МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри
кібербезпеки та
інформаційних технологій
Протокол № 18 від 26.08.2025 р.

ПОГОДЖЕНО
Проректор з навчально-методичної
роботи
Каріна НЕМАШКАЛО

МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	**12 Інформаційні технології**
Спеціальність	**125 Кібербезпека та захист інформації**
Освітній рівень	**перший (бакалаврський)**
Освітня програма	**Кібербезпека**
Статус дисципліни	**обов'язкова**
Мова викладання, навчання та оцінювання	**українська**

Розробник д.т.н., с.н.с. Андрій ЧУГАЙ

Завідувач кафедри
кібербезпеки та
інформаційних технологій Ольга СТАРКОВА

Гарант програми Вячеслав ЛИМАРЕНКО

Харків
2025

ВСТУП

Сучасне інформаційне суспільство характеризується стрімким розвитком цифрових технологій, широким впровадженням інформаційно-комунікаційних систем у всі сфери діяльності людини від науки і промисловості до фінансів, медицини, освіти та державного управління. Паралельно з цим зростає й кількість інформаційних загроз, спрямованих на порушення конфіденційності, цілісності та доступності даних. Це зумовлює потребу у створенні математично обґрунтованих методів захисту інформації, здатних забезпечити надійність і довіру до електронних комунікаційних процесів.

В основі будь-якої системи захисту інформації лежать криптографічні методи, які визначають способи перетворення даних з метою унеможливлення їх несанкціонованого використання. Криптологія, як наука, об'єднує два взаємопов'язані напрями — криптографію, що розробляє методи захисту, та криптоаналіз, який вивчає способи їх подолання. Успішний розвиток криптології неможливий без глибоких математичних знань, адже саме математичний апарат є інструментом формального опису, побудови та дослідження алгоритмів шифрування і методів аналізу їхньої стійкості. Дисципліна «Математичні основи криптології» займає фундаментальне місце у підготовці фахівців у галузі інформаційної безпеки, кіберзахисту та прикладної математики. Її завдання полягає у формуванні цілісного розуміння математичних принципів побудови сучасних криптографічних систем, аналізу їх властивостей та оцінки ефективності з точки зору обчислювальної складності.

У курсі розглядаються основи теорії чисел, теорії груп, кілець і полів, комбінаторних структур, теорії інформації, теорії ймовірностей, лінійної та булевої алгебри — саме ті розділи математики, що лежать в основі сучасних криптографічних алгоритмів. Особливу увагу приділено питанням практичної реалізації криптографічних систем симетричних і асиметричних алгоритмів шифрування, систем управління ключами, криптографічних геш-функцій, цифрових підписів, протоколів автентифікації та розподілу секретів. Також розглядаються методи криптоаналізу, які дозволяють оцінити стійкість криптографічних схем до різних типів атак. Вивчення цих питань базується на розумінні математичних основ складності обчислювальних задач, таких як розкладання на множники великих чисел, обчислення дискретного логарифма, знаходження ізоліній на еліптичних кривих тощо.

Курс спрямований не лише на вивчення теоретичних основ, але й на розвиток аналітичного мислення, уміння формулювати та доводити властивості алгоритмів, оцінювати ризики криптографічних рішень і застосовувати математичні методи для практичного моделювання задач безпеки даних.

Мета навчальної дисципліни «Математичні основи криптології» полягає у формуванні в здобувачів системи знань про математичні методи, моделі та алгоритми, що лежать в основі криптографічного захисту інформації, а також у набутті практичних навичок їх застосування для розробки, аналізу та оцінювання стійкості криптографічних систем.

Основними завданнями дисципліни є:

- засвоєння базових понять та принципів криптографії і криптоаналізу; - вивчення математичних основ сучасних криптографічних алгоритмів;

- формування вмінь будувати математичні моделі процесів шифрування та захисту даних;

- набуття практичних навичок аналізу криптосистем з використанням методів теорії чисел, алгебри, комбінаторики та теорії інформації;

- формування здатності оцінювати обчислювальну складність алгоритмів і визначати їхню криптографічну стійкість;

- розвиток навичок критичного мислення у контексті вибору і застосування криптографічних засобів захисту.

