КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційних систем та технологій

«ЗАТВЕРДЖУЮ»
Заступник декана з навчально-виховної роботи
_____Наталія ТМЄНОВА
«___»_____2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОСНОВИ КРИПТОГРАФІЇ ТА КРИПТОЛОГІЧНОГО АНАЛІЗУ В СИСТЕМАХ ІОТ
для здобувачів

галузь знань	**12 Інформаційні технології**
спеціальність	**126 Інформаційні системи та технології**
освітній рівень	**магістр**
освітня програма	**«Програмні технології інтернет речей»**
вид дисципліни	**вибіркова**
Форма навчання	**денна**

Навчальний рік	**2025/2026**
Семестр	**3**
Кількість кредитів ECTS	**5**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: **Ірина БОРИСЕНКО,** кандидат технічних наук;
Ганна ТЕРЕЩУК

Пролонговано: на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

КИЇВ – 2025

Розробники: **Ірина БОРИСЕНКО**, *к.т.н., доцент кафедри інформаційних систем та технологій,*

Ганна ТЕРЕЩУК, *асистент кафедри інформаційних систем та технологій;*

ЗАТВЕРДЖЕНО
Зав. кафедри
інформаційних систем та технологій
_____Володимир ДРУЖИНІН
(підпис) (прізвище та ініціали)

Протокол № 17_24/25 від 25 червня 2025 р

Схвалено науково - методичною комісією факультету інформаційних технологій
Протокол № 10 від 27 червня 2025 року

Голова науково-методичної комісії ФІТ_____ Ганна КРАСОВСЬКА

Програму перевірено

«_____» _____ 2025 року

ВСТУП

1. Мета дисципліни – є ознайомлення та вивчення студентами:

– основних методів захисту інформації шляхом її перетворення (кодування) у цифровому форматі. застосування сучасних технологій та методів захисту;

– використання криптографічних методів для захисту даних в IoT.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

– Знати: основні поняття і методи дискретної математики, теорії чисел, математичного аналізу, алгоритмики, структур даних, програмування.

3. Вміти: по опису перетворень створювати алгоритми і програми, що їх реалізують.

Анотація навчальної дисципліни: Дисципліна «Основи криптографії та криптологічного аналізу в системах IoT» спрямована на вивчення основних задач передачі та захисту інформації від несанкціонованого доступу. Вона забезпечує оволодіння сучасними методами криптографічних перетворень інформації. Криптографія включає криптографію з відкритими ключами: основні протоколи, цифровий підпис, геш-функції, блокчейн технологію, доведення з нульовим розкриттям, методи автентифікації.

4. Завдання (навчальні цілі): полягають у тому, щоб надати студентам всебічне розуміння принципів та методів забезпечення інформаційної безпеки в середовищі IoT. Перш за все, набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень у розв’язанні задач кодування інформації, відповідно науково-освітньої кваліфікації «Магістр». Зокрема, розвивати: здатність застосовувати теоретичні та практичні основи криптографічного захисту інформації. Це дозволить студентам зрозуміти, як функціонують пристрої IoT і як вони взаємодіють в мережі та яким чином застосовувати криптографічний захист.

Переваги безпеки, що надаються криптографією — конфіденційність, автентифікація, цілісність та незаперечність — забезпечують прямі, індивідуальні заходи щодо зменшення багатьох ризиків безпеки хостів, даних та комунікацій. Вирішення питань безпеки, необхідної для фахівця з інформаційних систем та техтологій - необхідна умова для безпечної та надійної інтеграції IoT в усі сфери та галузі суспільства. Принципи прикладної криптографії засосовують криптографічні рішення високого рівня під час розробки вбудованих пристроїв безпеки та архітектур безпеки на рівні системи.

5. Результати навчання за дисципліною:

Результат навчання (1. Знати; 2. Вміти; 3. Комунікація; 4.Автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання	Відсоток у підсумковій оцінці з дисципліни
Код	**Результат навчання**			
1.1	Знати основні принципи криптографії з відкритими ключами.	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**10**
1.2	Знати основні схеми криптографічних перетворень на основі односторонніх функцій..	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**10**
1.3	Знати основні протоколи розповсюдження ключів	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**10**
1.4	Знати основні схеми цифрового підпису.	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**10**
2.1	Вміти створювати алгоритми та програми, що реалізують криптографічні перетворення в IoT	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**10**
2.2	Вміти створювати системи захисту інформації, що передається по відкритим каналам зв’язку в IoT - системах.	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**10**
2.3	Вміти програмувати цифрові підписи.	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**5**
3.1	Оцінювати власні пропозиції по створенню систем криптозахисту, обговорювати з	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**5**

	колегами проекти систем..			
4.1	Демонструвати академічне та професійне володіння предметом , вміння створювати та обґрунтовувати нові системи захисту інформації.	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**5**
4.2	Демонструвати вміння працювати в групових виконаннях прективю	Лекції. Лабораторні Індивідуальна робота	Бліцопитування, модульні контрольні роботи, залік	**5**

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни / Програмні результати навчання	1.1	1.2	1.3	1.4	2.1	2.2	2.3	3.1	4.1	4.2
ПРН 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп'ютерних систем та середовищ з метою їх запровадження у професійній діяльності.	+	+	+	+	+	+	+	+	+	+
ПРН 15. Демонструвати знання основних методів та технологій об'єктно-орієнтованого програмування, а також основ інших парадигм програмування, основ конструювання програмного забезпечення, раціональні алгоритми вирішення задач оптимізації та оптимального керування, уміння ставити конкретну прикладну задачу, знаходити оптимальні рішення за допомогою методів прийняття рішень.	+	+	+	+	+	+	+	+	+	+
ПРН 19. Використовувати можливості апаратного забезпечення, використовувати можливості операційних систем, використовувати можливості мережевих програмних систем, забезпечувати захищеність програм і даних від несанкціонованих дій.	+	+	+	+	+	+	+	+		

