ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
“УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”
ІНЖЕНЕРНО-ТЕХНІЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА КОМП’ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

ЗАТВЕРДЖУЮ
Декан інженерно-технічного
факультету
_____ доц. Йолана ГОЛИК
“___” _____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМП’ЮТЕРНА КРИПТОГРАФІЯ

Рівень вищої освіти – другий (магістр)
Галузь знань – F – інформаційні технології
Спеціальність – F7 – комп’ютерна інженерія
Освітня програма – «комп’ютерні системи та мережі»
Статус дисципліни – обов’язкова
Мова навчання – українська

Ужгород – 2025

Робоча програма навчальної дисципліни «Комп'ютерна криптографія» для здобувачів спеціальності F7– «Комп’ютерна інженерія» освітньої програми «Комп’ютерні системи та мережі» – 12 с.

Розробники: Гапак О.М., доцент кафедри комп’ютерних систем та мереж, канд. пед. наук, доцент.

Робочу програму розглянуто та затверджено на засіданні кафедри комп’ютерних систем та мереж

протокол № 13 від «25» червня 2025 р.

Завідувач кафедри _____ доц. Петро ГОРВАТ
(підпис) (прізвище та ініціали)

Схвалено науково-методичною комісією інженерно-технічного факультету

протокол № 6 від «27» червня 2025 р.

Голова науково-методичної комісії _____ доц. Володимир ЦИГИКА
(підпис) (прізвище та ініціали)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td>Розподіл годин за навчальним планом</td></tr>
<tr><td>денна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС – 4</td><td>Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин – 120</td><td>1-й</td></tr>
<tr><td rowspan="2">Кількість модулів – 2</td><td>Семестр</td></tr>
<tr><td>1-й</td></tr>
<tr><td rowspan="4">Тижневих годин для денної форми навчання:
аудиторних – 2,7 години</td><td>Лекції</td></tr>
<tr><td>30 год</td></tr>
<tr><td>Практичні (семінарські)</td></tr>
<tr><td>-</td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: екзамен</td><td>Лабораторні</td></tr>
<tr><td>18 год</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td>Самостійна робота</td></tr>
<tr><td>72 год</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Комп'ютерна криптографія» є ознайомлення студентів із основами криптоаналізу та криптографічними протоколами.

Завдання дисципліни – сформувати погляд на захист інформації і криптографію як на систематичну науково-практичну діяльність, що носить прикладний характер. Сформувати базисні теоретичні поняття та практичні навички щодо проведення криптоаналізу класичних шифрів, блочних шифрів, асиметричних криптосистем та організацію криптографічних протоколів.

У результаті вивчення дисципліни студент повинен знати: основні види симетричних та асиметричних криптоалгоритмів, основні методи криптоаналізу та види протоколів; вміти: застосовувати математичні методи описання і дослідження криптосистем; аналізувати криптосистеми, оцінювати їх стійкість, вміло застосовувати основні методи криптоаналізу.

Відповідно до освітньої програми «Комп’ютерні системи та мережі», вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

- інтегральна (здатність розв’язувати складні задачі і проблеми у певній галузі професійної діяльності або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог);
- загальні (ЗК1-здатність до адаптації та дій в новій ситуації, ЗК2-здатність до абстрактного мислення, аналізу і синтезу; ЗК4-здатність до пошуку, оброблення та аналізу інформації з різних джерел; ЗК5- здатність генерувати нові ідеї (креативність); ЗК7-здатність приймати обґрунтовані рішення);
- фахові (СК1-здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп’ютерних систем та мереж різного призначення; СК2 - здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем та мереж, інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування; СК3-здатність проектувати комп’ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів; СК4-здатність будувати та досліджувати моделі комп’ютерних систем та мереж; СК8 - здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу; СК11- здатність обирати ефективні методи розв’язування складних задач комп’ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення).

