МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ «РІВНЕНСЬКИЙ ФАХОВИЙ КОЛЕДЖ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ»

Циклова комісія *програмування та інформаційних дисциплін*

ЗАТВЕРДЖУЮ
Заступник директора
з навчальної роботи
29 серпня 2025 р.
_____ Людмила БАЛДИЧ

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Прикладна криптографія

(назва навчальної дисципліни)

освітньо-професійна програма *Кібербезпека та захист інформації*
(назва освітньо-професійної програми)

галузь знань *12 Інформаційні технології*
(шифр і назва напряму підготовки)

спеціальність *125 Кібербезпека та захист інформації*
(шифр і назва спеціальності)

відділення *Інформаційних технологій*
(назва відділення)

Рівне – 2025 рік

Програму навчальної дисципліни *Прикладна криптографія* розроблено на основі освітньо-професійної програми «Кібербезпека та захист інформації», спеціальності 125 Кібербезпека та захист інформації, галузі знань 12 Інформаційні технології, затвердженої Вченою радою НУБіП України протокол від 26.04.2023 р. № 10.

Розробники: Черняк Тетяна Григорівна, викладач програмування та інформаційних дисциплін, спеціаліст вищої категорії, викладач методист.

Програма навчальної дисципліни затверджена на засіданні циклової комісії *програмування та інформаційних дисциплін*

Протокол від *29 серпня* 2025 року № *1*

Голова циклової комісії *програмування та інформаційних дисциплін*

29 серпня 2025 року _____ *Павло СТРИК*
(підпис) (ім'я та прізвище)

Погоджено методичною радою ВСП «РФК НУБіП України»

Протокол від *29 серпня* 2025 року № *1*

29 серпня 2025 року Голова _____ *Людмила БАЛДИЧ*
(підпис) (ім'я та прізвище)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань, напрям підготовки, спеціальність, освітньо-професійний ступінь	
Освітньо-професійний ступінь	Фаховий молодший бакалавр
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кіберпезпека та захист інформації
Характеристика навчальної дисципліни	
Вид	Обов’язкова
Загальна кількість годин	120
Кількість кредитів ECTS	4
Кількість змістових модулів	4
Мова викладання, навчання та оцінювання	українська
Курсовий проект (робота)	
Форма контролю	екзамен
Показники навчальної дисципліни для денної форм навчання	
Форма навчання	денна
Рік підготовки	2025-2026
Семестр	6
Аудиторні години:	80 год.
Лекційні	30 год.
Практичні	50 год.
Семінарські	
Самостійна робота	10 год.
Підготовка до екзамену	30 год.
Кількість тижневих годин для денної форми навчання	1,5

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни – формування у студентів теоретичних знань та практичних навичок щодо основних методів та алгоритмів сучасної криптографії, а також їхнього застосування для забезпечення інформаційної безпеки.

Завдання навчальної дисципліни:

- вивчення основних принципів криптографічного захисту інформації;
- засвоєння методів симетричного та асиметричного шифрування;
- ознайомлення з криптографічними хеш-функціями та їх застосуванням;
- розгляд принципів електронного цифрового підпису та його ролі в інформаційній безпеці;
- вивчення основ теорії чисел та комбінаторики, що застосовуються у криптографії;
- набуття практичних навичок роботи з сучасними криптографічними протоколами та інструментами;
- аналіз стійкості криптографічних алгоритмів та методів їх криптоаналізу;
- розгляд нормативно-правових аспектів криптографічного захисту інформації.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні методи та алгоритми криптографічного захисту інформації;
- принципи функціонування симетричних та асиметричних шифрів;
- особливості криптографічних хеш-функцій;
- механізми роботи електронного цифрового підпису;
- принципи генерації та розподілу криптографічних ключів;
- основи криптоаналізу та методи атаки на криптографічні алгоритми;
- нормативно-правові засади використання криптографічного захисту інформації.

вміти:

- застосовувати алгоритми симетричного та асиметричного шифрування для захисту даних;
- використовувати криптографічні хеш-функції для забезпечення цілісності інформації;
- створювати та перевіряти електронні цифрові підписи;
- реалізовувати механізми керування ключами;
- аналізувати стійкість криптографічних алгоритмів;
- використовувати сучасні криптографічні бібліотеки та програмні засоби.

