МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«___» _____ 20___р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«___» _____ 20___р.

РОБОЧА ПРОГРАМА

з дисципліни

«КРИПТОГРАФІЯ»

ступінь вищої освіти – **бакалавр**

галузь знань – **12 Інформаційні технології**

спеціальність – **125 Кібербезпека**

освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестри	Лекції (год.)	Лаб. занять (год.)	ІРС (год.)	Тренінг, КПІЗ (год)	СРС (год)	Разом (год.)	Іспит
Денна	3	5	42	42	5	8	53	150	5

31.08.2023 р.

Тернопіль - 2023

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека, затвердженої Вченою радою ЗУНУ (протокол №9 від 26.05.2021 р.)..

Робочу програму склав доктор технічних наук, професор, професор кафедри кібербезпеки Михайло КАСЯНЧУК

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол №1 від 28. 08. 2023 р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол №1 від 30. 08. 2023 р.

Керівник групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Ігор ЯКИМЕНКО

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни “Криптографія”

Дисципліна “Криптографія”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	галузь знань – 12 Інформаційні технології	**Статус дисципліни** обов’язкова **Мова навчання** українська
Кількість залікових модулів – 4	спеціальність – 125 Кібербезпека	Рік підготовки: *Денна – 3* Семестр: *Денна – 5*
Кількість змістових модулів – 3	ступінь вищої освіти – бакалавр	Лекції (год): *Денна – 42* Лабораторні заняття (год): *Денна – 42*
Загальна кількість годин – 150		Самостійна робота (год): *Денна – 61* (в т.ч. тренінг, КПІЗ – 8 год.) Індивідуальна робота (год): *Денна – 5*
Тижневих годин – 10, з них аудиторних – 6		Вид підсумкового контролю – іспит

2. Мета й завдання вивчення дисципліни “Криптографія”

2.1. Мета завдання дисципліни

Мета вивчення дисципліни “Криптографія” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного криптографічного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу “Криптографія» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи кібербезпеки», „Лінійна алгебра та аналітична геометрія”, «Дискретна математика», «Фізика», «Основи програмування»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни.

В результаті вивчення курсу „Криптографія” студенти повинні:

- засвоїти основні фундаментальні поняття і закони криптографічного захисту інформації для їх використання в сучасних системах;
- знати принципи побудови криптографічних алгоритмів, криптографічних стандартів та їх використання в задачах захисту інформації;
- використовувати основні математичний апарат та закони криптографії в професійній діяльності;
- вміти використовувати програмні засоби, які реалізують основні криптографічні функції;
- програмно реалізовувати криптографічні алгоритми вирішення типових задач захисту інформації;
- проектувати різного рівня криптографічні системи захисту;
- вміння використовувати методи та засоби криптографічного захисту даних.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Криптографія». Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Криптографія» та формуванні у студентів цілісної системи теоретичних знань з курсу «Криптографія».

Завдання проведення лабораторних занять

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення лабораторних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

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

- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
- здатність до пошуку, оброблення та аналізу інформації;
- здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;
- здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.);
- здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності;
- здатність виконувати оцінку якості криптографічного захисту інформації в інформаційно-телекомунікаційних системах.

2.4. Передумови для вивчення дисципліни

Вивчення курсу “Криптографія» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи кібербезпеки», „Лінійна алгебра та аналітична геометрія”, «Дискретна математика», «Фізика», «Основи програмування»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.5. Результати навчання

- виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах;
- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно телекомунікаційних системах програмно апаратними засобами та давати оцінку результативності якості прийнятих рішень;
- забезпечувати процеси захисту та функціонування інформаційно телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;
- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах;
- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
- впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
- приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

– забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

– підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно телекомунікаційних системах.

3. Програма навчальної дисципліни “Криптографія"

Змістовий модуль 1. Симетричні криптосистеми.

Тема 1. Вступ. Шифри перестановки та простої заміни.