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Вивчення даної дисципліни базується на знанні студентами курсу (ОК14) «Програмування», (ОК18) «Теорія інформації і кодування», (ОК11) «Теорія ймовірності і математична статистика», (ОК31) «Захист інформації в комп’ютерних системах».

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми «Комп’ютерні системи та мережі», вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

Програмні результати навчання	Шифр ПРН
Застосовувати загальні підходи пізнання, методи математики, природничих та інженерних наук до розв’язання складних задач комп’ютерної інженерії	ПРН1
Знаходити необхідні дані, аналізувати та оцінювати їх	ПРН2

Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.	ПРН6
Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем	ПРН9
Здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії, аналізувати та оцінювати цю інформацію	ПРН10

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни

Очікувані результати навчання з дисципліни	Шифр ПРН
Розуміння наукових та математичних положень та основних нормативних положень, що лежать у основі організації засобів захисту комп'ютерних систем та мереж, в тому числі-криптографії. Вміння застосовувати математичні методи описання і дослідження криптосистем; оцінювати криптографічну стійкість шифрів; проведення експериментів, збирання даних та моделювання в комп'ютерних системах.	ПРН1, ПРН2
Знання сучасних методів криптоаналізу та побудови крипто протоколів. Застосування новітніх технологій у криптології.	ПРН6, ПН9
Вміння системно мислити та застосовувати творчі здібності до формування нових ідей щодо нових методів у криптографії	ПРН10

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Робоча програма з дисципліни «Комп'ютерна криптографія», що вивчається на першому курсі магістратури за спеціальністю «Комп'ютерна інженерія» містить один модуль, що складається з двох змістових модулів ЗМ1 (Т1-Т5) ЗМ2 (Т1- Т5). Використовуються методи усного контролю та письмового контролю. Поточний контроль передбачає: опитування студентів під час захисту лабораторних робіт та опитування на лекціях; контрольні роботи, індивідуальні, самостійні завдання. Підсумковий контроль передбачає залік.

Оцінка ECTS, яку студент отримує після вивчення кредитного модуля дисципліни, визначається відповідно до рейтингу студента. Рейтинг студента з кредитного модуля складається з балів, що він отримує протягом семестру за такі види робіт:

1. Модульна контрольна робота (МКР) тривалістю по 2 акад. години. Максимальна кількість балів за МКР – 40 балів.

2. Виконання лабораторних робіт.

Протягом семестру студенти виконують 5 лабораторних робіт, де максимальна кількість балів – 50 за модуль.

Бали із індивідуальної та самостійної роботи студентів нараховуються за: підготовку рефератів, модернізацію завдань, за творчий підхід до виконання завдань, виконання завдань із удосконалення дидактичних матеріалів з дисципліни: 0-10 балів за кожен модуль.

Сума вагових балів контрольних заходів протягом семестру: 100 балів.

Необхідною умовою допуску до іспиту є відсутність заборгованостей з лабораторних робіт та зарахування контрольних робіт.

Розподіл балів, які отримують студенти за 1 модуль

Поточне опитування (лабораторні роботи)					Самостійна робота	Письмова контрольна робота	Сума
Змістовий модуль 1							
Т1	Т2	Т3	Т4	Т5			
10	10	10	10	10	10	40	100

Розподіл балів, які отримують студенти за 2 модуль

Поточне опитування (лабораторні роботи)					Самостійна робота	Письмова контрольна робота	Сума
Змістовий модуль 1							
Т1	Т2	Т3	Т4	Т5			
10	10	10	10	10	10	40	100

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1	
	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (виконання та захист)	5	50
Самостійна робота	1	10
Модульна контрольна робота	1	40
Разом		100

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота може проводитись у двох режимах:

- Письмова, яка містить шість завдань. Перші три завдання включають теоретичний і практичний матеріал, наступні 3 завдання – це тести.
- Тестова, що містить 50 тестів із вибором однієї правильної відповіді.