Предметом вивчення є математичні методи, моделі та алгоритми, що забезпечують побудову, аналіз і практичну реалізацію криптографічних систем, а також теоретичні основи оцінювання їхньої стійкості до атак.

Об'єктом вивчення є криптографічні та криптоаналітичні методи захисту інформації, які базуються на сучасних математичних теоріях і використовуються для забезпечення безпеки даних у комп'ютерних та комунікаційних системах.

Результати навчання та компетентності, які формує навчальна дисципліна визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	**Компетентності, якими повинен оволодіти здобувач вищої освіти**
РН 7	СК 8
РН 8	СК 8
РН 19	ЗК 5, СК 4, СК 8

де

РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН 8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

СК 4. Здатність забезпечувати захист Інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Змістовий модуль 1. Теоретичні та інформаційні основи криптології

Тема 1. Вступ у криптологію.

1.1. Історичний розвиток криптології.

У цій частині розглядатиметься становлення криптології як науки від перших спроб приховати зміст повідомлень у давнину до сучасних комп'ютерних криптосистем. Будуть наведені приклади класичних методів шифрування, таких як шифр Цезаря та шифр Віженера, розглянуто принципи роботи шифрувальної машини Енігма, а також пояснено, як розвиток обчислювальної техніки спричинив появу електронних алгоритмів шифрування. Окрема увага приділятиметься формуванню основних напрямів криптології криптографії, криптоаналізу, стеганографії та протоколів автентифікації, які разом формують фундамент сучасної інформаційної безпеки.

1.2. Базові поняття.

Цей розділ присвячено ознайомленню з основними термінами та поняттями, без яких неможливе розуміння криптографічних систем. Розглядатимуться визначення шифру, ключа, відкритого та закритого тексту, принцип роботи криптографічної функції, а також поняття криптографічної системи як сукупності алгоритмів і процедур для захисту інформації. Буде також подано загальне уявлення про криптоаналіз — науку, що займається дослідженням методів розкриття зашифрованих повідомлень без знання ключа. Цей матеріал формує теоретичну базу для подальшого вивчення конкретних алгоритмів шифрування.

1.3. Класифікація криптографічних методів.

У межах цього пункту розглядатимуться основні типи криптографічних систем — симетричні та асиметричні алгоритми шифрування, їхні принципи побудови, переваги та обмеження. Буде пояснено, у чому полягає різниця між спільним і відкритим ключем, та які математичні задачі лежать в основі їхньої стійкості. Також буде розглянуто основні принципи створення надійних криптографічних алгоритмів, зокрема важливість випадковості, незворотності функцій та захищеності від криптоаналітичних атак. Окремо буде приділено увагу криптографічним протоколам, цифровому підпису, сертифікації ключів і геш-функціям, як базовим інструментам сучасних систем безпеки.

1.4. Актуальні проблеми криптографії у сучасному світі.

У заключній частині теми буде розглянуто сучасний стан криптографії та основні виклики, які постають перед нею в умовах технологічного прогресу. Особлива увага приділятиметься проблемам постквантової епохи, де традиційні алгоритми можуть втратити свою стійкість через розвиток квантових обчислень. Також розглядатимуться питання довіри до криптографічних стандартів, відкритості алгоритмів, проблеми впровадження національних і міжнародних стандартів, таких як AES, RSA, ECC, SHA. Буде показано роль криптографії у забезпеченні глобальної інформаційної безпеки та напрями її подальшого розвитку.

Тема 2. Інформація та ентропія.

2.1. Поняття інформації в теорії Шеннона.

У цій темі розглядається основне поняття інформації з позиції математичної теорії, закладеної Клодом Шенноном. Пояснюється, як інформація вимірюється не за змістом повідомлення, а за ступенем зменшення невизначеності. Розкривається ймовірнісний підхід до визначення кількості інформації, де кількість інформації залежить від імовірності появи певного повідомлення. Детально вивчається ентропія як міра невизначеності або середньої кількості інформації, що міститься у повідомленні, а також її основні властивості — невід'ємність, максимальність при рівноймовірному розподілі, адитивність.