Вступ. Задачі криптографії. Основні поняття та положення комп’ютерної криптографії. Принципи криптографічного захисту інформації. Криптоаналітичні атаки. Їх види. Шифр скитала. Шифруючі таблиці. Шифр магічних квадратів. Шифр Кардано. Шифр атбаш. Полібіанський квадрат. Шифр Цезаря. Шифр Цезаря з ключовим словом. Шифруючі таблиці Трисемуса.

Тема 2. Шифри складної заміни. Шифр одноразового блокноту.

Шифр Гронсфельда. Шифр Гронсфельда з ключовим словом. Шифр Віженера. Шифр Віженера з ключовим словом. Роторні шифрувальні машини. Роторна шифрувальна машина Enigma. Біграмний шифр Плейфейра. Подвійний квадрат Уїтстона. Шифр чотирьох квадратів. Шифр ADFGVX. Шифр одноразового блокноту.

Тема 3. Алгоритм DES.

Структура алгоритму DES. Його переваги та недоліки. Операції алгоритму DES. Функція шифрування алгоритму DES. Генерація підключів алгоритму DES. Режими роботи алгоритму DES: електронна кодова книга, зчеплення блоків шифру, зворотній зв’язок по шифртексту, зворотній зв’язок по виходу. Галузі застосування алгоритму DES.

Тема 4. Алгоритми IDEA та ГОСТ28147–89.

Структура алгоритму IDEA. Його переваги та недоліки. Операції алгоритму IDEA. Генерація підключів алгоритму IDEA. Загальна структура алгоритму ГОСТ28147–89. Його переваги та недоліки. Операції алгоритму ГОСТ28147–89. Генерація підключів алгоритму IDEA. Режими роботи алгоритму ГОСТ28147–89: проста заміна, гамування, гамування із зворотним зв’язком, вироблення імітовставки. Галузі застосування алгоритмів IDEA та ГОСТ28147–89.

Тема 5. Український та світовий стандарти симетричного шифрування.

Український стандарт симетричного шифрування «Калина». Світовий стандарт симетричного шифрування AES (Rijndeal).

Тема 6. Сімейство алгоритмів RC.

RC-подібні алгоритми. Алгоритми RC 2, RC 4, RC 5, RC 6.

Змістовий модуль 2. Асиметричні криптосистеми та хеш-функції.

Тема 7. Арифметика асиметричних криптосистем.

Основні поняття. Алгоритм Евкліда, його наслідок, пошук оберненого елемента, китайська теорема про остачі. Функція Ейлера. Теореми Ейлера та Ферма.

Тема 8. Криптосистема RSA.

Опис криптосистеми RSA. Генерування ключів. Шифрування та розшифрування. Коректність, ефективність та надійність криптосистеми.

Тема 9. Криптосистема Рабіна.

Генерування ключів криптосистеми Рабіна. Шифрування та розшифрування в криптосистемі Рабіна. Коректність, ефективність та надійність криптосистеми.

Тема 10. Криптосистема Ель–Гамаля.

Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля. Коректність, ефективність та надійність криптосистеми.

Тема 11. Електронний цифровий підпис.

Поняття електронного цифрового підпису. Електронний цифровий підпис в системах RSA та Ель–Гамаля. Алгоритм DSA. Система Шнорра. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.

Тема 12. Шифрування із паролем.

Шифрування із паролем. Апаратні пристрої збереження ключів. Криптографічні акселератори. Біометрична ідентифікація.

Тема 13. Поняття хеш-функції. Застосування хеш-функцій.

Визначення функції хешування та вимоги до неї. Алгоритм функції хешування по ГОСТ Р 34.11-94. Аналіз алгоритму та особливостей його програмної реалізації. Геш-функції на основі ділення. Мультиплікативна схема гешування. Гешування рядків змінної довжини. Криптографічні хеш-функції. Геометричне гешування. Прискорення пошуку даних.

Тема 14. Хеш-функції типу MD та SHA. Український стандарт хешування.

