методи і засоби захисту інформації. Шифрування та стиснення інформації	4
12	Тема 12. Штучний інтелект в засобах захисту інформації. 1. Генеративний ШІ в руках хакерів. 2. Проблеми згенерованого коду.	4
13	Тема 13. Нейронні мережі в засобах захисту інформації. 1. Класичні асоціативні нейронні мережі. 2. Принципи розробки модельного програмного комплексу.	6
	Разом:	66

### 13. Індивідуальні завдання

Не передбачено навчальним планом.

#### 14. Інструменти, обладнання, програмне забезпечення

При вивченні дисципліни використовується середовище MS PowerPoint для створення презентацій та навчально-інформаційне середовище MOODLE, також використовується потрібне для виконання лабораторних робіт програмне забезпечення типу Total Commander, VirtualBox, антивірусне ПЗ та інше.

#### 15. Розподіл балів, які отримують студенти

Модуль №1 20				Модуль №2 35					Модуль №3 45						Всього балів	
T1	T2	T3	МКР 1	T4	T5	T6	T7	МКР 2	T8	T9	T10	T11	T12	T13		МКР 3
ПЗ 1	ПЗ 2-3	ПЗ 4-5		ПЗ 6-7	ПЗ 8-9	ПЗ 10-11	ПЗ 12-13		ПЗ 14-15	ПЗ 16-17	ПЗ 18-19	ПЗ 20-21	ПЗ 22-23	ПЗ 24		
4	5	5	6	6	6	6	6	11	5	5	5	6	6	5	13	100

#### 16. Рекомендовані джерела інформації

##### ЗАКОНОДАВЧІ ТА НОРМАТИВНІ ДОКУМЕНТИ

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (чинна редакція станом на 07.09.2025). URL:

<https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII (чинна редакція 07.09.2025). URL: <https://zakon.rada.gov.ua/laws/show/2163-19>

3. Про інформацію : Закон України від 02.10.1992 № 2657-XII (чинна редакція станом на 07.09.2025). URL: <https://zakon.rada.gov.ua/laws/show/2657-12>

4. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Системи управління безпекою інформації. Вимоги (ISO/IEC 27001:2022, IDT). – Київ : ДП «УкрНДНЦ», 2023. URL: [https://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=106197](https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=106197)

5. ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кібербезпека та захист приватності. Списки заходів з інформаційної безпеки (ISO/IEC 27002:2022, IDT). – Київ : ДП «УкрНДНЦ», 2023. URL: [https://webshop.ukrndnc.org.ua/index.php?route=product/product&product\\_id=280468](https://webshop.ukrndnc.org.ua/index.php?route=product/product&product_id=280468)

##### ОСНОВНА

##### Підручники (навчальні посібники)

6. Гапак, О. М.; Балага, С. І. Захист інформації в комп'ютерних системах : підручник. – Ужгород : ДВНЗ «УжНУ», 2021. – 184 с.

7. Гушин, І. В.; Киричок, О. В.; Куклін, В. М. Вступ до методів організації та оптимізації нейромереж : навч. посіб. – Харків : ХНУ ім. В. Н. Каразіна, 2021. – 152 с.

8. Жилін, А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 180 с.

9. Козюра, В. Д.; Хорошко, В. О.; Шелест, М. Є.; Ткач, Ю. М.; Балюнов, О. О. Захист інформації в комп'ютерних системах : підручник. – Ніжин : ФОП Лук'яненко В. В.; ТПК «Орхідея», 2020. – 236 с.

10. Манжай О. В., Манжай І. А. Правові засади захисту інформації: підручник. Харків : Панов, 2020. 162 с.

11. Остапов, С. Є.; Євсєєв, С. П.; Король, О. Г. Кібербезпека: сучасні технології захисту : навч. посіб. – Харків : Новий Світ-2000, 2020. – 678 с.

12. Смірнов, О. А.; Коноплицька-Слободенюк, О. К.; Смірнов, С. А.; Буравченко, К. О.; Смірнова, Т. В.; Книшук, А. В. Вступ до кібербезпеки : навч. посіб. – Кропивницький : ЦНТУ, 2022. – 967 с.

13. Терейковський, І. А.; Бушуєв, Д. А.; Терейковська, Л. О. Штучні нейронні мережі: базові положення : навч. посіб. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 271 с.
14. Терейковський, І. А.; Гнатюк, С. О. Захист інформації в комп'ютерних системах : навч. посіб. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 135 с.
15. Шевченко, А. І. (ред.) Стратегія розвитку штучного інтелекту в Україні : монографія. – Київ : Інститут проблем штучного інтелекту МОН і НАН України, 2023. – 460 с.
16. Юдін, О. К.; Корченко, О. Г.; Конахович, Г. Ф. Захист інформації в мережах передачі даних : підручник. – Київ : DIRECTLINE, 2019. – 714 с.

#### **ДОПОМІЖНА**

17. Bishop, M. Computer Security: Art and Science. 3rd ed. – Boston : Addison-Wesley, 2018. – 1376 p.
18. Anderson, R. Security Engineering : A Guide to Building Dependable Distributed Systems. 3rd ed. – Hoboken : Wiley, 2020. – 1232 p.
19. Katz, J.; Lindell, Y. Introduction to Modern Cryptography. 3rd ed. – Boca Raton : CRC Press, 2020. – 611 p.