Критерії оцінювання підсумкового семестрового контролю

До складання заліку допускаються лише студенти, які мають рейтинговий бал не менше 35. Залік з навчальної дисципліни студент може не складати, якщо він склав усі модулі та його влаштовує рейтингова оцінка. Студенти, які мають рейтинговий бал від 35 до 59 залік складають обов'язково. Студент може підвищити на заліку оцінку, при цьому рейтингова оцінка не може бути зменшена.

За результатами виконання студентом навчальної програми впродовж семестру рекомендується виставляти заліки та екзамени без додаткового опитування за такою шкалою:

Сумарні бали	Оцінка ECTS	Екзамен (диф.залік)	Залік
90 – 100	A	Відмінно	Зараховано
82 – 89	B	Добре	
74 – 81	C		
64 – 73	D	Задовільно	
60 – 63	E		
35 – 59	FX	Незадовільно з можливістю повторного складання	Незараховано з можливістю повторного складання
1 – 34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Незараховано з обов'язковим повторним вивченням дисципліни

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1

Змістовий модуль 1. Криптоаналіз.

Тема 1. Криптоаналіз: сучасний стан і перспективи розвитку. Основні поняття криптоаналізу, принципи криптоаналізу, класифікація атак, стійкість криптоалгоритма. Універсальні методи криптоаналізу.

Тема 2. Криптоаналіз класичних шифрів. Криптоаналіз: шифру стовпцевої перестановки, шифру простої заміни, шифру Цезаря, шифру Віжінера.

Тема 3. Лінійний та диференціальний криптоаналіз. Лінійний та диференціальний криптоаналіз блочних симетричних криптосистем.

Тема 4. Криптоаналіз потокових шифрів.

Тема 5. Криптоаналіз асиметричних систем, хеш-функцій.

Тема 6. Криптоаналіз за побічними каналами та використання нових технологій у криптоаналізі.

Модуль 2

Змістовий модуль 2. Криптографічні протоколи.

Тема 1. Основні поняття криптографічного протоколу. Класифікація протоколів. Використання симетричних та асиметричних систем для побудови криптографічних протоколів. Приклади протоколів.

Тема 2. Схеми цифрового підпису. Спеціальні види електронного підпису: сліпий підпис, невидимий підпис.

Тема 3. Протоколи аутентифікації. Схема Шнорра.

Тема 4. Протоколи розподілу ключів. Порогова схема. Схема обчислення ключа доступу. Схема Блеклі. Схема Шаміра та інші.

Змістовий модуль 3. Сучасні технології інформаційної безпеки

Тема 1. Гомоморфне шифрування та його застосування; блокчейн у кібербезпеці; квантова криптографія.

Тема 2. Тестування на проникнення та етичний хакинг. Види тестувань безпеки (black-box, white-box, grey-box). Використання Kali Linux та Metasploit. Аналіз вразливостей веб-додатків (OWASP Top 10).

Тема 3. Фінансова криптографія. Протоколи електронний платежів і цифрових грошей. Типи протоколів. Електронні платіжні системи України.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
1	2	3	4	5	6	7
Модуль 1						
Змістовий модуль 1. Криптоаналіз.						
Тема 1. . Криптоаналіз: сучасний стан і перспективи розвитку	6	2				4
Тема 2. Криптоаналіз класичних шифрів	14	4		6		4
Тема 3. Лінійний та диференціальний криптоаналіз	12	4		4		4
Тема 4. Криптоаналіз потокових шифрів.	10	2		4		4
Тема 5. Криптоаналіз асиметричних систем, хеш-функцій.	10	2		4		4
Тема 6. Криптоаналіз за побічними каналами та використання нових технологій у криптоаналізі	6	2				4
Разом за змістовим модулем 1	58	16		18		24
Модуль 2						
Змістовий модуль 2. Криптографічні протоколи. Фінансова криптографія.						
Тема 1. Основні поняття криптографічного протоколу	8	2				6
Тема 2. Схеми цифрового підпису.	8	2				6
Тема 3 . Протоколи аутентифікації	8	2				6
Тема 4 . Протоколи розподілу ключів.	8	2				6
Разом за змістовим модулем 2	32	8				24
Змістовий модуль 3. Сучасні технології інформаційної безпеки						
Тема 1 Гомоморфне шифрування, блокчейн у кібербезпеці; квантова криптографія	10	2				8
Тема 2. Тестування на проникнення та етичний хакинг	10	2				8
Тема 3 . Фінансова криптографія	10	2				8

