ЗАТВЕРДЖЕНО
Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 23 «ПРИКЛАДНА КРИПТОЛОГІЯ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека та захист інформаційя»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної інженерії та
кібербезпеки
28 серпня 2023 р., протокол № 7
Завідувач кафедри
_____ Андрій ЄФІМЕНКО
Гарант освітньо-
професійної програми
_____ Андрій ЄФІМЕНКО

Розробник: старший викладач кафедри комп'ютерної інженерії та кібербезпеки
Покотило Олександра Андріївна

Житомир
2025-2026 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітній ступінь	Характеристика навчальноїдисципліни
		денна формanавчання
Кількість кредитів – 4	Галузь знань 12 «Інформаційні технології»	Нормативна
Модулів – 1	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки:
Змістових модулів – 2		3-й
Загальна кількість годин –120		Семестр
		5-й
		Лекції
Тижневих годин для денної форми навчання: аудиторних – 5, самостійної роботи – 2,5	Освітній ступінь «бакалавр»	32 год.
		Практичні
		–
		Лабораторні
		48 год.
		Самостійна робота
		40 год.
		Вид контролю: екзамен

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 67 % аудиторних занять, 33 % самостійної таіндивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є вивчення принципів, методів, засобів побудови класичних та сучасних алгоритмів шифрування та методів їх зламу; формування та набуття професійних та предметних компетентностей, практичних знань та вмінь з криптографічного захисту інформаційних ресурсів та криптографічного аналізу.

Завданнями вивчення навчальної дисципліни є:

– забезпечення ґрунтовного оволодіння студентами основними поняттями, методами та алгоритмами криптології;

– формування у студентів предметних та професійних компетентностей, знань та вмінь з теорії та практики криптографічного захисту даних та криптографічного аналізу.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації» та освітньо-професійної програми «Кібербезпека»:

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК5. Здатність до пошуку, оброблення та аналізу інформації.

КФ2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів навчання** за спеціальністю 125 «Кібербезпека та захист інформації» та освітньо-професійної програмою «Кібербезпека»:

РН14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

РН17. 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.

РН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

РН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

РН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

3. Програма навчальної дисципліни

Змістовий модуль 1. Криптосистеми із закритим ключемТема 1. Основні поняття криптології

Загальні відомості про захист інформації в інформаційно-телекомунікаційних системах. Історія розвитку криптології. Цілі, завдання та принципи криптології. Основні поняття та визначення. Класифікація криптографічних систем.

Тема 2. Класичні шифри та їх криптоаналіз

Моноалфавітні шифри простої заміни (підстановки), афінні шифри заміни (підстановки). Шифри перестановки. Поліграмні шифри. Поліалфавітнікриптосистеми. Методи криптоаналізу класичних шифрів.

Тема 3. Криптографічна стійкість шифрів

Поняття криптографічної стійкості. Теоретична та практична стійкість шифрів. Розсіювання та перемішування. Типи атак на криптосистеми. Абсолютно стійкий шифр.

Тема 4. Потокові симетричні шифри

Основні властивості алгоритмів потокового симетричного шифрування даних. Класифікація потокових алгоритмів. Генератори псевдовипадкових послідовностей. Потоковий шифри RC4.

Тема 5. Алгоритм блокового симетричного шифрування DES

Основні властивості алгоритмів блокового симетричного шифрування даних. Мережа Фейстеля. Стандарт блокового симетричного шифрування DES. Безпека DES. Модифікації DES.

Тема 6. Режими шифрування блоків. Шифр IDEA

Режими роботи блокових шифрів: режим простої заміни, режим зв’язування блоків, режим зі зворотнім зв’язком по шифротексту, режим зі зворотнім зв’язком по виходу, режим лічильника. Міжнародний стандарт шифрування IDEA. Порівняльний аналіз DES та IDEA.

Тема 7. Удосконалений стандарт шифрування AES

Математична база алгоритму шифрування даних AES: додавання та множення байтів у полі Галуа. Основні операції при зашифруванні та дешифруванні за алгоритмом AES. Формування раундових ключів.

Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)

Етапи шифрування даних за алгоритмом «Калина». Формування допоміжного ключа та раундових (циклових) ключів шифрування. Режими роботи криптографічного алгоритму «Калина». Порівняльний аналіз AES та «Калина».

Змістовий модуль 2. Криптосистеми з відкритим ключем

Тема 9. Основні положення криптографії з відкритим ключем

Ідея криптосистеми з відкритим ключем. Поняття односторонньої функції. Математичні основи асиметричних шифрів. Алгоритм рюкзака (криптосистема Меркла-Хелмана). Порівняльний аналіз симетричних та асиметричних алгоритмів.

Тема 10. Асиметричні криптосистеми

Алгоритм RSA. Проблема розкладання на множники великих чисел. Алгоритм Ель-Гамаля. Алгоритм обміну ключами Діффі-Хелмана. Проблема дискретного логарифмування.

Тема 11. Криптографічні хеш-функції

Поняття хеш-функції та їх основні властивості. Область застосування хеш-функцій. Хеш-функція SHA-256. Хеш-функція «Купина» (ДСТУ 7564:2014).Інші хеш-функції.

Тема 12. Цифровий підпис

Принципи забезпечення автентичності даних з використанням цифрового підпису (ЦП). Процедури підписування та перевірки ЦП. Схеми цифровогопідпису RSA та Ель-Гамаля. Стандарт цифрового підпису DSS.

Тема 13. Криптографічні протоколи

Криптографічні протоколи управління ключами. Криптографічні протоколи автентифікації. Механізми розподілення таємниці. Синтез та аналіз криптографічних протоколів.

Тема 14. Основи криптографії на еліптичних кривих

Математичний опис криптографічних еліптичних кривих. Основні операції в групах точок еліптичних кривих. Алгоритм обміну ключами ECDH. Стандарт цифрового підпису ECDSS.

Тема 15. Елементи криптоаналізу сучасних шифрів

Завдання та принципи криптоаналізу. Диференціальний криптоаналіз.

Лінійний криптоаналіз. Інші методи криптоаналізу.

Тема 16. Нові напрямки в криптографії

Основи квантового шифрування. Технологія «блокчейн». Програмні засоби криптографічного захисту даних.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин			
	денна форма			
	усього	лекції	лабораторні	самостійна робота
Модуль 1				
Змістовий модуль 1. Криптосистеми із закритим ключем				
Тема 1. Основні поняття криптології	6	2	2	2
Тема 2. Класичні шифри та їх криптоаналіз	6	2	2	2
Тема 3. Криптографічна стійкість шифрів	6	2	2	2
Тема 4. Потокові симетричні шифри	6	2	2	2
Тема 5. Алгоритм блокового симетричногошифрування DES	10	2	4	4
Тема 6. Режими шифрування блоків. ШифрIDEA	8	2	4	2
Тема 7. Удосконалений стандарт шифруванняAES	10	2	4	4
Тема 8. Національний стандарт шифруванняДСТУ 7624:2014 («Калина»)	8	2	4	2
Разом за змістовий модуль 1	60	16	24	20
Змістовий модуль 2. Криптосистеми з відкритим ключем				
Тема 9. Основні положення криптографії звідкритим ключем	6	2	2	2
Тема 10. Асиметричні криптосистеми	10	2	4	4
Тема 11. Криптографічні хеш-функції	6	2	2	2
Тема 12. Цифровий підпис	6	2	2	2
Тема 13. Криптографічні протоколи	6	2	2	2
Тема 14. Основи криптографії на еліптичнихкривих	10	2	4	4
Тема 15. Елементи криптоаналізу сучаснихшифрів	8	2	4	2
Тема 16. Нові напрямки в криптографії	8	2	4	2
Разом за змістовий модуль 2	60	16	24	20
ВСЬОГО	120	32	48	40