Хеш-функція MD (MD-2, MD-4, MD-5). Сімейство хеш-функцій SHA (SHA-1, SHA-2, SHA-3, SHA-256). Український стандарт хешування ДСТУ 7564:2014 «Купина».

Тема 15. Генерація ЕЦП на основі хеш-функцій.

Процедура вироблення та перевірки електронного підпису по ДСТУ 4145-2002. Генерація загальних параметрів, секретного та відкритого ключів. Особливості програмної реалізації процедури. Алгоритм DSA.

Змістовий модуль 3. Еліптична та квантова криптографія, елементи стеганографії.

Тема 16. Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих.

Еліптичні криві над кінцевими полями. Еліптичні криві над полями непарної характеристики. Теорема Хассе. Еліптичні криві над полями характеристики 2. Проективні координати. Швидка редукція (NIST-криві). Еліптичні криві, рекомендовані NIST. Розмір ключа.

Тема 17. ЕЦП на основі еліптичних кривих

Особливості ЕЦП на основі еліптичних кривих. Вибір параметрів. Генерування ключів ECDSA. Переваги ECDSA перед DSA. Практична реалізація.

Тема 18. Криптографічні протоколи

Визначення криптографічного протоколу. Перелік вимог до криптографічного протоколу. Аналіз атак на криптографічні протоколи. Використання симетричного та несиметричного шифрування в криптографічних протоколах.

Тема 19. Приклади сучасних комп'ютерних криптографічних систем.

Характеристики протоколу SSL компанії Netscape Communication Corporation для захисту інформаційного обміну в середовищі Інтернет. Ієрархія ключів, блок-схема розсилки ключів абонентам мережі, блок-схема забезпечення цифрового підпису даних в мережі.

Тема 20. Елементи стеганографії.

Комп'ютерна стеганографія. Методи вкладення інформації у файли мультимедіа. Методи приховування інформації в зображеннях. Методи приховування інформації в аудіо сигналах.

Тема 21. Квантова криптографія

Поняття квантової криптографії. Квантовий розподіл ключів. Способи та пристрої генерації та передачі одиночних фотонів. Фазове та часове кодування. Основні напрямки розвитку та проблеми квантової криптографії. Порівняльний аналіз протоколів квантової криптографії.

4. Структура залікового кредиту дисципліни “Криптографія”

	Кількість годин					
	Лек-ції	Лабора-торні занятт я	Самостій-на робота	Індиві-дуальна робота	Тренінг, КПІЗ	Контро-льні заходи
Змістовий модуль 1. **Симетричні криптосистеми.**						
Тема 1. Вступ. Шифри перестановки та простої заміни.	2	2	5	-	2	Поточне опитува-ння
Тема 2. Шифри складної заміни. Шифр одноразового блокноту.	2	2	3	-		Поточне опитува-ння
Тема 3. Алгоритм DES.	2	2	3	-		Поточне опитува-ння
Тема 4. Алгоритми IDEA та ГОСТ28147–89.	2	2	-	-		Поточне опитува-ння

Тема 5. Український та світовий стандарти симетричного шифрування.	2	2	-	1		Поточне опитування
Тема 6. Сімейство алгоритмів RC.	2	2	-	1		Поточне опитування
Змістовий модуль 2. **Асиметричні криптосистеми та хеш-функції**						
Тема 7. Арифметика асиметричних криптосистем.	2	2	3	-	3	Поточне опитування
Тема 8. Криптосистема RSA.	2	2	3	-		Поточне опитування
Тема 9. Криптосистема Рабіна..	2	2	3	-		Поточне опитування
Тема 10. Криптосистема Ель–Гамаля.	2	2	3	-		Поточне опитування
Тема 11. Електронний цифровий підпис.	2	2	6	-		Поточне опитування
Тема 12. Шифрування із паролем.	2	2	3	-		Поточне опитування
Тема 13. Поняття хеш-функції. Застосування хеш-функцій	2	2	3	-		Поточне опитування
Тема 14. Хеш-функції типу MD та SHA. Український стандарт хешування	2	2	3	1		Поточне опитування
Тема 15. Генерація ЕЦП на основі хеш-функцій	2	2	6	1		Поточне опитування
Змістовий модуль 3. **Еліптична та квантова криптографія, елементи стеганографії.**						
Тема 16. Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих.	2	2	3	-	3	Поточне опитування
Тема 17. ЕЦП на основі еліптичних кривих.	2	2	3	-		Поточне опитування
Тема 18. Криптографічні протоколи.	2	2	-	-		Поточне опитування
Тема 19. Приклади сучасних комп'ютерних криптографічних систем.	2	2	3	-		Поточне опитування
Тема 20. Стеганографія.	2	2	-	-		Поточне опитування
Тема 21. Квантова криптографія	2	2	-	1		Поточне опитування
Разом	42	42	53	5	8	