Окрему увагу приділено розподілу ймовірностей у криптосистемах, де важливим є рівномірність розподілу символів шифротексту. Розглядається поняття інформаційної надлишковості, її роль у виявленні помилок і вплив на криптографічну стійкість. Завершує підрозділ поняття взаємної інформації, що характеризує ступінь залежності між відкритим текстом і шифротекстом, — чим вона менша, тим безпечніша система.

2.2. Зв'язок між ентропією, кількістю можливих ключів і криптографічною стійкістю.

У цьому розділі досліджується, як ентропія пов'язана з кількістю можливих ключів у криптосистемі та її криптографічною стійкістю. Пояснюється, що висока ентропія означає більшу невизначеність для зловмисника і, відповідно, вищий рівень захисту. Вводиться поняття інформаційної ентропії шифротексту, що показує ступінь випадковості зашифрованих даних.

Також розглядається поняття теоретично стійких систем, зокрема система Вернама (One-Time Pad), яка забезпечує абсолютну криптографічну стійкість за умови повної ентропії ключа — коли ключ абсолютно випадковий і не повторюється. Окремо аналізується ідея повної ентропії, яка є теоретичною межею безпеки шифрування, та роль співвідношення між ентропією повідомлення і ключа у досягненні цієї межі.

2.3. Використання ентропійних показників у сучасних методах оцінювання надійності криптосистем.

У цій частині розглядається практичне застосування ентропійних характеристик у сучасних методах аналізу безпеки криптографічних систем. Вивчаються способи вимірювання ентропії ключів, відкритих і зашифрованих текстів, що дозволяє оцінити ступінь випадковості та непередбачуваності криптосистеми.

Пояснюється, як ентропійні показники використовуються для виявлення вразливостей — наприклад, у випадках, коли шифротекст має знижене значення ентропії через систематичні закономірності. Описуються ентропійні тести випадковості, що застосовуються при сертифікації генераторів псевдовипадкових чисел і ключових послідовностей. Також аналізуються сучасні підходи, які поєднують ентропійні та статистичні методи для визначення надійності криптосистем, оцінки ефективності шифрів та контролю якості реалізації криптографічних алгоритмів.

Тема 3. Оцінка трудомісткості криптографічних алгоритмів.

3.1. Поняття трудомісткості та її значення в криптографії.

У цьому підрозділі розглядається, що означає трудомісткість алгоритму — кількісна міра обчислювальних ресурсів (часу, пам'яті, кількості операцій), необхідних для виконання криптографічних процедур. Пояснюється різниця між часовою та просторовою складністю, їх роль у практичній реалізації алгоритмів шифрування, розшифрування, хешування та цифрового підпису.

Наголошується на тому, що оцінка трудомісткості визначає ефективність алгоритму в реальних умовах і дозволяє прогнозувати його стійкість до атак повного перебору. Розглядається поняття асимптотичної складності, записаної через "O"-нотацію, як математичний інструмент для порівняння алгоритмів.

3.2. Методи аналізу обчислювальної складності криптографічних алгоритмів.

Тут розкриваються основні методи оцінювання складності, які використовуються в теоретичному та практичному криптоаналізі. Пояснюється підхід до підрахунку кількості базових операцій (арифметичних, логічних, побітових), необхідних для виконання алгоритму.

Розглядаються емпіричні методи оцінки, які базуються на вимірюванні часу виконання програмних реалізацій на різних платформах. Аналізуються підходи до моделювання середнього, гіршого та кращого випадків у криптографічних задачах. Пояснюється, як трудомісткість пов'язана з енергоспоживанням і продуктивністю криптографічних систем, особливо у вбудованих пристроях та IoT-середовищах.

3.3. Алгоритмічна складність основних криптографічних перетворень.

У цьому підрозділі розглядається трудомісткість типових криптографічних алгоритмів, таких як симетричні (AES, DES), асиметричні (RSA, ECC), хеш-функції (SHA-2, SHA-3) і генератори псевдовипадкових чисел. Пояснюється, які операції є найвитратнішими (наприклад, піднесення до степеня в RSA або операції на еліптичних кривих в ECC).

