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

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
"____"_____2023 р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
"____"_____2023 р.

ЗАТВЕРДЖУЮ
Директор навчально-наукового інституту новітніх освітніх технологій
_____ Святослав ПИТЕЛЬ
"____"_____2023 р.

РОБОЧА ПРОГРАМА

з дисципліни **«Програмно-апаратні засоби захисту інформації»**

ступінь вищої освіти – магістр
галузь знань – 12 "Інформаційні технології"
спеціальність – 123 "Комп'ютерна інженерія"
освітньо-професійна програма – „Комп'ютерна інженерія"

Кафедра комп'ютерної інженерії

Форма навчання	Курс	Семестр	Лекції (год.)	Практичні (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік сем.)	Екз. (сем.)
Денна	1	1	30	15	5	4	96	150	-	1
Заочна	1	1	8	4	-	-	138	150	-	2

31.08.2023

Тернопіль – ЗУНУ

2023

Робоча програма складена на основі освітньо – професійної програми підготовки магістра галузі знань 12 “Інформаційні технології” напряму підготовки 123 “Комп’ютерна інженерія”, затвердженої Вченою радою ЗУНУ (протокол № 10 від 23 червня 2023 р.).

Робочу програму склала к.т.н., доцент Леся ДУБЧАК

Робоча програма затверджена на засіданні кафедри комп’ютерної інженерії, протокол №1 від 28 серпня 2023 р.

Завідувач кафедри _____ Леся ДУБЧАК

Розглянуто та схвалено групою забезпечення спеціальності «Комп’ютерна інженерія», протокол №1 від 28 серпня 2023 р.

Голова ГЗС _____ Олег БЕРЕЗЬКИЙ

Гарант ОП «Комп’ютерна інженерія» _____ Григорій МЕЛЬНИК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. ОПИС ДИСЦИПЛІНИ "ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ"

Дисципліна – «Програмноапаратні засоби захисту інформації»	**Галузь знань, спеціальність, ступінь вищої освіти**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS: 5.	Галузь знань – 12 Інформаційні технології	Статус дисципліни – обов'язкова Мова навчання – українська
Кількість залікових модулів: 4	Спеціальність – 123 "Комп'ютерна інженерія"	**Рік підготовки:** *Денна* – 1 *Заочна – 1* **Семестр:** *Денна* – 1 *Заочна – 1*
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	**Лекції:** *Денна* – 30 *Заочна – 8* **Практичні заняття:** *Денна* – 15 *Заочна – 4*
Загальна кількість годин – 150 год.		**Самостійна робота:** *Денна* – 100 *Заочна – 138* **Індивідуальна робота** – 5 год.
Тижневих годин: денна форма навчання: 1 семестр: 10 год., з них аудиторних – 3 год.		Вид підсумкового контролю – екзамен

2. МЕТА Й ЗАВДАННЯ ВИВЧЕННЯ ДИСЦИПЛІНИ "ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ"

2.1. Мета вивчення дисципліни

Програма та тематичний план дисципліни орієнтовані на отримання студентами навиків та знань щодо захисту інформації в комп'ютерних системах.

2.2 Завдання вивчення дисципліни

Завданнями вивчення дисципліни «Програмно-апаратні засоби захисту інформації» є:

- ознайомлення студентів з сучасними криптографічними концепціями, з основами захисту інформації;
- формування цілісного уявлення про сучасні програмні та апаратні засоби захисту інформації;
- освоєння навичок вибору, розробки та використання засобів захисту інформації.

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

СК 6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів.

2.4 Передумови для вивчення дисципліни

Засвоєння знань за програмою вступного фахового випробування по спеціальності (додаткового вступного фахового випробування по спеціальності), цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи.

2.5. Результати навчання

В результаті вивчення дисципліни студенти повинні:

ПРН 2. Знаходити необхідні дані, аналізувати та оцінювати їх.

ПРН 4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.

ПРН 8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.

ПРН 9. Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.

ПРН 11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

3. ПРОГРАМА ДИСЦИПЛІНИ "ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ"

Змістовий модуль 1. Класичні та сучасні симетричні криптосистеми.

Тема 1. Задачі криптографії

1. Вступ. Задачі криптографії. 2. Основні поняття та положення комп'ютерної криптографії. 3. Принципи криптографічного захисту інформації. 4. Криптоаналітичні атаки, їх види. 5. Історія розвитку криптографії.

Література: 2, 6.

Тема 2. Історія розвитку засобів захисту інформації.

