МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Проректор з наукової роботи

_____ Микола ДИВАК

«_____»_____2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Криптографія в децентралізованих системах»

Ступінь вищої освіти (освітньо – кваліфікаційний рівень) – **доктор філософії**

Галузь знань – **12 Інформаційні технології**

Спеціальність – **125 Кібербезпека та захист інформації**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	СРС (год.)	Разом (год.)	Екз. (сем.)
Денна	1	2	20	20	80	120	2

Тернопіль – 2024

Робоча програма складена на основі освітньо-наукової програми підготовки доктора філософії, галузь знань 12 - «Інформаційні технології», спеціальності: 125 “Кібербезпека та захист інформації” затвердженої Вченою радою ЗУНУ (протокол № 11від 26 червня 2024 р.)

Робочу програму склав д.т.н., професор, завідувач кафедри кібербезпеки Яцків Василь Васильович

Розглянуто та схвалено групою забезпечення спеціальності
протокол № 1 від 30 серпня 2024 р.

Голова ГЗС _____ Василь ЯЦКІВ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Проректор з наукової роботи

_____ Микола ДИВАК

«_____»_____2024 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Криптографія в децентралізованих системах»

Ступінь вищої освіти (освітньо – кваліфікаційний рівень) **– доктор філософії**

Галузь знань **– 12 Інформаційні технології**

Спеціальність **– 125 Кібербезпека та захист інформації**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	СРС (год.)	Разом (год.)	Екз. (сем.)
Денна	1	2	20	20	80	120	2

Тернопіль – 2024

Робоча програма складена на основі освітньо-наукової програми підготовки доктора філософії, галузь знань 12 - «Інформаційні технології», спеціальності: 125 “Кібербезпека та захист інформації” затвердженої Вченою радою ЗУНУ (протокол № 11від 26 червня 2024 р.)

Робочу програму склав д.т.н., професор, завідувач кафедри кібербезпеки Яцків Василь Васильович

Розглянуто та схвалено групою забезпечення спеціальності
протокол № 1 від 30 серпня 2024 р.

Голова ГЗС _____ Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Опис дисципліни «Криптографія в децентралізованих системах»

Дисципліна «Криптографія в децентралізованих системах»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 4	Галузь знань: 12 - Інформаційні технології	Обов'язкова
Кількість залікових модулів	Спеціальності – 125 Кібербезпека та захист інформації	Рік підготовки: *Денна – 1* Семестр: *Денна – 2*
Кількість змістових модулів – 2	Ступінь вищої освіти – доктор філософії	Лекції: *Денна – 20* Практичні заняття: *Денна – 20*
Загальна кількість годин – 120		Самостійна робота: *Денна – 80*
Тижневих годин: з них аудиторних: 4		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Криптографія в децентралізованих системах»

2.1. Мета вивчення дисципліни.

Метою дисципліни «Криптографія в децентралізованих системах» є Забезпечення майбутніх докторів філософії знаннями та навичками, необхідними для аналізу, створення та оцінки криптографічних рішень в децентралізованих системах.

2.2. Завдання вивчення дисципліни:

– ознайомлення з основами сучасних криптографічних алгоритмів та протоколів;

– дослідження криптографії у контексті децентралізованих та розподілених систем;

– оцінка загроз та методів захисту в криптографічних системах;

– застосування теоретичних знань у практичних задачах для створення систем з підвищеним рівнем безпеки.

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

СК-1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі кібербезпеки.

СК-6. Уміння відслідковувати тенденції й напрямки розвитку інформаційної та кібербезпеки, а також суміжних і прикладних областей.

2.4. Програмні результати навчання

В результаті вивчення дисципліни аспірант повинен:

ПРН-2. Знати сучасні методи проведення досліджень в галузі кібербезпеки.

ПРН-7. Вміти досліджувати проблеми кібербезпеки критичної інфраструктури.

ПРН-8. Вміти синтезувати науково обґрунтовані рішення по захисту інформації в комп’ютерних та кіберфізичних системах.

3. Зміст дисципліни «Криптографія в децентралізованих системах»

Змістовий модуль 1. **Криптографія та децентралізовані системи.**

Тема 1. **Вступ до криптографії та децентралізованих систем.**

Основні поняття криптографії (шифрування, хешування, цифровий підпис).