Очікувані результати навчання

Загальні компетентності:

ЗК03. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК04. Здатність спілкуватися іноземною мовою.

ЗК05. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК06. Здатність до пошуку, оброблення та аналізу інформації з різних

джерел.

Фахові компетентності:

СК01. Здатність алгоритмічно та логічно мислити.

СК04. Здатність дотримуватися стандартів при розробці програмного забезпечення.

СК07. Здатність розробляти модулі та компоненти програмного забезпечення з використанням криптографічних алгоритмів.

СК10. Здатність застосовувати криптографічні методи захисту інформації.

Програмні результати навчання:

РН02. Систематизувати та узагальнювати інформацію про підходи, методи та засоби криптографічного захисту інформації.

РН04. Використовувати знання математичних методів на рівні, необхідному для розв’язання типових задач криптографії.

РН08. Аналізувати вимоги до інформаційної безпеки та криптографічного захисту даних.

РН09. Розуміти основні принципи командної роботи при впровадженні криптографічних рішень.

РН10. Обирати та застосовувати ефективні методи оптимізації криптографічних алгоритмів.

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1. ОСНОВИ КРИПТОГРАФІЇ

Тема 1.1. Вступ до криптографії

Історія криптографії. Основні поняття та термінологія. Принципи сучасної криптографії. Налаштування середовища розробки. Встановлення та конфігурація криптографічних бібліотек. Базові операції з OpenSSL

Тема 1.2. Математичні основи криптографії

Теорія чисел. Модулярна арифметика. Алгебраїчні структури.
Реалізація базових математичних операцій. Робота з великими числами. Практичні завдання з модулярної арифметики.

Тема 1.3. Класичні шифри

Шифр заміни. Шифр перестановки. Аналіз класичних шифрів.
Реалізація шифру Цезаря та Віженера. Частотний аналіз. Криптоаналіз простих шифрів.

Модуль 2: СИМЕТРИЧНА КРИПТОГРАФІЯ

Тема 2.1. Блокові шифри

DES та його модифікації. AES (Rijndael). Режими роботи блокових шифрів.
Реалізація AES в різних режимах. Порівняльний аналіз режимів роботи. Оптимізація продуктивності.

Тема 2.2. Потокові шифри

RC4. ChaCha20. Принципи роботи потокових шифрів.
Реалізація простого потокового шифру. Робота з ChaCha20. Аналіз та порівняння з блоковими шифрами.

Тема 2.3. Хеш-функції та MAC

MD5, SHA-1, SHA-2, SHA-3. HMAC. Застосування хеш-функцій.
Реалізація хешування паролів. Створення та перевірка MAC. Аналіз колізій

Змістовий модуль 3. АСИМЕТРИЧНА КРИПТОГРАФІЯ

Тема 3.1. Основи асиметричної криптографії

Принципи роботи. Порівняння з симетричною криптографією. Математичні основи. Генерація ключових пар. Базові операції з відкритими та закритими ключами. Аналіз продуктивності.

Тема 3.2. Алгоритми з відкритим ключем

RSA. Схема Діффі-Геллмана. Криптографія на еліптичних кривих (ECC).
Реалізація RSA. Протокол обміну ключами Діффі-Геллмана. Робота з ECC.

Тема 3.3. Цифрові підписи

DSA. ECDSA. Застосування цифрових підписів.

Створення та перевірка цифрових підписів. Реалізація ECDSA. Інтеграція підписів у документи.

Змістовий модуль 4. КРИПТОГРАФІЧНІ ПРОТОКОЛИ ТА ПРИКЛАДНІ АСПЕКТИ.

Тема 4.1. Управління ключами

Генерація ключів. Розподіл ключів. Зберігання ключів.

Реалізація системи управління ключами. Безпечне зберігання ключів. Розробка протоколів обміну ключами.

Тема 4.2. Криптографічні протоколи

SSL/TLS. IPSec. SSH.

Налаштування SSL/TLS. Реалізація захищеного з'єднання. Аналіз мережевого трафіку.