1.Біграмний шифр Плейфейра. 2. Подвійний квадрат Уїтстона. 3. Шифр чотирьох квадратів. 4. Шифр ADFGVX. 5. Шифр Гронсфельда. 6. Шифр Гронсфельда з ключовим словом. 7. Шифр Віженера. 8. Шифр Віженера з ключовим словом. 9. Роторні шифрувальні машини, Enigma. 10. Шифр одноразового блокноту.

Література: 1, 7.

Тема 3. Сучасні симетричні криптосистеми.

1. Структура алгоритму DES, його переваги та недоліки. 2. Операції алгоритму DES, функція шифрування алгоритму DES. 3. Генерація підключів алгоритму DES. 4. Режими роботи алгоритму DES. 5. Структура алгоритму IDEA, його переваги та недоліки. 6. Операції алгоритму IDEA. 7. Генерація підключів алгоритму IDEA. 8. Генерація підключів алгоритму IDEA.

Література: 3, 6.

Змістовий модуль 2. Сучасні асиметричні криптосистеми.

Тема 4. Арифметика асиметричних криптосистем, генерація ключів.

1. Основні поняття. 2. Алгоритм Евкліда, його наслідок, пошук оберненого елемента, китайська теорема про остачі. 3. Функція Ейлера. 4. Теореми Ейлера та Ферма.

Література: 2, 5.

Тема 5. Криптосистема RSA.

1. Опис криптосистеми RSA. 2. Генерування ключів. 3. Шифрування та дешфрування. 4. Коректність, ефективність та надійність криптосистеми.

Література: 4, 7.

Тема 6. Криптосистеми Рабіна та Ель–Гамаля.

1. Генерування ключів криптосистеми Рабіна. 2. Шифрування та дешифрування в криптосистемі Рабіна. 3. Коректність, ефективність та надійність криптосистеми. 4. Криптосистема Ель–Гамаля. 5. Шифрування та дешифрування в криптосистемі Ель–Гамаля. 6. Коректність, ефективність та надійність криптосистеми. Література: 2, 6.

Змістовий модуль 3. Сучасні криптографічні протоколи та методи криптоаналізу.

Тема 7. Алгоритми електронного цифрового підпису.

1. Поняття електронного цифрового підпису. 2. Електронний цифровий підпис в системах RSA та Ель–Гамаля. 3. Алгоритм DSA. 4. Система Шнорра. 5. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.

Література: 3, 6.

Тема 8. Криптографічні протоколи.

1. Поняття криптографічного протоколу. 2. Протоколи обміну ключем, жеребу по телефону, розподілу таємниці.

Література: 1, 7.

Тема 9. Класичні та сучасні методи криптоаналізу.

1. Поняття криптоаналізу. 2. Частотний аналіз. 3. Метод зустрічі посередині. 4. Метод «парадоксу днів народження». 5. Сучасні атаки на реалізацію та засоби захисту від них.

Література: 2, 6.

Тема 10. Засоби захисту фінансових даних

1.Internet-банкінг. 2.POS-термінали, банкомати. 3.Методи захисту фінансових даних.

Література: 2, 6.

Тема 11. Сучасні апаратні засоби захисту інформації

1.Засоби аутентифікації користувача. 2.Засоби протидії несанкціонованому доступу. 3.Засіб захисту інформації «Ельбрус».

Література: 2, 6.

Тема 12. Політика безпеки інформації. Законодавча база захисту інформації в Україні.

1.Політика безпеки. 2.Нормативно-правове та організаційне забезпечення безпеки. 3.Комунікаційно-технічне забезпечення. 4.Програмне забезпечення.

Література: 1, 2, 3.

4. СТРУКТУРА ЗАЛІКОВОГО КРЕДИТУ ДИСЦИПЛІНИ "ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ"

(денна форма навчання)

№	Т Е М А	Кількість годин				
		Лекції	Практичні заняття	Самостійна робота	Індивідуальні робота	Контрольні заходи
Змістовий модуль 1						
1.	Задачі криптографії	2	–	10		опитування
2.	Історія розвитку засобів захисту інформації.	2	2	10		опитування
3.	Сучасні симетричні криптосистеми.	2	3	10	1	опитування
4.	Арифметика асиметричних криптосистем, генерація ключів.	2	2	10		опитування
5.	Криптосистема RSA.	2	3	10	1	опитування
6.	Криптосистеми Рабіна та Ель–Гамаля.	2	2	10	1	опитування