Разом за змістовим модулем 3	30	6				24
Разом за модулем 2	62	14				48
Разом	120	30		18		72

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
	Модуль 1	
1	Криптоаналіз шифрів перестановки	2
2	Криптоаналіз шифру простої заміни	4
3	Криптоаналіз шифру Цезаря	2
4	Криптоаналіз шифру Віжінера	6
5	Засоби криптоаналізу у криптологічному пакеті CrypTool: криптоаналіз потокових шифрів, хеш-функцій, лінійний та диференціальний криптоаналіз блокових шифрів	4
	Разом за модуль	18

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Умови та особливості здійснення криптоаналізу.	5
2	Сутність та вразливості симетричних крипто перетворень.	5
3	Аналіз уразливостей блокових шифрів.	5
4	Порівняльний аналіз методів криптоаналізу симетричних шифрів.	5
5	Вимоги до криптостійкості блокових шифрів.	5
6	Приклади протоколів симетричних та асиметричних криптосистем.	5
7	Протоколи ідентифікації на основі самосертифікуючих ключів.	5
8	Протоколи генерування та передачі ключів симетричних криптосистем.	5
9	Протоколи відкритого розподілу ключів та їх вразливості.	5
10	Приклади прикладних протоколів.	5
11	Гомоморфне шифрування,;	5
12	Блокчейн у кібербезпеці	5
13	Квантова криптографія	5
14	Тестування на проникнення та етичний хакинг	7
	Разом	72

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

Використовуються традиційні методи навчання: лекції, лабораторні заняття, самостійна та індивідуальна робота студентів, консультації.

Лабораторні роботи виконуються на персональних комп'ютерах із встановленою операційною системою Windows, Linux. Програмне забезпечення: пакет Microsoft Office або LibreOffice, OpenOffice.org і т.д. Середовище програмування C#, криптологічний пакет CrypTool.

8. РЕКОМЕНДОВАНІ ЛІТЕРАТУРНІ ДЖЕРЕЛА

Основна література

1. Гапак О.М. Основи криптоаналізу. Криптографічні протоколи: навчальний посібник для студентів напряму підготовки «комп'ютерна інженерія». – Ужгород: «АУТДОР-ШАРК», 2021. – 120 с.
2. Гапак О.М. Методичні вказівки і завдання до лабораторних робіт з курсу «Комп'ютерна криптографія» для студентів спеціальності «комп'ютерна інженерія». – Ужгород: «АУТДОР-ШАРК», 2021. – 59 с.
3. Загацька Н.О. Огляд різних версій пакета Cryptool як засобу захисту інформаційних ресурсів/ Н.О. Загацька // Інформаційні технології і засоби навчання. 2012. №5 (31). [Електронний ресурс]. — Режим доступу до журналу: http://www.journal.iitta.gov.ua.
4. Остапов С. Е., Валь Л.О. Основи криптографії: навчальний посібник. Чернівці: Книги–XXI, 2008. – 188 с.