Принципи роботи децентралізованих систем.

Роль криптографії в забезпеченні безпеки децентралізованих систем.

Застосування криптографії у сучасному світі.

Література: 1, 2.

Тема 2. **Основні математичні задачі в криптографії.**

Задача факторизації цілих чисел.

Задача дискретного логарифма.

Задача про еліптичні криві.

Квантові виклики. Проблеми зламування традиційних алгоритмів через квантові обчислення.

Математичні властивості, що забезпечують безпеку. Принципи: односторонність функцій, випадковість і хаотичність. Приклади математичних функцій, що відповідають цим критеріям.

Оцінка швидкодії та безпеки алгоритмів.

Література: 1, 2.

Тема 3. **Криптографічні протоколи.**

Протоколи обміну ключами (Diffie-Hellman, ECDH).

Застосування у сертифікації та SSL/TLS.

Безпечний обмін повідомленнями.

Електронна пошта та цифрові підписи.

Література: 1, 2.

Тема 4. **Цілісність даних в децентралізованих системах.**

Основи хеш-функцій: визначення та властивості.

Роль хеш-функцій у цифрових підписах та автентифікації.

Алгоритми хешування: MD5, SHA-2, SHA-3.

Використання хеш-функцій у блокчейн-системах.

Дерева Меркла: структура та застосування для верифікації даних.

Виявлення колізій у хеш-функціях: методи та вплив на безпеку.

Література: 1, 2.

Тема 5. **Протоколи згоди та їх безпека у блокчейн-системах.**

Основи протоколів згоди: принципи та класифікація.

Proof of Work (PoW): механізм, переваги та недоліки.

Proof of Stake (PoS): концепція, реалізація та енергетична ефективність.

Інші протоколи згоди: Delegated PoS, Proof of Authority, та їхні сценарії використання.

Література: 1, 2.

Змістовий модуль 2. **Постквантова криптографія в децентралізованих системах**

Тема 6 **Постквантова криптографія: теорія та алгоритми.**

Основи постквантової криптографії: концепція та цілі.

Класифікація алгоритмів стійких до квантових обчислень.

Алгоритми NTRU: теорія та реалізація.

Алгоритми Kyber та Dilithium: аналіз стійкості та продуктивності.

Порівняння класичних та постквантових алгоритмів.

Вплив постквантових технологій на сучасні криптографічні системи.
Література: 2, 3.

Тема 7. **Постквантові криптосистеми на основі кодів.**
Класичні схеми: McEliece, Niederreiter.
Аналіз безпеки систем на основі кодів.
Стійкість до квантових атак.
Порівняння з іншими постквантовими схемами.
Перспективи розвитку та стандартизація.
Література: 4.

Тема 8. **Гомоморфне шифрування: теорія та застосування.**
Основи гомоморфного шифрування: визначення та види.
Часткове гомоморфне шифрування: адитивне та мультиплікативне.
Повне гомоморфне шифрування: теоретичні основи та алгоритми.
Застосування гомоморфного шифрування у хмарних обчисленнях.
Проблеми ефективності та перспективи розвитку.
Приклади сучасних систем із використанням гомоморфного шифрування.
Література: 5, 6.

Тема 9. **Докази з нульовим розголошенням: концепція та застосування.**

Основи доказів з нульовим розголошенням (ZKP): визначення та принципи.

Інтерактивні та неінтерактивні докази: відмінності та сценарії використання.

Протоколи Zero-Knowledge у блокчейн-системах (наприклад, zk-SNARKs, zk-STARKs, Bulletproofs).

Використання доказів з нульовим розголошенням для захисту конфіденційності.

Технологічні виклики та обмеження реалізації ZKP.

Література: 7, 8.

Тема 10. **Переваги та перспективи застосування ZKP в децентралізованих системах**.
Блокчейн.
Електронне голосування.
Децентралізовані фінанси (DeFi).
Ідентифікація.
Інтернет речей та інші.
Література: 9, 10.