7.	Алгоритми електронного цифрового підпису.	2	3	10	1	опитування
8.	Криптографічні протоколи.	2	–	15	1	опитування
9.	Класичні та сучасні методи криптоаналізу.	4	–	15		опитування
10.	Засоби захисту фінансових даних	2	-			опитування
Змістовий модуль 2						
11.	Сучасні апаратні засоби захисту інформації	4				опитування
12	Політика безпеки інформації. Законодавча база захисту інформації в Україні	4				опитування
Разом		30	15	10	5	

(заочна форма навчання)

№	Т Е М А	Кількість годин		
		Лекції	Практичні заняття	Самостійна робота
1.	Задачі криптографії	1	–	15
2.	Історія розвитку засобів захисту інформації.		-	15
3.	Сучасні симетричні криптосистеми.	1	2	14
4.	Арифметика асиметричних криптосистем, генерація ключів.	1	-	10
5.	Криптосистема RSA.	1	1	10

6.	Криптосистеми Рабіна та Ель–Гамаля.	1	-	10
7.	Алгоритми електронного цифрового підпису.	1	1	10
8.	Криптографічні протоколи.		–	10
9.	Класичні та сучасні методи криптоаналізу.	1	–	10
10.	Засоби захисту фінансових даних		-	10
11.	Сучасні апаратні засоби захисту інформації	1	-	14
12.	Політика безпеки інформації. Законодавча база захисту інформації в Україні.		-	10
	Разом	8	4	138

5. ТЕМАТИКА ПРАКТИЧНИХ РОБІТ

Практична робота №1.

Тема: Представлення тексту в цифровій формі. Шифр одноразового блокноту.

Мета: Вивчення методів представлення тексту в цифровій формі та реалізація шифру одноразового блокноту.

Питання для обговорення:

1. Способи представлення тексту
2. Найпростіші шифри
3. Шифр одноразового блокноту

Література: 2, 6.

Практична робота №2.

Тема: Стандарт шифрування даних DES.

Мета: Ознайомлення з симетричним алгоритмом шифрування даних DES, оволодіння методами його реалізації та аналізу.

Питання для обговорення:

1. Симетричні криптоалгоритми
2. Алгоритм DES
3. Шифрування тексту алгоритмом DES

Література: 2, 5.

Практична робота №3.

Тема: Афінні шифри.

Мета: Вивчення та аналіз афінних шифрів.

Питання для обговорення:

1. Алгоритм афінних шифрів
2. Основні характеристики афінних шифрів
3. Реалізація афінних шифрів

Література: 3, 7.

Практична робота №4.

Тема: Дослідження процедури шифрування та дешифрування в криптосистемі RSA.

Мета: Оволодіння методами для шифрування та дешифрування в криптосистемі RSA.

Питання для обговорення:

1. Асиметричні криптоалгоритми
2. Алгоритм шифрування RSA
3. Основні характеристики криптоалгоритму RSA Література: 2, 6.

Практична робота №5.

Тема: Дослідження особливостей цифрового електронного підпису Ель–Гамаля.

Мета: Вивчення та дослідження особливостей схеми шифрування Ель–Гамаля.

Питання для обговорення:

1. Цифровий електронний підпис та його застосування
2. Сучасні алгоритми ЕЦП
3. Цифровий електронний підпис Ель–Гамаля

Література: 3, 7.

Практична робота №6.

Тема: Дослідження апаратних засобів захисту від несанкціонованого доступу до інформації.

Мета: Вивчення та дослідження особливостей побудови політики бузпеки на основі апаратних засобів засобів захисті від несанкціонованого доступу до інформації.

Питання для обговорення:

1. Поняття політики безпеки
2. Сучасні апаратні та програмні засоби захисту інформації 3. Розробка політики безпеки для конкретних завдань

Література: 1, 4.

6. КОМПЛЕКСНЕ ПРАКТИЧНЕ ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Варіанти КПІЗ з дисципліни «Програмно-апаратні засоби захисту інформації»:

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.
7. Розробка і програмна реалізація алгоритму обчислення цифрового дайджеста повідомлення.
8. Програмна реалізація алгоритмів цифрового підпису.
9. Схема режиму шифрування DES-ECB.
10. Схема режиму шифрування DES-CBC.
11. Схема режиму шифрування DES-CPB и DES-OFB.
12. Потрійний DES. Сфери застосування різних режимів DES.
13. 14 Схема режиму шифрування простої заміни ГОСТ 28147-89.
14. Реалізація алгоритму шифрування RSA.
15. Реалізація алгоритму шифрування Ель-Гамаля.
16. Алгоритм шифрування на основі задачі про укладку портфеля.
17. Реалізація алгоритму шифрування на основі еліптичних кривих.
18. Реалізація основних хеш-функцій.
19. Реалізація хеш-функції. MD5.