Тема 4.3. Квантова та постквантова криптографія

Основи квантової криптографії. Постквантові алгоритми. Майбутнє криптографії.

Дослідження постквантових алгоритмів. Оцінка стійкості існуючих систем. Планування міграції на постквантові алгоритми.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин денна форма			
	всього	лекційні	практичні	Самостійне вивчення
1	**2**	**3**	**4**	**5**
Змістовий модуль 1. ОСНОВИ КРИПТОГРАФІЇ				
Тема 1.1 Вступ до криптографії	6	2	4	-
Тема 1.2 Математичні основи криптографії	10	4	4	2
Тема 1.3 Класичні шифри	8	2	4	2
Разом за змістовим модулем 1	**24**	**8**	**12**	**4**
Змістовий модуль 2. СИМЕТРИЧНА КРИПТОГРАФІЯ				
Тема 2.1. Блокові шифри	10	4	6	-
Тема 2.2. Потокові шифри	6	2	4	-
Тема 2.3. Хеш-функції та MAC	6	2	2	2
Разом за змістовим модулем 2	**22**	**8**	**12**	**2**
Змістовий модуль 3. АСИМЕТРИЧНА КРИПТОГРАФІЯ.				
Тема 3.1. Основи асиметричної криптографії	6	2	4	-
Тема 3.2. Алгоритми з відкритим ключем	8	4	4	-
Тема 3.3. Цифрові підписи	8	2	4	2
Разом за змістовим модулем 3	**22**	**8**	**12**	**2**
Змістовий модуль 4. КРИПТОГРАФІЧНІ ПРОТОКОЛИ ТА ПРИКЛАДНІ АСПЕКТИ				
Тема 4.1. Управління ключами	8	2	6	-
Тема 4.2. Криптографічні протоколи	6	2	4	-
Тема 4.3. Квантова та постквантова криптографія	8	2	4	2
Разом за змістовим модулем 4	**22**	**6**	**14**	**2**
Усього годин	**90**	**30**	**50**	**10**
Підготовка до екзамену:	**30**			
Усього годин	**120**			

5. ТЕМИ ЛЕКЦІЙНИХ, ЛАБОРАТОРНИХ ЗАНЯТЬ ТА ЗМІСТ САМОСТІЙНОГО ВИВЧЕННЯ

№ теми	№ заняття	Вид навчальної діяльності	Назва теми	Кількість годин
I семестр				
Змістовий модуль 1. ОСНОВИ КРИПТОГРАФІЇ				**24**
1	**Тема 1.1. Вступ до криптографії**			**6**
	1	лекція 1	Історія криптографії. Основні поняття та термінологія. Принципи сучасної криптографії.	2
	2	практична робота 1	Налаштування середовища розробки. Встановлення та конфігурація криптографічних бібліотек.	2
	3	практична робота 2	Базові операції з OpenSSL	2
2	**Тема 1.2. Математичні основи криптографії**			**10**
	4	лекція 2	Теорія чисел. Модулярна арифметика.	2
	5	лекція 3	Алгебраїчні структури.	2
		самостійне вивчення	Вирішення задач на mod-арифметику.	2
	6	практична робота 3	Реалізація базових математичних операцій.	2
	7	практична робота 4	Робота з великими числами. Практичні завдання з модулярної арифметики.	2
3	**Тема 1.3. Класичні шифри**			**8**
	8	лекція 4	Шифр заміни. Шифр перестановки. Аналіз класичних шифрів.	2
		самостійне вивчення	Самостійний аналіз тексту за допомогою частотного аналізу.	2
	9	практична робота 5	Реалізація шифру Цезаря та Віженера.	2
	10	практична робота 6	Частотний аналіз. Криптоаналіз простих шифрів.	2
Змістовий модуль 2. СИМЕТРИЧНА КРИПТОГРАФІЯ				**22**
4	**Тема 2.1. Блокові шифри**			**10**
	11	лекція 5	DES та його модифікації.	2
	12	лекція 6	AES (Rijndael). Режими роботи блокових шифрів.	2
		самостійне вивчення	Провести тестування продуктивності різних режимів (ECB, CBC)	-
	13,14	практична робота 7,8	Реалізація AES в різних режимах. Порівняльний аналіз режимів роботи.	4
	15	практична робота 9	Оптимізація продуктивності.	2
5	**Тема 2.2. Потокові шифри**			**6**
	16	лекція 7	RC4. ChaCha20. Принципи роботи потокових шифрів.	2
		самостійне вивчення	Виконай порівняння між блоковими та потоковими шифрами (швидкодія, стійкість).	-