5. Тематика лабораторних занять.

Лабораторне заняття № 1

Тема: Реалізація шифрів перестановки.

Мета: Реалізація шифрів перестановки.

Література: 1-14.

Лабораторне заняття №2

Тема: Реалізація шифрів простої та складної заміни.

Мета: Реалізувати шифри простої та складної заміни.

Література: 1-14.

Лабораторне заняття № 3

Тема: Реалізація біграмних шифрів.

Мета: Реалізувати біграмні шифри.

Література: 1-14.

Лабораторне заняття № 4

Тема: Реалізація шифру одноразового блокноту.

Мета: Запрограмувати процес шифрування та дешифрування за допомогою шифру одноразового блокноту.

Література: 1-14.

Лабораторне заняття № 5

Тема: Вивчення стандарту шифрування даних DES.

Мета: Засвоїти методику побудови симетричних алгоритмів шифрування даних.

Література: 1-14.

Лабораторне заняття № 6

Тема: Реалізація стандарту шифрування даних DES.

Мета: Реалізація стандарту шифрування даних DES

Література: 1-14.

Лабораторне заняття № 7

Тема: Вивчення та реалізація режимів шифрування даних стандартом DES.

Мета: Вивчити та реалізувати режими шифрування даних стандартом DES.

Література: 1-14.

Лабораторне заняття № 8

Тема: Алгоритм IDEA.

Мета: Вивчити та дослідити алгоритм IDEA.

Література: 1-14.

Лабораторне заняття №9

Тема: Сімейство алгоритмів RC.

Мета: Вивчення та дослідження сімейства алгоритмів RC

Література: 1-14.

Лабораторне заняття № 10

Тема: Український та світовий стандарти симетричного шифрування..

Мета: Вивчення та дослідження українського та світового стандартів симетричного шифрування.

Література: 1-14.

Лабораторне заняття №11

Тема: Арифметика асиметричних криптосистем.

Мета: Вивчення та дослідження арифметики асиметричних криптосистем.

Література: 1-14.

Лабораторне заняття №12

Тема: Реалізація афінних шифрів.

Мета: Запрограмувати процес шифрування та дешифрування в афінних шифрах.

Література: 1-14.

Лабораторне заняття № 13

Тема: Вивчення процедури шифрування та дешифрування в криптосистемі RSA.

Мета: Засвоїти методику та отримати практичні навики побудови засобів захисту інформації на основі криптосистеми RSA.

Література: 1-16.

Лабораторне заняття № 14

Тема: Реалізація процедури шифрування та дешифрування в криптосистемі RSA.

Мета: Запрограмувати процедури шифрування та дешифрування в криптосистемі RSA.
Література: 1-14.

Лабораторне заняття № 15

Тема: Реалізація схеми шифрування Ель-Гамаля.
Мета: Запрограмувати схему шифрування Ель-Гамаля
Література: 1-14.

Лабораторне заняття № 16

Тема: Вивчення та дослідження особливостей побудови електронного цифрового підпису на основі алгоритму RSA.
Мета: Засвоїти методику та отримати практичні навики побудови електронних підписів на прикладі ЕЦП на основі алгоритму RSA
Література: 1-14.