20. Реалізація основних криптографічних протоколів.
21. Реалізація протоколів обміну ключами.
22. Реалізація протоколів аутентифікації.
23. Реалізація парольної ідентифікації/аутентифікації.
24. Реалізація протоколу ідентифікації/аутентифікації на основі шифрування з відкритим ключем.
25. Сервер аутентифікації Kerberos.
15. Ідентифікація/аутентифікація з допомогою біометричних даних.
16. Реалізація електронного цифрового підпису.
17. Реалізація ЕЦП на базі алгоритму RSA. 30. Реалізація ЕЦП на базі алгоритму DSA.

7. САМОСТІЙНА РОБОТА СТУДЕНТІВ

№ 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 захисту інформації
17	Аутентифікація в комп’ютерних системах
18	Математичний формалізм в криптографії

8. ТРЕНІНГ З ДИСЦИПЛІНИ «ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

№п/п	Вид роботи	Порядок проведення тренінгу	Кількість годин
1	Огляд сучасних програмних середовищ для вирішення задач комп'ютерної криптографії	− розгляд сучасних програмних середовищ для вирішення задач комп'ютерної криптографії; − вивчення можливостей сучасних програмних середовищ для вирішення задач комп'ютерної криптографії.	1
2	Розгляд процесу програмної реалізації криптографічних алгоритмів	− постановка задачі; − опис технічного завдання; − програмна реалізація криптографічних алгоритмів.	1
3	Розв'язування наскрізних задач, що охоплюють усі розділи дисципліни «Програмно-апаратні засоби захисту інформації»	− опис наскрізної задачі захисту інформації; − розбиття задачі на окремі підзадачі; − об'єднання розв'язаних підзадач в єдине ціле з метою вирішення усієї задачі.	2

9. ЗАСОБИ ОЦІНЮВАННЯ ТА МЕТОДИ ДЕМОНСТРУВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

У навчальному процесі застосовуються: лекції, в тому числі з використанням мультимедіапроектора та інших ТЗН; практичні заняття; індивідуальні заняття, самостійна робота студента, робота в Інтернет.

У процесі вивчення дисципліни "Програмно-апаратні засоби захисту інформації " використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточні опитування;
- залікове модульне тестування та опитування;
- наскрізні проекти;

- командні проекти;
- презентації результатів виконання завдань та досліджень;
- оцінювання результатів КПІЗ;
- студентські презентації та виступи на наукових заходах;
- ректорська контрольна робота;
- екзамен.

10. КРИТЕРІЇ, ФОРМИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

В процесі вивчення дисципліни "Програмно-апаратні засоби захисту інформації" використовуються наступні методи оцінювання навчальної роботи студента:

- поточне опитування;
- підсумкове тестування по кожному змістовому модулю;
- ректорська контрольна робота;
- комплексне практичне індивідуальне завдання (КПІЗ);
- письмовий екзамен.

Підсумковий бал (за 100-бальної шкалою) з дисципліни "Програмно-апаратні засоби захисту інформації" визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1	**Заліковий модуль 2**	**Заліковий модуль 3 (підсумкова оцінка за КПІЗ)**	**Заліковий модуль 4 (екзамен)**	**Разом**
20%	**20%**	**20%**	**40%**	**100%**
1. Усне опитування під час занять (6 тем по 5 балів = 30 балів) 2. Письмова робота = 70 балів	1. Усне опитування під час занять(6 тем по 5 балів = 30 балів) 2. Письмова робота = 70 балів	1. Написання та захист КПІЗ = 80 балів 2. Виконання завдань під час тренінгу = 20 балів	1. Тестові завдання = 50 балів 2. Практичне завдання = 50 балів	

Шкала оцінювання:

За шкалою університету	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)

11. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

№	Найменування	Номер теми
1.	Операційні системи Linux, Windows	10, 12
2.	Microsoft Word	1-12
3.	Internet Browser Firefox	1-12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1.Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко,В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.

2. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Проведення робіт.

4.Закон України «Про державну таємницю» від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93.

5.Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

6. Закон України «Про інформацію» // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651.

7.Остапов С.Е. Кібербезпека: сучасні технології захисту / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. – К.:.Новий світ-2000, 2020. – 678 с. 17. Хорошко В. О. Проєктування комплексних систем захисту інформації./ В.О. Хорошко. – Львів: Видавництво Львівської політехніки, 2020. – 317 с.