Надається порівняння обчислювальної складності між класами алгоритмів — симетричні зазвичай швидші, але потребують спільного ключа, тоді як асиметричні більш трудомісткі, проте зручніші у розподілі ключів. Аналізується, як складність залежить від довжини ключа, типу операцій (модульна арифметика, перестановки, підстановки) та архітектури обчислювальної системи.

3.4. Трудомісткість криптоаналізу і криптографічна стійкість.

Цей розділ присвячений співвідношенню між обчислювальною складністю злому та рівнем безпеки криптосистеми. Пояснюється, що криптографічна стійкість визначається кількістю обчислень, необхідних для відновлення ключа або відкритого тексту без знання секретних параметрів.

Розглядаються приклади атак повного перебору, диференціального та лінійного криптоаналізу, а також їх обчислювальна вартість. Описується поняття еквівалентного рівня безпеки (наприклад, 128-бітна безпека означає, що для злому потрібно $\approx 2^{128}$ операцій).

Також пояснюється, як поява квантових обчислень змінює оцінку трудомісткості, зокрема через алгоритми Шора і Гровера, що скорочують складність факторизації та пошуку ключів.

3.5. Практичні аспекти оптимізації та оцінки ефективності реалізацій.

У підрозділі розглядаються методи оптимізації реалізацій криптографічних алгоритмів для підвищення швидкодії та зменшення ресурсних витрат. Пояснюється роль апаратного прискорення (GPU, FPGA, апаратні інструкції AES-NI), а також паралельної обробки даних.

Наголошується на важливості балансу між безпекою та продуктивністю — надто складні алгоритми можуть бути безпечними, але повільними, що неприйнятно для реального часу чи мобільних пристроїв.

Також розглядаються критерії порівняльного аналізу — швидкість шифрування, енергоспоживання, використання пам'яті, масштабованість і час генерації ключів.

Тема 4. Елементарні поняття теорії чисел

4.1. Основні об'єкти теорії чисел: натуральні, прості, складені числа.

Подається класифікація цілих чисел: натуральні числа основні елементи лічби; складені числа ті, що мають більше двох дільників; та прості числа, які діляться лише на 1 і на себе.

Особливу увагу приділено простим числам, оскільки вони є ключовими у побудові криптографічних систем, зокрема RSA. Обговорюється властивість того, що будь-яке натуральне число можна представити у вигляді добутку простих множників — основна теорема арифметики. Саме складність розкладу великих чисел на прості множники лежить в основі обчислювальної складності сучасних криптографічних методів.

4.2. Дільники та кратні. Алгоритм Евкліда для знаходження найбільшого спільного дільника.

У цьому підрозділі розглядаються поняття ділителя та кратного, які відіграють важливу роль у побудові обчислень у теорії чисел. Пояснюється, як визначити найбільший спільний дільник (НСД) двох чисел і його практичне значення — наприклад, при перевірці взаємної простоти чисел у криптосистемах.

Описується алгоритм Евкліда, який дозволяє швидко знайти НСД за допомогою послідовних операцій ділення з остачею. Також наводиться розширений алгоритм Евкліда, що дає змогу знайти коефіцієнти, які лінійно поєднують два числа, — цей метод використовується при обчисленні мультиплікативної зворотної за модулем.

Змістовий модуль 2. Алгебраїчні та комбінаторні основи криптографії

Тема 5. Важливі функції теорії чисел.

5.1. Арифметичні функції та основні теореми теорії чисел.

Розглядаються функції Ейлера, Мобіуса та Кармайкла, їхні властивості, взаємозв'язки та застосування у криптографії. Вивчаються теореми Ферма й Ейлера та їх роль у побудові та оптимізації криптографічних алгоритмів.

5.2. Використання функцій теорії чисел у криптосистемах.

Аналізується застосування арифметичних функцій при побудові систем RSA, Diffie–Hellman, ElGamal. Розглядається поняття порядку елемента в

мультиплікативній групі, а також відмінності між простими та складеними модулями.