	17	практична робота 10	Реалізація простого потокового шифру.	2
	18	практична робота 11	Робота з ChaCha20. Аналіз та порівняння з блоковими шифрами	2
6	**Тема 2.3. Хеш-функції та MAC**			**6**
	19	лекція 8	MD5, SHA-1, SHA-2, SHA-3. HMAC. Застосування хеш-функцій.	2
		самостійне вивчення	Реалізуй хешування паролів у Python, використовуючи бібліотеку hashlib.	2
	20	практична робота 12	Реалізація хешування паролів. Створення та перевірка MAC. Аналіз колізій	2
Змістовий модуль 3. АСИМЕТРИЧНА КРИПТОГРАФІЯ.				**22**
7	**Тема 3.1. Основи асиметричної криптографії**			**6**
	21	лекція 9	Принципи роботи. Порівняння з симетричною криптографією. Математичні основи симетричної криптографії.	2
		самостійне вивчення	Використати OpenSSL для створення ключів і проведення шифрування/розшифрування.	-
	22	практична робота 13	Генерація ключових пар.	2
	23	практична робота 14	Базові операції з відкритими та закритими ключами. Аналіз продуктивності.	2
8	**Тема 3.2. Алгоритми з відкритим ключем**			**8**
	24	лекція 10	RSA. Схема Діффі-Геллмана.	2
	25	лекція 11	Криптографія на еліптичних кривих (ECC).	2
		самостійне вивчення	Досліди приклади застосування ECC в реальних проєктах (напр., у криптовалютах).	-
	26	практична робота 15	Реалізація RSA. Протокол обміну ключами Діффі-Геллмана.	2
	27	практична робота 16	Робота з ECC.	2
9	**Тема 3.3. Цифрові підписи**			**8**
	28	лекція 12	DSA. ECDSA. Застосування цифрових підписів.	2
		самостійне вивчення	Досліди, як працює підписання транзакцій у блокчейні.	2
	29	практична робота 17	Створення та перевірка цифрових підписів.	2
	30	практична робота 18	Реалізація ECDSA. Інтеграція підписів у документи.	2
Змістовий модуль 4. КРИПТОГРАФІЧНІ ПРОТОКОЛИ ТА ПРИКЛАДНІ АСПЕКТИ				**22**
10	**Тема 4.1. Управління ключами**			**8**
	31	лекція 13	Генерація ключів. Розподіл ключів. Зберігання ключів.	2
		самостійне вивчення	Ознайомися з практиками безпечного зберігання ключів (напр., у апаратних безпечних модулях).	-
	32	практична робота 19	Реалізація системи управління ключами.	2
	33	практична робота 20	Безпечне зберігання ключів.	2
	34	практична робота 21	Розробка протоколів обміну ключами.	2
11	**Тема 4.2. Криптографічні протоколи**			**6**

	35	лекція 14	SSL/TLS. IPSec. SSH.	2
		самостійне вивчення	Провести аналіз мережевого трафіку за допомогою Wireshark.	-
	36	практична робота 22	Налаштування SSL/TLS. Реалізація захищеного з'єднання.	2
	37	практична робота 23	Аналіз мережевого трафіку.	2
12	**Тема 4.3. Квантова та постквантова криптографія**			**8**
	38	лекція 15	Основи квантової криптографії. Постквантові алгоритми. Майбутнє криптографії.	2
		самостійне вивчення	Знайти та проаналізувати кейси міграції на постквантові алгоритми.	2
	39	практична робота 24	Дослідження постквантових алгоритмів. Оцінка стійкості існуючих систем.	2
	40	практична робота 25	Планування міграції на постквантові алгоритми.	2
			Разом	**90**
			Підготовка до екзамену	**30**
			Всього	**120**

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуально-консультативна робота виконується за графіком у таких формах: індивідуальні заняття, консультації, перевірка виконання індивідуальних завдань і захист результатів їх виконання тощо.