4. Структура залікового кредиту з дисципліни «Криптографія в децентралізованих системах»

	Кількість годин	
	Лекції	Практичні заняття
Змістовий модуль 1. Криптографія та децентралізовані системи		
Тема 1. Вступ до криптографії та децентралізованих систем	2	2
Тема 2. Основні математичні задачі в криптографії	2	2
Тема 3. Криптографічні протоколи	2	2
Тема 4. Цілісність даних в децентралізованих системах	2	2
Тема 5. Протоколи згоди та їх безпека у блокчейн-системах	2	2
Змістовий модуль 2. Постквантова криптографія в децентралізованих системах		
Тема 6. Постквантова криптографія: теорія та алгоритми	2	2
Тема 7. Постквантові криптосистеми на основі кодів	2	2
Тема 8. Гомоморфне шифрування: теорія та застосування	2	2
Тема 9. Докази з нульовим розголошенням: концепція та застосування.	2	2
Тема 10. Переваги та перспективи застосування ZKP в децентралізованих системах	2	2
Разом	20	20

5. Тематика практичних (семінарських або лабораторних) занять

Практичне заняття №1.

Тема: Вступ до криптографічних інструментів та бібліотек

Мета: Ознайомити студентів з основними криптографічними інструментами та бібліотеками (наприклад, OpenSSL, Crypto++, PyCryptodome), які використовуються для розробки децентралізованих систем.

Практичні завдання:

- Генерація пар ключів RSA та ECC.
- Шифрування та дешифрування даних за допомогою різних алгоритмів (AES, RSA).
- Обчислення хеш-функцій (SHA-256, SHA-3).
- Підписи цифрових документів.

Література: 1, 2

Практичне заняття №2.

Тема: Реалізація простих криптографічних протоколів.

Мета: Навчити студентів реалізовувати базові криптографічні протоколи, такі як обмін ключами Diffie-Hellman, протокол цифрового підпису.

Практичні завдання:

Реалізація протоколу обміну ключами Diffie-Hellman.

Реалізація простого протоколу цифрового підпису.

Аналіз вразливостей простих протоколів.

Література: 1, 2.

Практичне заняття №3.

Тема: Застосування криптографії в блокчейні.

Мета: Показати, як криптографічні інструменти використовуються в блокчейні для забезпечення безпеки та довіри.

Практичні завдання:

Реалізація простого блокчейну з використанням криптографії.

Аналіз роботи алгоритму консенсусу (Proof of Work, Proof of Stake).

Створення смарт-контрактів з використанням мови програмування Solidity.

Література: 1, 2.

Практичне заняття №4.

Тема: Криптографічні хеш-функції та їх застосування.

Мета: Дослідити властивості криптографічних хеш-функцій та їх застосування в блокчейні.

Практичні завдання:

Порівняння різних хеш-функцій за швидкістю та стійкістю до атак.

Використання хеш-функцій для створення цифрових відбитків файлів.

Реалізація механізму доказу роботи (Proof of Work) на основі хеш-функцій.

Література: 1, 2.

Практичне заняття №5

Тема: Асиметрична криптографія та її застосування.

Мета: Вивчити принципи роботи асиметричної криптографії та її застосування в децентралізованих системах.

Практичні завдання:

Реалізація протоколу цифрового підпису RSA.

Створення цифрових сертифікатів.

Аналіз атак на системи з відкритим ключем.

Література: 1, 2

Практичне заняття №6

Тема: Симетрична криптографія та її застосування.

Мета: Ознайомити студентів з принципами роботи симетричної криптографії та її застосування в децентралізованих системах.

Практичні завдання:

Реалізація алгоритмів блокового шифрування (AES).

Реалізація алгоритмів потокового шифрування (RC4).

Порівняння ефективності різних алгоритмів симетричного шифрування.

Література: 1, 2.

Практичне заняття №7

Тема: Криптографічні протоколи для безпечного обміну ключами

Мета: Вивчити різні протоколи для безпечного обміну ключами в ненадійних мережах.

Практичні завдання:

Реалізація протоколу Diffie-Hellman.

Реалізація протоколу обміну ключами на основі цифрових сертифікатів.

Аналіз вразливостей протоколів обміну ключами.

Література: 1, 2.

Практичне заняття №8

Тема: Гомоморфне шифрування.

Мета: Ознайомити студентів з концепцією гомоморфного шифрування та його застосуваннями в реальному світі.Надати практичні навички роботи з бібліотеками гомоморфного шифрування. Продемонструвати можливості та обмеження гомоморфного шифрування на простих прикладах. Розвинути критичне мислення щодо застосування гомоморфного шифрування в різних сферах.