5.3. Генерація та перевірка простих чисел у криптографії.

Вивчаються методи генерації великих простих чисел, стохастичні тести простоти (Ферма, Міллера–Рабіна, Соловея–Штрассена), використання псевдопростих чисел і принципи реалізації генерації простих у сучасних криптографічних бібліотеках.

Тема 6. Елементи комбінаторики у криптології.

6.1. Базові комбінаторні принципи та кількісна оцінка простору ключів.

Розгляд правил суми і добутку, перестановок, розміщень і сполучень; застосування цих понять для підрахунку розміру простору ключів та кількості можливих повідомлень або конфігурацій. Оцінка кількості варіантів атак (наприклад, кількість можливих ключів для brute-force) та наслідки збільшення довжини ключа для безпеки.

6.2. Ймовірнісні моделі та закони великої кількості випадків у криптоаналізі.

Використання ймовірнісних оцінок для моделювання ймовірності успішного розкриття шифру, роль закону великих чисел і оцінок середнього поведінки у статистичних атаках. Моделі випадкових подій у протоколах (наприклад, генерація випадкових nonces, колізії) та способи кількісної оцінки ризиків.

6.3. Комбінаторні підходи в генераторах псевдовипадкових послідовностей і оцінка атак.

Застосування комбінаторики при побудові та аналізі PRNG/PRF (кількість можливих станів, період, кореляції між елементами). Аналіз ефективності повного перебору (brute-force) з урахуванням комбінаторних оптимізацій, а також оцінка ймовірнісних та структурних атак, що використовують комбінаторні властивості простору ключів і вихідних послідовностей.

Тема 7. Конгруенції та криптографічні застосування.

7.1. Основні поняття та властивості конгруенцій.

Визначення конгруенції, базові властивості й операції. Розв’язання лінійних і квадратичних конгруенцій та їх практичне значення у криптографії, зокрема при побудові алгоритмів шифрування й цифрового підпису.

7.2. Китайська теорема про залишки (CRT) та мультиплікативна група за модулем.

Розгляд принципів Китайської теореми про залишки, способів її використання для прискорення обчислень у системах RSA та інших алгоритмах з великими числами. Поняття мультиплікативної групи за модулем і її роль у побудові криптографічних протоколів.

7.3.Криптографічні застосування конгруенцій.

Використання конгруенцій у побудові геш-функцій, генераторів псевдовипадкових чисел (лінійних конгруентних генераторів), а також у методах формування ключів та перевірки автентичності повідомлень.

Тема 8. Алгебраїчні структури у криптографії.

8.1. Основні алгебраїчні структури: групи, кільця та поля.

Визначення та властивості груп, кілець і полів. Розгляд операцій над елементами цих структур і їх значення для побудови криптографічних алгоритмів. Пояснення, чому саме поля забезпечують зворотність операцій, необхідну для шифрування та дешифрування.

8.2. Кінцеві поля та їх побудова.

Огляд полів GF(p) і $GF(2^n)$, способів їх побудови за допомогою незвідних поліномів. Операції додавання, множення, знаходження оберненого елемента в скінченних полях. Приклади використання у криптографії реалізація операцій у симетричних шифрах, зокрема в алгоритмі AES.

8.3. Застосування алгебраїчних структур у криптографічних перетвореннях.

Використання лінійних і нелінійних відображень при побудові підстановок (S-box) та перестановок у блокових шифрах. Роль алгебраїчних властивостей у побудові стійких систем шифрування, кодуванні інформації та створенні цифрових підписів.

Тема 9. Еліптичні криві та сучасна криптографія.

9.1. Основи теорії еліптичних кривих і групові операції.

Визначення еліптичної кривої над дійсними та скінченними полями. Геометричне тлумачення додавання точок, побудова групи точок еліптичної кривої. Алгоритми додавання та подвоєння точок, що лежать в основі криптографічних операцій.

9.2. Криптографічні системи на еліптичних кривих.

Розгляд задачі дискретного логарифма на еліптичній кривій (ECDLP) як основи стійкості таких систем. Основи роботи криптосистем ECDSA (цифровий підпис), ECDH (узгодження ключів) та Ed25519 (ефективна реалізація підпису).