Формами організації індивідуально-консультативної роботи є:

а) консультації з теоретичного матеріалу:

- інтерактивне спілкування (питання-відповідь);
- групові (розгляд типових завдань);
- диспути (обговорення вирішення типових питань);

б) індивідуальні та групові консультації з освоєння практичного матеріалу;

в) індивідуальна здача та захист виконаних робіт для комплексної оцінки ступеня оволодіння програмним матеріалом.

№	*Тема дисципліни*	*Вид завдання (реферати, дослідницькі, розрахункові роботи тощо)*	*Календарні строки і форма контролю*
1	Історія розвитку криптографії: від давніх шифрів до сучасних алгоритмів	реферат	лютий
2	Теорія чисел у криптографії: основні математичні принципи	реферат	лютий
3	Класичні шифри: шифр Цезаря, Віженера, Плейфера	реферат	лютий
4	Аналіз частотності та методи криптоаналізу класичних шифрів	реферат	лютий
5	Поняття секретності та стійкості криптографічних алгоритмів	реферат	лютий
6	Еволюція криптографії у військових конфліктах	реферат	лютий
7	Криптографія в культурі та кіно: міфи та реальність	реферат	лютий
8	Використання криптографії в історичних документах	реферат	лютий
9	Блокові шифри: принципи роботи та застосування	реферат	березень
10	Аналіз стійкості алгоритму AES	реферат	березень
11	Потокові шифри: RC4, ChaCha20, їх переваги та недоліки	реферат	березень
12	Режими роботи блокових шифрів: ECB, CBC, CFB, OFB, CTR	реферат	березень
13	Хеш-функції: MD5, SHA-1, SHA-2, SHA-3	реферат	березень
14	Колізії в хеш-функціях: теоретичні та практичні аспекти	реферат	березень
15	Використання хешування для збереження паролів	реферат	березень
16	MAC-коди та їх застосування для автентифікації повідомлень	реферат	березень
17	Шифрування файлів та баз даних: підходи та алгоритми	реферат	березень
18	Генерація криптографічно стійких випадкових чисел	реферат	березень
19	Алгоритм RSA: принцип роботи та застосування	реферат	квітень
20	Проблеми факторизації та безпека RSA	реферат	квітень
21	Діффі-Геллманівський обмін ключами: принципи та загрози	реферат	квітень
22	Криптографія на еліптичних кривих (ECC): переваги та обмеження	реферат	квітень

23	Цифровий підпис: DSA, ECDSA та їх використання	реферат	квітень
24	Криптографія у блокчейн-технологіях: Bitcoin та Ethereum	реферат	квітень
25	Використання криптографії в електронному голосуванні	реферат	квітень
26	Роль криптографії в захисті месенджерів (Signal, WhatsApp, Telegram)	реферат	квітень
27	Протоколи безпечного з'єднання: SSL/TLS та їх вразливості	реферат	квітень
28	Методи атаки на асиметричні алгоритми (відкритий текст, атака на підпис)	реферат	квітень
29	Управління криптографічними ключами: принципи та методи	реферат	травень
30	Атаки на криптографічні протоколи: MITM, Replay Attack	реферат	травень
31	Квантова криптографія: принципи роботи та перспективи	реферат	травень
32	Постквантова криптографія: алгоритми та виклики	реферат	травень
33	Біометричні методи автентифікації та їх криптографічні аспекти	реферат	травень
34	Законодавство у сфері криптографії: правові обмеження та регулювання	реферат	травень

7. ПЕРЕЛІК ПИТАНЬ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Модуль 1: Основи криптографії

1. Що таке криптографія і які її основні завдання?
2. Які основні типи криптографічних алгоритмів існують?
3. У чому різниця між симетричним і асиметричним шифруванням?
4. Які етапи розвитку криптографії можна виділити в історії?
5. Що таке модулярна арифметика і як вона використовується у криптографії?
6. Які властивості простих чисел роблять їх важливими для криптографії?
7. Як працює шифр Цезаря?
8. У чому полягає принцип шифру Віженера?
9. Як працює метод частотного аналізу?
10. Що таке криптоаналіз і які його основні методи?