Лабораторне заняття № 17

Тема: Реалізація електронного цифрового підпису на основі алгоритму RSA.
Мета: Запрограмувати алгоритм електронного цифрового підпису на основі алгоритму RSA.
Література: 1-14.

Лабораторне заняття № 18

Тема: Поняття хеш-функції. Генерування та види хеш-функцій.
Мета: Вивчити та дослідити поняття хеш-функції, її види та методи генерування.
Література: 1-14.

Лабораторне заняття № 19

Тема: Хеш-функції типу SHA. Український стандарт хешування. Генерація ЕЦП на основі хеш-функцій.
Мета: Вивчити та дослідити хеш-функції типу SHA, український стандарт хешування, генерацію ЕЦП на основі хеш-функцій.
Література: 1-14.

Лабораторне заняття № 20

Тема: Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих. ЕЦП на основі еліптичних кривих.
Мета: Вивчення поняття еліптичної криптографії. Вивчення та дослідження методів реалізації шифрування на еліптичних кривих. Вивчення та дослідження ЕЦП на основі еліптичних кривих.
Література: 1-14.

Лабораторне заняття № 21

Тема: Криптографічні протоколи обміну ключем, жеребу по телефону, розподілу таємниці. Приклади сучасних комп'ютерних криптографічних систем.
Мета: Вивчення та дослідження криптографічних протоколів обміну ключем, жеребу по телефону, розподілу таємниці. Вивчення та дослідження прикладів сучасних комп'ютерних криптографічних систем.
Література: 1-14.

6. Комплексне практичне індивідуальне завдання (КПІЗ).

Індивідуальне завдання з курсу “Криптографія” виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Метою виконання КПІЗ є дослідження та оволодіння навиками застосування криптографічних алгоритмів для конкретних задач. Студенти повинні дослідити та застосувати криптографічні алгоритми за одним із варіантів:

1. Розробка та аналіз простих криптографічних алгоритмів на основі методів перестановок та підстановок.
2. Генерація псевдовипадкових послідовностей чисел в системах захисту інформації.
3. Оцінка статистичних характеристик датчика псевдовипадкових чисел із заданим законом розподілу.
4. Розробка і реалізація варіанта симетричного криптографічного алгоритму з DES – подібною структурою.
4. Оцінка швидкості роботи криптоалгоритму.

5. Розробка алгоритму та програмна реалізація атаки на симетричну криптографічну систему.

6. Програмна реалізація алгоритму RSA.

7. Розробка і програмна реалізація протокола обміну симетричними ключами на основі алгоритму Diffyie-Hellman.

8. Розробка і програмна реалізація алгоритму обчислення цифрового дайджеста повідомлення.

9. Програмна реалізація алгоритмів цифрового підпису.

10. Схема режиму шифрування DES-ECB.

11. Схема режиму шифрування DES-CBC.

12. Схема режиму шифрування DES-CPB и DES-OFB.

13. Потрійний DES. Сфери застосування різних режимів DES.

14 Схема режиму шифрування простої заміни ГОСТ 28147-89.

15. Реалізація алгоритму шифрування RSA.

16. Реалізація алгоритму шифрування Ель-Гамаля.

17. Алгоритм шифрування на основі задачі про укладку портфеля.

18. Реалізація алгоритму шифрування на основі еліптичних кривих.

19. Реалізація основних хеш-функцій.

20. Реалізація хеш-функції. MD5.

21. Реалізація основних криптографічних протоколів.

22. Реалізація протоколів обміну ключами.

23. Реалізація протоколів аутентифікації.

24. Реалізація парольної ідентифікації/аутентифікації.

25. Реалізація протоколу ідентифікації/аутентифікації на основі шифрування з відкритим ключем.

26. Сервер аутентифікації Kerberos.

27. Ідентифікація/аутентифікація з допомогою біометричних даних.

28. Реалізація електронного цифрового підпису.

29. Реалізація ЕЦП на базі алгоритму RSA.