9.3. Переваги та виклики еліптичної криптографії.

Порівняння еліптичної криптографії з класичними системами (RSA, Diffie–Hellman): менша довжина ключа при тій самій стійкості, висока ефективність. Обговорення постквантових загроз і перспектив розвитку стійких до квантових атак схем.

У процесі вивчення дисципліни здобувачі отримують системні знання про математичні основи криптографічного захисту інформації, навички аналітичного оцінювання складності алгоритмів і стійкості криптосистем, розуміння алгебраїчних і комбінаторних принципів, що лежать в основі сучасних методів шифрування.

Перелік лабораторних занять за навчальною дисципліною наведено в табл. 2.

Таблиця 2

Перелік лабораторних робіт

Назва теми та / або завдання	Зміст
Тема1. Лабораторна робота 1. Вступ до криптології	Ознайомлення з основними поняттями криптології: криптографія, криптоаналіз, ключі, повідомлення. Аналіз історичних методів шифрування (Цезаря, Віженера, Трітемія). Демонстрація базових операцій шифрування та дешифрування. Визначення основних принципів безпеки шифрів.
Тема 2. Лабораторна робота 2. Інформація та ентропія	Обчислення ентропії повідомлень у різних мовах. Аналіз інформаційної надлишковості текстів. Порівняння ентропії відкритого та зашифрованого тексту. Використання ентропійного аналізу для оцінки стійкості шифрів.
Тема 3. Лабораторна робота 3. Оцінка трудомісткості криптографічного алгоритму	Аналіз складності обчислень для типових криптографічних задач. Експериментальне дослідження часу виконання алгоритмів шифрування і дешифрування залежно від довжини ключа. Оцінка ефективності криптографічних систем за часовими та ресурсними параметрами.
Тема 4. Лабораторна робота 4. Елементарні поняття теорії чисел	Ознайомлення з поняттями ділення, остачі, взаємно простих чисел. Виконання операцій у модульній арифметиці. Реалізація алгоритму Евкліда для знаходження найбільшого спільного дільника. Застосування цих понять у криптосистемах. Прості числа , алгоритм пошуку простих чисел
Тема 5.Лабораторна робота 5. Важливі функції теорії чисел	Обчислення функції Ейлера, сигма-функції та функції Мебіуса. Використання функції Ейлера у криптографічних алгоритмах (RSA). Перевірка властивостей чисел, важливих для генерації ключів.
Тема 6. Лабораторна робота 6. Елементи комбінаторики	Розрахунок кількості можливих ключів, перестановок та комбінацій у різних криптосхемах. Дослідження впливу розміру ключового простору на криптостійкість. Моделювання комбінаторних процесів у задачах шифрування.
Тема 7, 8. Лабораторна робота 7. Алгебраїчні структури	Ознайомлення з групами, кільцями, полями як основою побудови сучасних криптосистем. Операції у скінченних полях GF(p). Застосування алгебраїчних структур у сучасних шифрах (RSA, ECC). Практичне виконання операцій над елементами поля.