Модуль 2: Симетрична криптографія

11. Які основні принципи роботи блокових шифрів?
12. Які особливості має алгоритм DES?
13. Чому DES був замінений на AES?
14. Як працює алгоритм AES?
15. Які режими роботи блокових шифрів існують і як вони впливають на безпеку?
16. Що таке потокові шифри і як вони відрізняються від блокових?
17. Як працює алгоритм RC4 і які його вразливості?
18. Які переваги має алгоритм ChaCha20?
19. Що таке хеш-функція і які її основні властивості?
20. Чим відрізняються MD5, SHA-1, SHA-2 та SHA-3?
21. Що таке HMAC і для чого він використовується?
22. Як можна забезпечити цілісність повідомлення за допомогою хеш-функцій?
23. Як зберігаються паролі за допомогою хешування?
24. Що таке атака на колізії у хеш-функціях?
25. Які алгоритми використовуються для генерації криптографічно стійких випадкових чисел?

Модуль 3: Асиметрична криптографія

26. Як працює алгоритм RSA?
27. Чому проблема факторизації цілих чисел є основою безпеки RSA?
28. Що таке відкритий та закритий ключ у RSA?
29. У чому суть обміну ключами за алгоритмом Діффі-Геллмана?
30. Які переваги має криптографія на еліптичних кривих (ECC)?
31. Як працює цифровий підпис і для чого він використовується?
32. Які алгоритми цифрового підпису існують?
33. Що таке ECDSA і як він працює?
34. Як здійснюється перевірка цифрового підпису?
35. Чим відрізняється автентифікація від конфіденційності у криптографічних системах?

Модуль 4: Криптографічні протоколи та прикладні аспекти

36. Як працює SSL/TLS і для чого він використовується?
37. Що таке сертифікат SSL і як він пов’язаний із центрами сертифікації?
38. Які основні рівні захисту інформації у протоколі IPSec?
39. Як працює протокол SSH і які його переваги?
40. Що таке управління ключами і чому воно важливе у криптографії?
41. Які методи розподілу ключів існують?
42. Як забезпечується безпечне зберігання криптографічних ключів?
43. Які основні загрози для криптографічних протоколів?
44. Що таке атака «людина посередині» (MITM) і як від неї захищаються?
45. Як працює двофакторна автентифікація і які методи вона використовує?
46. Що таке квантова криптографія і які проблеми вона вирішує?
47. Які існують постквантові криптографічні алгоритми?
48. Як блокчейн використовує криптографію для забезпечення безпеки?
49. Які законодавчі обмеження існують щодо використання криптографії в різних країнах?
50. Як можна оцінити продуктивність криптографічного алгоритму?

8. МЕТОДИ НАВЧАННЯ

Під час вивчення дисципліни «Прикладна криптографія» у навчальному процесі застосовуються такі методи навчання: розповідь, бесіда, проблемні лекції, пояснення, демонстрація, ілюстрація, навчальна дискусія, диспут, мозкові атаки, робота в малих групах, кейс-метод, самостійне виконання лабораторних завдань, розв'язування задач, виконання вправ.

9. КОНТРОЛЬ РЕЗУЛЬТАТІВ НАВЧАННЯ

9.1. Форми та засоби поточного і підсумкового контролю

Контроль знань здобувачів освіти здійснюється за модульно-рейтинговою системою.

Засобами діагностики та методами демонстрування результатів навчання здобувачів освіти з дисципліни є:

- індивідуальне опитування, фронтальне опитування;
- поточне тестування;
- підсумкове тестування з кожного змістовного модуля;
- директорська контрольна робота;
- залік;
- екзамен.

Зміст курсу дисципліни «Прикладна криптографія» поділений на 3 змістових модулів. Кожний модуль включає в себе лекції, лабораторні заняття та самостійну роботу здобувачів освіти і завершуються рейтинговим контролем рівня засвоєння знань програмного матеріалу відповідної частини курсу.

Після завершення відповідного змістового модуля проводяться ***модульні контрольні роботи*** **(МК).** До модульної контрольної роботи допускаються здобувачі освіти, які опрацювали весь обсяг теоретичного матеріалу в т.ч. і матеріал самостійно, виконали лабораторні роботи.