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		денна форма
1	Математичні основи криптографії	4
2	Класичний шифр простої заміни та його криптоаналіз. Біграмний шифр	4
3	Класичний шифр поліалфавітної заміни та його криптоаналіз. Криптосистема Хілла	4
4	Дослідження властивостей потокових шифрів RC4, STRUMOK	4
5	Моделювання процесів шифрування за допомогою шифруодноразового блокноту. Алгоритм DES	4
6	Дослідження властивостей блокового симетричного шифру AES	4
7	Дослідження основних операцій шифру «Калина» у процесіформування допоміжного ключа	4
8	Асиметричні шифри RSA та Ель-Гамаля. Алгоритм обміну ключами Діффі-Хелмана	4
9	Хеш-функції SHA-256, Whirlpool	4
10	Цифровий підпис	4
11	Криптографічні перетворення в групах точок еліптичних кривих	4
12	Приховування даних в просторовій області нерухомих зображень методом модифікації найменшого значущого біта	4
РАЗОМ		48

6. Завдання для самостійної роботи

Тема 1. Основні поняття криптології

1. Математична модель шифрів, теорія зв’язку в секретних системах Клода Шенона.
2. Законодавча база України в галузі криптографії.

Тема 2. Класичні шифри та їх криптоаналіз

1. Взаємний індекс збігу.
2. Роторні шифрувальні машини та їх криптоаналіз.

Тема 3. Криптографічна стійкість шифрів

1. Модель порушника.
2. Методи та види несанкціонованого доступу.

Тема 4. Потокові симетричні шифри

1. Порівняльний аналіз генераторів псевдовипадкових послідовностей.
2. Потоковий шифр SNOW 2.0.
3. Потоковий шифр Salsa 20.

Тема 5. Алгоритм блокового симетричного шифрування DES

1. Алгоритм шифрування Lucifer.
2. Способи доповнення блоків (padding).

Тема 6. Режими шифрування блоків. Шифр IDEA

1. Режим зв'язування блоків із поширенням (PCBC).
2. Безпека IDEA.

Тема 7. Удосконалений стандарт шифрування AES

1. Алгоритми-фіналісти конкурсу AES: MARS, RC6, Serpent, Twofish.
2. Режими шифрування AES.

Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)

1. Стандарт криптографічного перетворення даних ДСТУ ГОСТ28147:2009.
2. Порівняльний аналіз ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014 («Калина»).

Тема 9. Основні положення криптографії з відкритим ключем

1. Основи модулярної арифметики.
2. Поняття і властивості алгебраїчних груп.
3. Тестування чисел на простоту.

Тема 10. Асиметричні криптосистеми

1. Головоломка Меркла.
2. Криптосистема Рабіна.
3. Джерела ключів асиметричних криптосистем та вимоги до них.

Тема 11. Криптографічні хеш-функції

1. Хеш-функції на основі блокових шифрів. MAC-коди.
2. Порівняльний аналіз хеш-функцій MD2, MD4, MD5 та MD6.

Тема 12. Цифровий підпис

1. Правове регулювання ЦП в Україні та світі.
2. Алгоритм цифрового підпису Шнорра.
3. Сліпий підпис, незаперечний підпис, груповий підпис.

Тема 13. Криптографічні протоколи

1. Вимоги до протоколів автентифікації.
2. Модель загроз порушення автентичності.
3. Модель взаємної недовіри та взаємного захисту.

Тема 14. Основи криптографії на еліптичних кривих

1. Алгоритм обчислення порядку еліптичної кривої.
2. Криптосистема Мессі-Омури над групою точок еліптичної кривої.
3. Аналіз вразливостей криптографічної схеми цифрового підпису ECDSA.

Тема 15. Елементи криптоаналізу шифрів

1. Силові методи криптоаналізу.
2. Криптоаналіз по побічним каналам.

Тема 16. Нові напрямки в криптографії

1. Стеганографія та її застосування.
2. Квантовий криптоаналіз.

7. Індивідуальні завдання

Індивідуальні завдання не передбачено навчальним планом.