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3

Таблиця 3

Перелік самостійної роботи

Тема	Зміст роботи
Тема 1. Вступ до криптології	1. Дослідити історію розвитку одного класичного методу шифрування (Цезар, Віженер, Енігма) та порівняти його з сучасним аналогом. 2. Підготувати таблицю з порівнянням симетричних та асиметричних алгоритмів шифрування (переваги, недоліки, приклади). 3. Проаналізувати роль стандартів AES, RSA, ECC, SHA у сучасній безпеці цифрових систем.
Тема 2. Інформація, ентропія та міри невизначеності	1. Розрахувати ентропію заданого тексту (українською або англійською мовою) за методом Шеннона. 2. Дослідити залежність між ентропією повідомлення та криптостійкістю алгоритму. 3. Навести приклади систем, у яких використовується ідея повної ентропії (система Вернама).
Тема 3. Оцінка трудомісткості криптографічних алгоритмів	1. Пояснити відмінності між класами задач P, NP, NP-повними, навівши приклади. 2. Розрахувати трудомісткість виконання шифрування для простого симетричного алгоритму. 3. Підготувати короткий огляд впливу квантових алгоритмів (Шора, Гровера) на сучасну криптографію.
Тема 4. Елементарні поняття теорії чисел	1. Реалізувати алгоритм Евкліда для знаходження НСД двох чисел. 2. Розв’язати приклади з модульної арифметики, показавши використання у криптосистемах RSA або Diffie–Hellman. 3. Пояснити, як мультиплікативний обернений за модулем використовується у криптографії.
Тема 5. Функції теорії чисел та їх криптографічне застосування	1. Розрахувати значення функції Ейлера $\varphi(n)$ для кількох заданих чисел. 2. Навести приклади використання теореми Ейлера або Ферма у системах RSA чи ElGamal. 3. Дослідити роботу стохастичних тестів простоти (Міллера–Рабіна, Ферма) на прикладах.
Тема 6. Елементи комбінаторики та теорії ймовірностей у криптології	1. Обчислити кількість можливих ключів для системи з заданою довжиною ключа. 2. Проаналізувати ймовірність успішної brute-force-атаки залежно від довжини ключа. 3. Дослідити роль закону великих чисел у криптоаналізі та генераторах випадкових чисел.
Тема 7. Конгруенції та криптографічні застосування	1. Розв’язати систему конгруенцій із застосуванням Китайської теореми про залишки. 2. Навести приклад використання конгруенцій у геш-функціях або генераторах псевдовипадкових чисел.

	3. Реалізувати перевірку конгруенції для обчислення хешу в простому прикладі.
Тема 8. Алгебраїчні структури у криптографії	1. Навести приклади груп, кілець і полів, що використовуються в криптографії (зокрема $GF(2^n)$). 2. Пояснити принцип побудови поля $GF(2^8)$, яке використовується в алгоритмі AES. 3. Проаналізувати приклад лінійного та нелінійного відображення у шифрі підстановки.
Тема 9. Еліптичні криві та сучасна криптографія	1. Вивести рівняння еліптичної кривої над полем GF(p) і побудувати кілька точок. 2. Продемонструвати операцію додавання точок на еліптичній кривій графічно або числово. 3. Провести короткий аналіз криптосистеми ECDSA — описати принципи та переваги. 4. Підготувати міні-реферат про постквантові загрози для криптографії на еліптичних кривих.

Кількість годин лекційних та лабораторних занять та годин самостійної роботи наведено в робочому плані (технологічній карті) з навчальної дисципліни.

МЕТОДИ НАВЧАННЯ

У процесі викладання навчальної дисципліни для набуття визначених результатів навчання, активізації освітнього процесу передбачено застосування таких методів навчання, як:

Словесні (Теми 1-9).

Наочні (демонстрація (Тема 1-9)).

Лабораторні роботи (Теми 1-9)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних, лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів, для дисциплін з формою семестрового контролю залік: максимальна сума – 100 балів; мінімальна сума – 60 балів.

Підсумковий контроль включає семестровий контроль та атестацію здобувача вищої освіти.

Семестровий контроль проводиться у формі диференційованого заліку.

Підсумкова оцінка за навчальною дисципліною визначається: для дисциплін з формою семестрового контролю залік – сумуванням всіх балів, отриманих під час поточного контролю.

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи: Поточний контроль: лабораторні роботи (90 балів), письмова