Рейтингову кількість балів здобувачів освіти формують бали, отримані за модульні контрольні роботи, які проводяться у формі тестування, та середній рейтинг виконання лабораторних робіт.

Участь здобувачів освіти в контрольних заходах обов'язкова. МК проводиться у письмовій тестовій формі, тестові завдання обов'язково включають матеріал, який передбачено до самостійного опрацювання здобувачами освіти. Студент, який не виконав вимоги щодо самостійної роботи чи будь якого іншого виду навчальної діяльності, не допускається до складання МК і даний модуль йому не зараховується.

Семестрові бали (семестровий рейтинг) студент отримує як середнє арифметичне балів змістових модулів з усіх тем п'яти змістових модулів.

9.2. Критерії оцінювання результатів навчання

Оцінка «відмінно» виставляється студенту, який має стійкі системні, глибокі і різнобічні знання, відмінно володіє матеріалом, знає нормативну і законодавчу базу та її застосування за певних умов, дає обґрунтовані, правильні відповіді на питання, доцільно використовує термінологію дисципліни (предмета), усвідомлює взаємозв’язок окремих розділів дисципліни, їхнє значення для майбутньої професії, виявляє творчі здібності у розумінні та використанні навчально-програмного матеріалу, проявляє здатність до самостійного оновлення і поповнення знань. Практичні завдання і задачі вирішує правильно, розрахунки проводить без помилок, отримує достовірні результати, правильно заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- глибоке, теоретично обґрунтоване розкриття питання; розрахунки, зроблені без помилок, проведено повний аналіз, відображена власна позиція – оцінюються в **48-50 балів**;
- обґрунтоване розкриття питання чи/та розрахунки, зроблені з незначними неточностями, які істотно не впливають на правильність відповіді – **45-47 балів**;

Оцінка «добре» виставляється студенту, який знає викладений матеріал і добре ним володіє але допускає незначні помилки у формулюванні термінів, категорій, понять, використанні нормативно-правової бази, показує стійкий рівень знань з дисципліни і та професійної діяльності. Під час виконання практичних завдань, вирішення задач, проведення розрахунків допускає незначні помилки, але за допомогою викладача швидко орієнтується і знаходить правильні відповіді, правильно або з незначними помилками заповнює і складає документи, робить відповідні узагальнення і висновки та охайно оформляє виконані завдання та звіти.

- відповідь не дає повного розкриття питання, не проведено повний аналіз результатів розрахунків, немає власної позиції – **42-44 балів**;
- неповне розкриття питання, доведені до завершення розрахунки але не зроблено їх аналіз; загалом наявні достатні знання – **38-41 балів**;

Оцінка «задовільно» виставляється студенту, який посередньо володіє матеріалом, виявив знання основного навчально-програмного матеріалу в обсязі, необхідному для подальшого навчання та наступної роботи за професією, справляється з виконанням завдань, передбачених програмою, дає неправильну

відповідь на окремі питання або на всі питання дає малообґрунтовані, невичерпні відповіді, знання має обмежені, несистемні, слабо орієнтується у нормативно-правових документах. Під час виконання практичних завдань, вирішення задач, проведення розрахунків припускається грубих помилок і тільки за допомогою викладача може виправити допущені помилки, із значними помилками заповнює і складає документи, поверхово робить узагальнення і висновки та не зовсім охайно оформляє виконані завдання та звіти.

- питання розкрите фрагментарно, наявні фактологічні помилки під час викладу чи/та помилки під час проведення розрахунків – **34-37 балів**;

- відповідь неповна, наявні суттєві помилки при викладі та проведенні розрахунків – **30-33 балів**;

Оцінка «незадовільно» виставляється студенту, який не виявив достатніх знань основного навчально-програмного матеріалу, дає відповіді лише на деякі питання або дає неправильні відповіді на питання, може відтворити кілька термінів, не знає термінології дисципліни і основних нормативно-правових документів, не може без допомоги викладача використати знання у подальшому навчанні, не спромігся оволодіти навичками самостійної роботи. Допускає принципові помилки у виконанні передбачених програмою завдань, вирішенні задач, проведенні розрахунків припускається грубих помилок і не може їх виправити, не виконує практичне завдання у визначений термін, із значними помилками заповнює і складає документи, не робить узагальнення і висновки та не охайно оформляє виконані завдання та звіти.