Практичні завдання:

Вибір бібліотеки. Ознайомитися з існуючими бібліотеками для гомоморфного шифрування (наприклад, SEAL, PALISADE, TFHE). Вибрати бібліотеку для подальшої роботи, обґрунтувавши свій вибір.

Генерація ключів. Створити пару ключів для гомоморфного шифрування.

Зберегти приватний ключ в безпечному місці.

Шифрування даних. Зашифрувати набір даних (числа, вектори) за допомогою створених ключів.

Виконання простих обчислень над зашифрованими даними:

Здійснити арифметичні операції (додавання, віднімання, множення) над зашифрованими даними.

Переконатися, що результати обчислень правильні після розшифрування.

Література: 1, 2.

Практичне заняття №9

Тема: Докази з нульовим розголошенням (ZKP).

Мета: Ознайомити студентів з концепцією ZKP та їх застосуванням в децентралізованих системах.

Практичні завдання:

Реалізація простого протоколу ZKP.

Використання бібліотек для створення ZKP.

Аналіз застосування ZKP в блокчейні для забезпечення конфіденційності.

Література: 1, 2.

Практичне заняття №10

Тема практичного заняття: Розподілена захищена система зберігання даних: архітектура, безпека та реалізація.

Мета заняття:

1. Ознайомлення з принципами побудови розподілених систем зберігання даних.

2. Вивчення механізмів забезпечення конфіденційності, цілісності та доступності даних у таких системах.

3. Розробка та тестування базової моделі розподіленої системи зберігання з використанням сучасних криптографічних методів.

4. Формування практичних навичок роботи з розподіленими технологіями (IPFS, Storj, Filecoin тощо).

Практичні завдання:

1. Ознайомлення з теоретичними основами розподілених систем:

- розглянути ключові компоненти розподілених систем зберігання даних (ноди, реплікація, шардінг);

- проаналізувати типи атак на такі системи та методи їх запобігання.

2. Дослідження механізмів захисту даних:

- застосувати шифрування для забезпечення конфіденційності даних перед зберіганням;

- реалізувати алгоритм перевірки цілісності з використанням хеш-функцій.

3. Реалізація моделі розподіленої системи:

- побудувати просту модель розподіленого сховища з використанням однієї з технологій (наприклад, IPFS);

- налаштувати механізм розподілу даних між вузлами.

4. Захист системи від зловмисників:

- реалізувати алгоритм авторизації доступу до даних на основі криптографічних ключів;

- забезпечити стійкість до атак типу "людина посередині" та підробки даних.

5. Практичний аналіз продуктивності системи:

- виміряти швидкість зберігання та доступу до даних у розподіленій системі;

- оцінити вплив масштабування системи на її продуктивність.

Література: 1, 2.

6. Самостійна робота

Для самостійної роботи кожному аспіранту пропонується виконання вибраного наскрізного завдання. Орієнтовна тематика наскрізних завдань.