контрольна робота (10 балів). Семестровий контроль: Залік

Більш детальну інформацію щодо системи оцінювання наведено в робочому плані (технологічній карті) з навчальної дисципліни.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В. Кібербезпека: основи кодування та криптографії: навч. Посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов. – Харків: ХПІ, 2023. – 658 с.
2. Стасюк М. Елементи математичних основ криптографії : навчальний посібник / М. Стасюк. – Львів : ЛДУ БЖД, 2021. – 216 с.
3. Щур Н.О. Основи криптології: навч. Посібник / Н.О. Щур, О.А. Покотило. – Житомир: Державний університет «Житомирська політехніка» . – 2021. – 120с.
4. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Кондор, 2021. - 272 с.
5. Остапов С. Е. Кібербезпека: сучасні технології захисту : навч. посіб. Львів : Новий Світ-2000, 2021. - 679 с.
6. Євсеєв, С. П. Лабораторний практикум з основ криптографічного захисту [Електронний ресурс] : навч. посіб. / С. П. Євсеєв, О. В. Мілов, О. Г. Король ; Харківський національний економічний університет ім. С. Кузнеця. - Електрон. текстові дан. (12,3 МБ). - Харків : ХНЕУ ім. С. Кузнеця, 2020. - 221 с. http://www.repository.hneu.edu.ua/handle/123456789/24508
7. Математичні моделі і методи прийняття рішень. Лабораторний практикум для здобувачів вищої освіти спеціальностей 122 “Комп’ютерні науки”, 126 “Інформаційні системи та технології” другого (магістерського) рівня / Н. Д. Сізова, О. О. Шаповалова. - Харків: ХНУБА, 2021. - 144 с. http://repository.hneu.edu.ua/handle/123456789/31956

Додаткова

8. Barakat M. An Introduction to Cryptography [Electronic resource]. / Mohamed Barakat, Christian Eder, Timo Hanke . – September 20, 2018. – 145 pp. –. Available at: https://agag-ederc.math.rptu.de/~ederc/download/Cryptography.pdf.
9. Bellare M. Introduction to modern cryptography [Electronic resource]. – / Mihir Bellare and Phil Rogaway. – May 11, 2005. – 283 pp. – Available at: https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.
10. Bourke C. CSCE 477/877: Cryptography and Computer Security [Electronic resource] / Chris Bourke. – Department of Computer Science & Engineering, University of Nebraska–Lincoln. – 2015. – 138 pp. – Available at: https://cse.unl.edu/~cbourke/cryptoNotes.pdf .
11. Boneh D. A Graduate Course in Applied Cryptography / Dan Boneh, Victor Shoup. – 2020. – 943 p.
12. Kölbl S. Design and Analysis of Cryptographic Algorithms [Electronic

resource] : [A Report on Ph.D. thesis] / Stefan Kölbl.– DTU Compute PHD-2016. – Number 434. – Kgs. Lyngby, Technical University of Denmark. – 2017. – 272 pp. – Available at: Design and analysis of cryptographic algorithms — Welcome to DTU Research Database.

13. Lecture Notes on Introduction to Cryptography [Electronic resource]. – [Course 15356/15856, Fall 2020] / E. Masserova. – Vipul Goyal, CMU. – 119 pp. – Available at: https://www.cs.cmu.edu/~goyal/15356/lecture_notes.pdf. 11.Shivakumar V. A Report on Application of Cryptography and Groups [Electronic resource] – / V. Shivakumar. – May 2020. – 27 pp. – Available at: (PDF) Application of Cryptography and Groups (researchgate.net) . https://www.math.wustl.edu/~matkerr/NTCbook.pdf.

14. Сучасні інформаційні технології та системи [Електронний ресурс] : монографія / Н. Г. Аксак, Л. Е. Гризун, О. В. Щербаков [та ін.] ; за заг. ред. Пономаренка В. С. — Електрон. текстові дан. (22,9 МБ). — Харків: ХНЕУ ім. С. Кузнеця, 2022. — 270 с. http://repository.hneu.edu.ua/handle/123456789/29233

15. Yevseiev S. Evaluation of Cryptographic Strength and Energy Intensity of Design of Modified Crypto-Code Structure of McEliece with Modified Elliptic Codes / S. Yevseiev, O. Korol, O. Veselska, S. Pohasii, V. Khvostenko // Міжнар. наук.-практ. конф. «Інформаційна безпека та інформаційні технології», Харків – Одеса, 13-19 вер. 2021 р. : матер. конф. – Харків : ХНЕУ ім. С. К узнеця. http://repository.hneu.edu.ua/handle/123456789/26827

Інформаційні ресурси

16. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Математичні основи криптології" https://pns.hneu.edu.ua/course/view.php?id=8977