8. Методи навчання

Застосовуються наступні методи навчання:

МН01 – вербальні (лекція, пояснення, розповідь, бесіда, інструктаж);

МН02 – наочні (спостереження, ілюстрація, демонстрація);

МН03 – практичні (різні види вправ та завдань, виконання розрахунків тощо);

МН04 – пояснювально-ілюстративний (передбачає надання готової інформації викладачем та її засвоєння студентами;

МН05 – репродуктивний, в основу якого покладено виконання різного роду завдань за зразком;

МН06 – метод проблемного викладу;

МН07 – частково-пошуковий (евристичний);

МН08 – дискусійний метод;

МН09 – метод активного навчання (проведення ділових ігор, ігрового проектування);

МН10 – ситуаційний метод, розв’язування кейсових завдань.

9. Методи контролю

Передбачено заходи поточного та підсумкового контролю. Під час проведення заходів контролю передбачено використання наступних методів оцінювання:

МО01 – оцінювання роботи під час аудиторних занять;

МО02 – виконання практичних завдань;

МО03 – поточне тестування;

МО04 – виконання аудиторної контрольної роботи;

МО05 – захист індивідуального завдання (за наявності);

МО06 – екзамен.

8. Розподіл балів

16 лекцій по 2 год. (32 год.)	12 лабораторних по 4 год. (48 год.)		10 тестів	2 модульні контрольні роботи	Сума
0,5 балів за відвідування	3 бали за звіт	1 бал зароботу на парі	1 бал за тест	17 балів	
8 балів	36 балів	12 балів	10 балів	34 бали	100 балів

Шкала оцінювання

За шкалою	Екзамен	Бали
A	Відмінно	90-100
B	Добре	82-89
C		74-81
D	Задовільно	64-73
E		60-63
FX	Незадовільно	35-59
F		0-34

11. Рекомендована література

Основна література

1. Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; 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.
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Л. Я. Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
3. Горбенко І. Д. // Прикладна криптологія: Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2013. – 880 с.
4. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К. :Мінекономрозвитку України, 2015.
5. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С.Олексюк. – К. -Тернопіль: Підручники і посібники, 2007. – 272 с.
6. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
7. Корченко О. Г. Прикладна криптологія: системи шифрування : підручник /О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.
8. Щур Н.О. Основи криптології: навч. посіб. / Н. О. Щур, О. А. Покотило. - Житомир: Державний університет «Житомирська політехніка», 2021. - 120 с.
9. Щур Н.О. Прикладна криптологія. Методичні рекомендації до виконання лабораторних робіт. / Н. О. Щур - Житомир: Державний університет «Житомирська політехніка», 2021. – 104 с.
10. Alfred J. Menezes. Handbook of Applied Cryptography/ Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Publisher: CRC Press, 2001. – 780 pages

11. Bruce Schneier. Applied cryptography: protocols, algorithms, and source code inC / 2nd ed. – New York : JohnWiley & Sons, Inc.,1995. – 792 pages.
12. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption Paperback. Kindle Edition, 2017. – 313 pages.

Допоміжна література

1. Бабенко Т.В. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В.Бабенко, Г.М.Гулак, С.О.Сушко, Л.Я.Фомичова. – Д.: Національний гірничий університет, 2013. – 318 с.
2. Ємець В. Сучасна криптографія. Основні поняття / Ємець В., Мельник А., Попович Р. – Л.: БаК, 2003. – 144 с.
3. Маркова І.І. Захист інформації. Криптографічні методи: Підручник для вищих навчальних закладів. / І.І. Маркова, А.І. Рибак, Ю.С. Ямпольський. – Одеса, 2001. – 175 с.

12. Інформаційні ресурси в Інтернеті

1. The CrypTool Portal [Електронний ресурс]. – Режим доступу : http://www.cryptool.org/en
2. CrypTool-Online [Електронний ресурс].– Режим доступу: https://www.cryptool.org/en/cto/
3. GnuPG [Електронний ресурс]. – Режим доступу: http://www.gnupg.org