7. Схема формування оцінки

а. Форми оцінювання

рівень досягнення усіх запланованих результатів навчання визначається за

результатами вивчення відеолекцій розміщених в Teams, проміжного тестування за двома модулями, захисту результатів лабораторних робіт, опитування та реферативної доповіді в рамках дисципліни. Дисципліна закінчується заліком. Питома вага результатів навчання у підсумковій оцінці за умови її опанування на належному рівні така:

• результати навчання 1-(знання) РН 1.1., РН 1.2., РН 1.3., РН 1.4., РН 1.5. - до 30% ;
• результати навчання 2-(вміння) РН 2.1., РН 2.2., РН 2.3.- до 40% ;
• результати навчання 3-(комунікація) РН 3 - до 10%,
• результати навчання 4-(комунікація) РН 3 - до 20%,

.
.

b. Організація оцінювання

Семестрове оцінювання: 100 балів (100%) Оцінка за семестр формується шляхом успішного виконання та обов'язкового захисту лабораторних робіт, а також реферативних виступів та відповідей при дискусіях на лекційних заняттях.

Поточне оцінювання проводиться у формі опитування студентів за темами попередніх лекцій, темами лабораторних робіт. Здобувач виконує та захищає 6 лабораторних робіт, що оцінюються від 6 до 10 балів за кожну роботу (всього від 36 до 60 балів).

Якщо здобувач не вчасно виконує лабораторну роботу, то оцінка знижується на 0,5 бали за кожен тиждень протермінування. Робота вважається зданою вчасно, коли захист відбувається на наступній парі після видачі завдання, якщо викладачем не повідомлено інші терміни. Терміни здачі викладач оголошує та викладає окремим повідомленням в команді системи Microsoft Teams (чи інших затверджених кафедрою системах навчання).

Для студентів, які набрали сумарно меншу кількість балів ніж критично-розрахунковий мінімум (36 балів), для допуску до заліку не допускаються. Обов'язковими є виконання та захист запланованих індивідуальних лабораторних, на бали від 60%. Підсумкове оцінювання у формі заліку: складає 40 модульних балів (40% від загального рейтингу). На останньому занятті проводиться залікова робота у формі тестування. Оцінка за залік не може бути меншою 24 балів для отримання позитивної оцінки за предмет.

Підсумкова оцінка визначається шляхом підсумовування балів семестрової роботи та залікового тестування. Якщо у підсумку студент набрав більше 60 балів, йому ставиться оцінка «зараховано».

	Лабораторні роботи	Залікове тестування	Підсумкова оцінка
Min. – балів	36	24	60
Max – балів	60	40	100

c. Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74

8. Структура навчальної дисципліни. Тематичний план лекцій, лабораторних та практичних занять

№ п/п	Назва теми	Кількість годин		
		лекції	Лб	С/Р
Змістовий модуль 1				
1	**Тема 1**. Основи теорії чисел та алгебри.	2	2	10
2	**Тема 2.** Квадратичні лишки.	2	2	10
3	**Тема 3.** Одностороння функція. Приклади. Індивідуальна робота: програмування пошуку простих чисел.	2	2	10
4	**Тема 4.** Метод Діффі-Хеллмана розповсюдження ключів. Груповий GDH-алгоритм.	2	2	10
5	**Тема 5.** RSA-алгоритм та його узагальнення. Цифровий підпис.	2	2	10
6	**Тема 6.** Геш-функції. MD 5 and SHA. Дерево Меркля. Блокчейн. Індивідуальна робота: Програмування дерева Меркля	2	4	10
Змістовий модуль 2				
7	**Тема 7.** Схема Голдвассер-Мікалі, що базується на квадратисчних лишках	2	4	10
8	**Тема 8.** RSA в недетермінованому варіанті (OAEP). Pailier та Benaloh схеми.	2	4	10
9	**Тема 9**. Методи автентифікації. Схема Фіата Шаміра автентифікації смарт-карти.. Схема Шнорра.	2	4	20
	Всього за семестр	**18**	**28**	**100**

Загальний обсяг ***150*** *год.,* в тому числі:
Лекцій **–** ***18*** *год.*
Лабораторні заняття – ***28*** *год.*
Консультації – ***4*** *год.*
Самостійна робота **–** ***100*** *год.*

РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна:

1.Oded Goldreich, Foundations of Cryptography, Cambridge University Press, 2004, 372pp.

2 D. Salomon, Handbook of Data Compression.-Springer-Verlag, 2010, 1370pp.

3 J.Kutz, Y.Lindel, Introduction to Modern Cryptography.-Chaptman&Hall, 2014, 603 pp. 4 A.M. Antonopoulas, Mastering Bitcoin Open Edition, 2014

4. Graham Bartlett, Amjad Inamdar. IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS. – Cisco Press, 2016 – 608 c.

5.Duane Wessels. Squid: The Definitive Guide. – O'Reilly Media, 2004 – 472 c

Додаткова:

1. Hoffstein, J. An Introduction to Mathematical Cryptography [Text] / J. Hoffstein, J. Pipher, J.H. Silverman. – Springer, 2008. – 523 p.
2. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications [Text]: NIST Special Publication 800-22 Rev1. – Gaithersburg, Maryland: NIST, 2008. – 153 p.