- відповідь має значні помилки елементарного рівня – **1-30 бали**;
- відсутність відповіді на питання – **0 балів**.

9.3. Оцінювання за формами контролю

	Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4	Заліковий модуль 5	**Разом**
%	20	20	20	20	20	100
Мінімум	0	0	0	0	0	0
Максимум	50	50	50	50	50	50

9.4. Шкала оцінювання

Відсоток опрацьованого матеріалу	**Рейтинг за 50-бальною шкалою**	**Оцінка за п'ятибальною шкалою**	**Запис у заліковій книжці студента та відомості**	**Оцінка за 12-бальною шкалою**
97-100	49, 50	5	відмінно	12
93-96	47, 48	5	відмінно	11
90-92	45, 46	5	відмінно	10
85-89	43,44	4	добре	9
80-84	40, 41, 42	4	добре	8
75-79	38, 39	4	добре	7
69-74	35, 36, 37	3	задовільно	6
65-68	33, 34	3	задовільно	5
60-64	30, 31, 32	3	задовільно	4
менше 60	0-29	2	незадовільно	2

10. МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. Витяг з навчального плану
2. Навчальна (типова) програма
3. Плани занять
4. Конспект лекцій з дисципліни
5. Завдання для обов'язкової контрольної роботи
6. Інструкційно-методичні матеріали до практичних занять
7. Інструкційно-методичні матеріали до самостійної роботи
8. Питання до заліків з модулів
9. Контрольні тестові завдання до заліків з модулів
10. Навчальний посібник
11. Роздавальний матеріал
12. Презентації до тем

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Брюс Шнайєр. *Прикладна криптографія: Протоколи, алгоритми та вихідний код на C* (2-ге видання, 1996).
2. Вільям Столлінгс. *Криптографія та безпека мереж: принципи та практика* (7-ме видання, 2016).
3. Джонатан Кац, Єгуда Лінделл. *Вступ до сучасної криптографії* (3-тє видання, 2020).
4. Дуглас Р. Стінсон, Маура Б. Патерсон. *Криптографія: теорія і практика* (4-те видання, 2018).
5. Крістоф Паар, Ян Пельцль. *Розуміння криптографії: підручник для студентів та практиків* (2010).

Допоміжна

6. Нілс Фергюсон, Брюс Шнайєр, Тадайоші Коно. *Інженерія криптографії: принципи розробки та практичне застосування* (2010).
7. Джоан Демен, Вінсент Раймен. *Проєктування Rijndael: AES – стандарт розширеного шифрування* (2002).
8. Девід МакКей. *Теорія інформації, висновки та алгоритми навчання* (2003).
9. Альфред Дж. Менезес, Пол К. ван Оршот, Скотт А. Ванстон. *Довідник з прикладної криптографії* (1996).
10. Найджел Смарт. *Криптографія простою мовою* (2016).

Додаткова

11. Чарлі Кауфман, Радія Перлман, Майк Спесінер. *Безпека мереж: приватне спілкування у публічному світі* (3-тє видання, 2010).
12. Пол К. Кочер, Ден Боне, Метью Грін. *Курс прикладної криптографії* (2021).
13. Йенс-Петер Капс, Берк Сунар, Вільям Дієль. *Інженерія криптографії* (2009).
14. Марк А. Нільсен, Ісаак Л. Чуанг. *Квантові обчислення та квантова інформація* (10-річне видання, 2011).
15. Даніель Дж. Бернштейн, Таня Ланге. *Постквантова криптографія* (2008).

11. ІНФОРМАЦІЙНІ РЕСУРСИ

16. edX – курси з інформаційної безпеки та криптографії – **https://www.edx.org**
17. Crypto101 – безкоштовний курс криптографії – **https://crypto101.io**
18. Cryptopals – набір завдань для практичного вивчення криптографії – **https://cryptopals.com**
19. Open Security Training – безкоштовні навчальні матеріали з криптографії – **https://opensecuritytraining.info**