1. Аналіз продуктивності алгоритмів AES, DES і ChaCha20 при шифруванні великих обсягів даних. Дослідіть вплив розміру блоку даних на час виконання.
2. Порівняння ефективності RSA, ECC та ElGamal для шифрування повідомлень різного розміру. Використайте відкриті бібліотеки для реалізації та аналізу.
3. Розробка гібридної криптосистеми з використанням AES та RSA. Оцініть її продуктивність у реальних умовах.
4. Аналіз стійкості протоколу обміну ключами Diffie-Hellman до атак "людина посередині". Змоделюйте атаку та визначте умови її успіху.
5. Дослідження продуктивності протоколу TLS в умовах великої кількості одночасних з'єднань. Виконайте моделювання з різними параметрами конфігурації.
6. Розробка та тестування протоколу аутентифікації для IoT-пристроїв. Дослідіть його захищеність від атак повтору.
7. Реалізація алгоритму перевірки цілісності даних у файлових системах на основі Merkle-дерев. Перевірте ефективність на великих обсягах даних.
8. Моделювання атак на механізми цілісності у децентралізованих системах (наприклад, IPFS). Розробіть рекомендації для покращення захисту.
9. Дослідження стійкості алгоритмів хешування (SHA-256, Blake2) до колізій. Реалізуйте тестування із застосуванням різних наборів даних.
10. Порівняння продуктивності протоколів Proof of Work, Proof of Stake та Delegated Proof of Stake. Оцініть енергетичні витрати та пропускну здатність.
11. Моделювання атаки 51% на блокчейн-систему з використанням симулятора. Визначте шляхи захисту від такої атаки.
12. Розробка та аналіз варіанту протоколу консенсусу для приватного блокчейну. Оцініть його ефективність у мережах з обмеженою кількістю учасників.
13. Реалізація та тестування алгоритму McEliece у постквантовій криптосистемі. Оцініть швидкість шифрування та розшифрування.
14. Аналіз стійкості алгоритмів NTRU та Kyber до атак квантових комп'ютерів. Використайте симуляцію квантових обчислень.
15. Порівняння продуктивності класичних та постквантових алгоритмів у сценаріях обміну ключами. Виконайте вимірювання часу обчислень.
16. Реалізація криптосистеми на основі коду Гоппи. Оцініть обсяг пам'яті, необхідний для зберігання ключів.
17. Дослідження варіантів зменшення розміру ключів у кодових криптосистемах. Протестуйте різні підходи до оптимізації.
18. Моделювання атак на криптосистеми, засновані на кодах Ріда-Соломона. Розробіть стратегії підвищення безпеки.
19. Реалізація протоколу гомоморфного шифрування для обчислення середнього значення зашифрованих даних. Оцініть швидкість обчислень.

20. Дослідження ефективності гомоморфного шифрування для аналізу великих даних у хмарних середовищах. Виконайте тестування на реальних наборах даних.

Ці завдання дозволяють аспірантам поглибити свої знання та навички у різних аспектах криптографії.

7. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни **«Криптографія в децентралізованих системах»** використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- залікове модульне тестування та опитування;
- оцінювання виконання практичних завдань;
- презентації та виступи на наукових заходах;
- інші види індивідуальних та групових завдань;
- екзамен.

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов’язковим повторним курсом)

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

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 10
2.	Комп’ютерна лабораторія. Доступ до Інтернету.	1 - 10

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Salami, Y., Khajevand, V., & Zeinali, E. (2023). Cryptographic algorithms: a review of the literature, weaknesses and open challenges. *J. Comput. Robot*, *16*(2), 46-56.

2. Aumasson, J. P. (2024). *Serious cryptography: a practical introduction to modern encryption*. No Starch Press, Inc.

3. Gancher, J., Sojakova, K., Fan, X., Shi, E., & Morrisett, G. (2023). A core calculus for equational proofs of cryptographic protocols. *Proceedings of the ACM on Programming Languages*, *7*(POPL), 866-892.

4. Bavdekar, R., Chopde, E. J., Agrawal, A., Bhatia, A., & Tiwari, K. (2023, January). Post quantum cryptography: A review of techniques, challenges and standardizations. In *2023 International Conference on Information Networking (ICOIN)* (pp. 146-151). IEEE.

5. Rana, S., Parast, F. K., Kelly, B., Wang, Y., & Kent, K. B. (2023). A comprehensive survey of cryptography key management systems. *Journal of Information Security and Applications*, *78*, 103607.

6. Bashir, I. (2023). *Mastering Blockchain: Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3*. Packt Publishing Ltd.

7. Haidary Makoui, F., Gulliver, T. A., & Dakhilalian, M. (2023). A new code-based digital signature based on the McEliece cryptosystem. *IET Communications*, *17*(10), 1199-1207.

8. Agrawal, R., Ahn, J. H., Bergamaschi, F., Cammarota, R., Cheon, J. H., DM de Souza, F., & Wang, W. (2023, November). High-precision RNS-CKKS on fixed but smaller word-size architectures: theory and application. In Proceedings of the 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (pp. 23-34).

9. Doan, T. V. T., Messai, M. L., Gavin, G., & Darmont, J. (2023). A survey on implementations of homomorphic encryption schemes. The Journal of Supercomputing, 79(13), 15098-15139.

10. The RareSkills Book of Zero Knowledge. Режим доступу: https://www.rareskills.io/zk-book