Інформаційні ресурси в мережі Інтернет

1. CrypTool-Online [Електронний ресурс]. — Режим доступу : http://www.cryptool-online.org.

Додаток 1

Перелік питань до модульного контролю
ЗМ1

1. Криптоаналіз. Основні принципи криптоаналіз.
2. Класифікація атак у криптоаналізі
3. Класифікація стійкості криптоалгоритмів
4. Універсальні методи криптоаналізу: Метод повного перебору ключа, частотний аналіз, безключове читання у колонках, метод «зустрічі посередині»» та інші.
5. Частотний криптоаналіз.
6. Первинний аналіз шифровки.
7. Криптоаналіз шифрів за методом перестановок.
8. Криптоаналіз шифрів стовпцевої перестановки.
9. Криптоаналіз шифрів за методом простої заміни.
10. Криптоаналіз шифру Цезаря.
11. Криптоаналіз шифру Віжінера.
12. Визначення довжини ключа у шифрі Віжінера.
13. Дешифрування за методом гамування.
14. Лінійний та диференціальний криптоаналіз блочних симетричних криптосистем.
15. Криптоналіз потокових шифрів.
16. Розкриття шифрів блокових алгоритмів.
17. Криптоаналіз систем з відкритим ключем.
18. Атаки на криптосистему шифрування RSA.
19. Атаки на ЕЦП RSA.
20. Використання нових технологій в криптоаналізі.
21. Нейронні мережі.
22. Генетичні алгоритми.
23. Квантові комп’ютери у криптографії.
24. Криптоаналіз за побічними каналами.
25. Атака за часом.
26. Атака за продуктивністю.
27. Атака за помилками обчислень.

ЗМ2

1. Поняття криптографічного протоколу. Специфіка взаємодії віддалених абонентів.
2. Підходи до класифікації криптографічних протоколів
3. Підходи до моделювання криптографічних протоколів
4. Приклади криптографічних протоколів.
5. Інтерактивна система доведення
6. Протоколи аутентифікації. Протокол ідентифікації Шнорра і його зв'язок з цифровою підписом.
7. Використання симетричних і асиметричних шифросистем для побудови криптографічних протоколів. Приклади.
8. Захищені обчислення. Приховування інформації від оракула. Задача про двох мільйонерах.

9. Протокол підкидання монети по телефону.
10. Спеціальні види електронного підпису: сліпий та невидимий.
11. Поділ секрету. Порогова схема поділу секрету.
12. Схема обчислення ключа доступу.
13. Протокол Шаміра і його властивості. Схема Блеклі.
14. Метод « розшаровування » зображення.
15. Протокол поділу секрету, що перевіряється.
16. Протокол поділу секрету, що перевіряється за схемою Шаміра.
17. Груповий протокол розподілу ключів для телеконференції.
18. Протоколи конфіденційного обчислення.
19. Передача ключів з використанням систем з відкритими ключами.
20. Протокол відкритого розподілу ключів Діффі - Хеллмана і його властивості.
21. .Протокол відкритого розподілу ключів на основі самосертифікуючих ключів, що залежать від ідентифікаторів.
22. Протокол відкритого розподілу ключів KEA.
23. Протокол відкритого розподілу ключів STS. Приклад атаки.
24. Попередній розподіл ключів.
25. Схема попереднього розподілу ключів Блома і її стійкість до компрометації і оптимальність.
26. Схеми попереднього розподілу ключів на основі перетину множин. Спосіб побудови.
27. Фінансова криптографія.
28. Задача криптографів, які вечеряють.
29. Електронні гроші. Протоколи електронних платежів.
30. Автономні системи електронних платежів.
31. Протокол ідентифікації Фіата-Шаміра і його зв'язок з цифровим підписом.
32. Протокол ідентифікації Окамото і його безпека.
33. Протокол Guillou-ідентифікації Quisquater і його безпека.
34. Протокол ідентифікації на основі самосертифікуючих відкритих ключів, що залежать від ідентифікаторів.
35. Протокол розподілу ключів NSPK і його вразливість.
36. Протоколи аутентифікації і розподілу ключів Kerberos V5 та KriptoKnight.
37. Протокол розподілу ключів EKE з використанням пароля.
38. Протокол аутентифікації / SPX розподілу ключів.
39. Сертіфікати відкритих ключів і протоколи їх видачі.
40. Протокол відкритого розподілу ключів MTI. Приклад атаки.