30. Реалізація ЕЦП на базі алгоритму DSA.

31. Реалізація алгоритму цифрового підпису ГОСТ 34.10-94.

32. Реалізація алгоритму цифрового підпису ГОСТ 34.10-2001.

Виконання КПІЗ є одним із обов’язкових складових модулів залікового кредиту.

7. Самостійна робота та дуальна освіта

№ п/п	Тематика
1	Основні загрози безпеки інформації та забезпечення її захисту.
2	Шифри скитала, Цезаря, частоколу.
3	Подання тексту у цифровій формі.
4	Блокові та потокові шифри. Багаторазове шифрування.
5	Афінні шифри.
6	Стійкість криптографічних алгоритмів.
7	Ймовірнісні алгоритми.
8	Оракульна модель.
9	Методи генерування простих чисел.
10	Псевдопрості числа.
11	Обчислення функції Ейлера.
12	Первісні корені за простим модулем.
13	Складність факторизації та дискретного логарифмування.
14	Система Шнорра.
15	Приклади перспективних ефективних алгоритмів блокового шифрування.
16	Перспективи застосування асиметричних алгоритмів для забезпечення

	інформаційної безпеки в комп'ютерних системах.
17	Аутентифікація в комп'ютерних системах.
18	Математичний формалізм у криптографії. Основна теорема арифметики.

8. Організація та проведення тренінгу з дисципліни «Криптографія»

№п/п	Вид роботи	Порядок проведення тренінгу
1	Огляд сучасних комп'ютерних систем шифрування інформації	− розгляд сучасних засобів проектування криптографічних алгоритмів; − вивчення можливостей проектування криптографічних алгоритмів в різних середовищах.
2	Розгляд процесу проектування системи для генерації електронного цифрового підпису	− постановка задачі; − опис технічного завдання; − проектування схеми для генерації електронного цифрового підпису
3	Розв'язування наскрізних задач, що охоплюють усі розділи дисципліни «Криптографія»	− опис наскрізної задачі; − розбиття задачі на окремі підзадачі; − об'єднання розв'язаних підзадач в єдине ціле з метою вирішення усієї задачі.

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Тематика тренінгу: Застосування симетричних та асиметричних криптосистем для захисту інформаційних потоків.

9. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; робота в Інтернет.

10. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни "Криптографія" використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумкове тестування за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– ректорська контрольна робота;
– комплексне практичне індивідуальне заняття (КПІЗ);
– підсумковий письмовий іспит.

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни “Криптографія” визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту

Семестр 5 – іспит

%

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4 (письмовий екзамен)
20%	20%	20%	40%
1. Усне опитування на лабораторних заняттях: 11 тем по 2 бали – max 22 балів. 2. Письмова робота – max 56 балів. 3. Практичне завдання: Захист 11 лабораторних робіт по 2 бали – max 22 балів.	1. Усне опитування на лабораторинх заняттях: 10 тем по 2 бали – max 20 балів. 2. Письмова робота – max 50 балів. 3. Практичне завдання: Захист 10 лабораторних робіт по 3 бали – max 30 бали.	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Виконання завдань на тренінгах – max 30 балів	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

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)

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

№	Найменування	Номер теми
1	Електронний варіант лекцій	1 -21
2	Методичні вказівки до виконання лабораторних робіт (електронний варіант)	1 - 21
3	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-21

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
2. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
3. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
4. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
5. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
6. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
7. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160/
8. Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
9. Асиметричні алгоритми шифрування у системі залишкових класів / Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138.
10. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
11. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
12. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків/ І.З. Якименко, Л.М. Тимошенко, М.М. Касянчук. Сучасна спеціальна техніка, №2, 2018. С.63-71.
13. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах/ М. М. Касянчук, М. П. Карпінський, С. В. Казмірчук. Захист інформації, №2, т.21, 2019. С.65-73.
14. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання/ М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко. Informatics & Mathematical Methods in Simulation, №11, 2021. С. 47-57.