#### **ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ**

1. Security and Privacy Controls for Information Systems and Organizations <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
2. Zero Trust Architecture <https://csrc.nist.gov/publications/detail/sp/800-207/final>
3. AI Risk Management Framework <https://www.nist.gov/itl/ai-risk-management-framework>
4. Науково-технічна бібліотека ім. Г. Денисенка <http://www.library.kpi.ua/>
5. Наукова періодика України. Електронний ресурс: <http://journals.uran.ua/>
6. Діагностичні програми. – <https://biblprog.org.ua/ua/diagnostic/>
7. Офіційний сайт Cisco – <https://www.netacad.com/ru/courses/all-courses>
8. <https://www.aida64.com/>
9. <https://www.oracle.com/>
10. <https://www.acronis.com/>
11. <https://www.techpowerup.com/>
12. <https://www.cpubid.com/>
13. <https://www.hwinfo.com/>
14. <https://www.3dmark.com/>

## **КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАТЬ СТУДЕНТІВ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»**

### **Для денної форми здобуття освіти**

Оцінювання знань студентів здійснюється за 100-бальною шкалою (поточний, модульний та підсумковий контроль (диференційований залік).

Робочою програмою дисципліни передбачено вивчення 3-х розділів обсягом 150 годин (5 кредитів ЄКТС):

1 модуль – 1 (30 год) – 20 балів;

2 модуль – 2 (60 год) – 35 балів.

3 модуль – 2 (60 год) – 45 балів;

Робочою програмою навчальної дисципліни передбачено застосування 3-х форм контролю знань студентів: поточного, модульного, підсумкового.

#### **1. Поточний контроль.**

Поточний контроль здійснюється у формі усних відповідей, доповнень на практичних заняттях, письмового опитування, розв'язування задач, виконання тестів тощо.

За кожним елементом модуля, передбаченого робочою програмою, обов'язкова певна форма поточного оцінювання знань.

Такими формами можуть бути:

- письмова контрольна робота (відповіді на питання лекційного курсу, розв'язання задач тощо);

- тестування знань студентів з певного розділу (теми) або з певних окремих питань лекційного курсу;

- перевірка розв'язання завдань (задачі, вправи) тощо.

#### **Критеріями оцінки є:**

##### **На практичному занятті оцінюються:**

- розуміння теоретичних основ;
- виконання практичних завдань;
- аналіз та вирішення проблем;
- часові рамки та ефективність;
- усні відповіді на контрольні питання.

##### **Оцінювання самостійної роботи студента.**

Контроль самостійної роботи студентів здійснюється як під час аудиторних занять (на семінарах, практичних заняттях), так і у позааудиторний час.

Контроль самостійної роботи передбачає:

- визначення ступеня засвоєння матеріалу;
- визначення якості виконання завдань;
- своєчасне виконання і здача поточних завдань;
- оцінку знань, здобутих у результаті самостійної навчальної роботи.

#### **2. Модульний контроль.**

Кожен модуль завершується виконанням студентом модульної контрольної роботи. Модульний контроль є підсумком певного етапу вивчення навчальної дисципліни. Його мета – виявлення проміжних результатів засвоєння студентами змісту навчальної дисципліни. На модульну контрольну роботу передбачено 30% від суми балів, виділених на модуль. Модульна контрольна робота проводиться у тестовій письмовій формі. Критерії оцінювання знань за модульну контрольну роботу наводиться у пояснювальній записці до неї. Оцінка за модуль визначається як сума набраних балів за поточну роботу та за модульну контрольну роботу.

#### **3. Підсумковий контроль.**

Формою підсумкового контролю з дисципліни «Захист інформації в комп'ютерних системах» є диференційований залік, який виставляється виключно за результатами поточного

та модульного контролю (сума набраних балів за всі модулі). Залік виставляється під час останнього практичного заняття.

Залежно від балів, отриманих за кожний вид навчальної роботи, студент одержує суму балів, яка переводиться в національну оцінку за відповідною шкалою згідно з табл.1:

**Таблиця 1. Переведення рейтингу студента за 100-бальною шкалою в оцінку за національною шкалою**

Рейтинг студента, бали	Оцінка національна
90-100	Відмінно
74-89	Добре
60-73	Задовільно
0-59	Незадовільно

Оцінка «**Відмінно**» виставляється студенту, який систематично працював протягом семестру, показав різнобічні і глибокі знання програмного матеріалу, вмів успішно виконувати завдання, які передбачені програмою, засвоїв зміст основної та додаткової літератури, усвідомив взаємозв'язок окремих розділів навчальної дисципліни, їхнє значення для майбутньої професії, виявив творчі здібності у розумінні та використанні навчально-програмного матеріалу, проявив здатність до самостійного оновлення і поповнення знань.

Оцінка «**Добре**» виставляється студенту, який виявив повне знання навчально-програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу, що рекомендована програмою, показав достатній рівень знань з навчальної дисципліни і здатний до їх самостійного оновлення та поповнення у ході подальшого навчання та професійної діяльності.

Оцінка «**Задовільно**» виставляється студенту, який виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та наступної роботи за професією, справляється з виконанням завдань, передбачених програмою, допустив окремі похибки при виконанні екзаменаційних завдань, але володіє необхідними знаннями для подолання допущених похибок під керівництвом педагогічного працівника.

Оцінка «**Незадовільно**» виставляється студенту, який не виявив достатніх знань основного навчально-програмного матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань, не може без допомоги викладача використати знання при подальшому навчанні, не спромігся оволодіти навичками самостійної роботи.