


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

ЗАТВЕРДЖУЮ

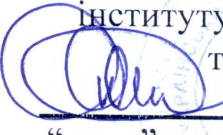
Декан факультету комп'ютерних
 інформаційних технологій

 Ігор ЯКИМЕНКО
 “ ” 2024 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної
 роботи

 Віктор ОСТРОВЕРХОВ
 “ ” 2024 р.

ЗАТВЕРДЖУЮ

Директор навчально-наукового
 інституту новітніх освітніх
 технологій

 Святослав ПИТЕЛЬ
 “ ” 2024 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.)	Екз. (сем.)
Денна	1	1	32	14	5	6	93	150	1
Заочна	1	1	8	4	-	-	138	150	2

30.08.2024


Тернопіль – ЗУНУ

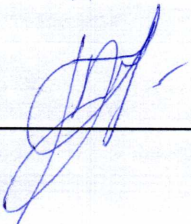
2024

Робочу програму склала к.т.н., доцент

Леся ДУБЧАК

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії,
протокол №2 від 30 вересня 2024р.

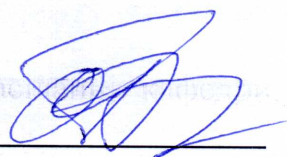
Завідувач кафедри



Леся ДУБЧАК

Розглянуто та схвалено групою забезпечення спеціальності «Комп'ютерна
інженерія», протокол №2 від 30 вересня 2024 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: <i>Денна – 1</i> <i>Заочна – 1</i> Семестр: <i>Денна – 1</i> <i>Заочна – 1</i>
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції: <i>Денна – 32</i> <i>Заочна – 8</i> Практичні заняття: <i>Денна – 14</i> <i>Заочна – 4</i>
Загальна кількість годин – 150 год.		Самостійна робота: <i>Денна – 93</i> <i>Заочна – 138</i> 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.

ПРН12. Вільно спілкуватись усно і письмово українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською) при обговоренні професійних питань, досліджень та інновацій в галузі інформаційних технологій.

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.

Література: 2, 6.

Тема 2. Історія розвитку засобів захисту інформації.

1. Шифр чотирьох квадратів. 2. Шифр ADFGVX. 3. Шифр Віженера. 4. Роторні шифрувальні машини, Епігма. 5. Шифр одноразового блокноту.

Література: 1, 7.

Тема 3. Сучасні симетричні криптосистеми.

1. Структура алгоритму DES, його переваги та недоліки. 2. Генерація підключів алгоритму DES. 3. Режими роботи алгоритму DES. 4. Структура алгоритму IDEA, його переваги та недоліки.

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. Теорема Ейлера та Ферма.

Література: 2, 5.

Тема 5. Криптосистема RSA.

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

Література: 4, 7.

Тема 6. Криптосистеми Рабіна та Ель–Гамалія.

1. Генерування ключів криптосистеми Рабіна. 2. Шифрування та дешифрування в криптосистемі Рабіна. 3. Криптосистема Ель–Гамалія. 4. Шифрування та дешифрування в криптосистемі Ель–Гамалія. 5. 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–Гамалія. 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. 3. Протокол жеребу по телефону. 4. Протокол 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. 3. Захист конфіденційних даних при користуванні банкоматами. 4. Методи захисту фінансових даних.

Література: 2, 6.

Тема 11. Сучасні апаратні засоби захисту інформації

1.Засоби аутентифікації користувача. 2.Засоби протидії несанкціонованому доступу. 3.Сучасні засоби захисту інформації.

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 роботи	Тренінг	Контрольні заходи
Змістовий модуль 1							
1.	Задачі криптографії	2	2	10	4	3	опитування
2.	Історія розвитку засобів захисту інформації.	2	2	10			опитування
3.	Сучасні симетричні криптосистеми.	2	2	10			опитування
4.	Арифметика асиметричних криптосистем, генерація ключів.	2	2	10			опитування
5.	Криптосистема RSA.	2	2	10			опитування

6.	Криптосистем и Рабіна та Ель– Гамалія.	2	2	10			опитування
7.	Алгоритми електронного цифрового підпису.	2	2	10			опитування
8.	Криптографіч ні протоколи.	2	–	10		1	опитування
9.	Класичні та сучасні методи криптоаналіз у.	4	–	5			опитування
10	Засоби захисту фінансових даних	4	-	5			опитування
Змістовий модуль 2							
11	Сучасні апаратні засоби захисту інформації	4		2	1	2	опитування
12	Політика безпеки інформації. Законодавча база захисту інформації в Україні	4		1			Опитуванн я
Разом		32	14	93	5	6	

(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–Гамалія.	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–Гамалія.

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

Питання для обговорення:

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

Література: 3, 7.

Практична робота №6.

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

Мета: Вивчення та дослідження особливостей побудови політики безпеки на основі апаратних засобів захисту 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 ТРЕНІНГ З ДИСЦИПЛІНИ «ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

№п/п	Вид роботи	Порядок проведення тренінгу
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.
2	Розгляд процесу програмної реалізації криптографічних алгоритмів	– постановка задачі; – опис технічного завдання; – програмна реалізація криптографічних алгоритмів.
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.

7. САМОСТІЙНА РОБОТА СТУДЕНТІВ

№ п/п	Тематика	Завдання
1	Основні загрози безпеки інформації та забезпечення її захисту.	Дослідити можливості застосування старих криптоалгоритмів для сучасного захисту інформації.
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.	Дослідження блокових шифрів
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	Застосування сучасних криптосистем для захисту інформації
17	Аутентифікація в комп'ютерних системах	
18	Математичний формалізм в криптографії	

8. КРИТЕРІЇ, ФОРМИ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

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

- поточне тестування та опитування;
- підсумкове тестування по кожному змістовому модулю;
- підсумкова оцінка за виконання завдань тренінгу;
- оцінювання наскрізного проекту у результаті самостійної роботи;
- підсумковий екзамен.

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

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20 %	20 %	5 %	15 %	40%
Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота	Екзамен
Середнє арифметичне за 6 практичних занять	Тестові завдання	Виконання 3 завдань	Виконання наскрізного проекту із 3 завдань	2 теоретичних питання 2 по 25 балів = 50 балів, Задача = 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)

9. 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. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації.

Основні положення.

2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації.

Проведення робіт.

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

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

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

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

7. Massimo Bertaccini, Cryptography Algorithms: A guide to algorithms in blockchain, quantum cryptography, zero-knowledge protocols, and homomorphic encryption , Packt Publishing, 2022. – 325 p.