МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра Комп'ютерної інженерії та інноваційних технологій

Введено в дію наказом ректора
Міжнародного гуманітарного
університету від 26.08.24 № 1

Ректор _____ К.В. Громовенко

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕТОДИ ПОБУДОВИ КРИПТОГРАФІЧНИХ СИСТЕМ

Галузь знань 12 Інформаційні технології

Спеціальність 125 «Кібербезпека та захист інформації»

–

Назва освітньої програми «Кібербезпека»

Рівень вищої освіти другий (магістерський) рівень

Одеса - 2024 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 29.08.24 року.

Розробники і викладачі	Контактний тел.	E-mail
Доцент кафедри комп'ютерної інженерії та інноваційних технологій, кандидат технічних наук, доцент **Йона Лариса Григорівна**	+380677463777	yonalarysa66@gmail.com

Завідувач кафедри комп'ютерної інженерії та інноваційних технологій, к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми к.т.н., доцент, _____ Лариса ЙОНА

Узгоджено Начальник навчального відділу _____ Лариса РАЙЧЕВА

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="9">Кількість кредитів – 4, загальна кількість годин – 120

Мова навчання – українська</td><td rowspan="9">Галузь 12 – Інформаційні технології
Спеціальність – 125 «Кібербезпека та захист інформації»

Рівень вищої освіти – другий (магістерський) рівень</td><td colspan="2">обов’язкова</td></tr>
<tr><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>2-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>22 год.</td><td>6год</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>22 год.</td><td>6 год</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>76 год.</td><td>108год</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>залік</td><td>залік</td></tr>
</table>

Дисципліна **Методи побудови криптографічних систем** є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 125 «Кібербезпека та захист інформації», а також обов’язковим компонентом освітньої програми для здобуття освітнього рівня «магістр» та має на меті формування у здобувачів уявлення про принципи побудови симетричних та асиметричних криптографічних систем, проблеми захисту інформації від порушення її конфіденційності, цілісності та доступності; принципи побудови та режими роботи блокових алгоритмів шифрування; розгляд концепції криптосистем з відкритим ключем; методи побудови схем електронно-цифрових підписів та керування криптографічними ключами.

Метою викладання навчальної дисципліни Методи побудови криптографічних систем є забезпечення здобувачів знаннями з питань принципів побудови криптографічних систем та проблем захисту інформації у системах комунікацій від порушення її конфіденційності, цілісності та доступності з урахуванням сучасного стану та перспективних напрямів розвитку криптографії.

Передумови для вивчення дисципліни – знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Інформаційна безпека інноваційної діяльності» формуються наступні компетентності із передбачених освітньо-професійною програмою «Кібербезпека» зі спеціальності 125 Кібербезпека.

Інтегральна компетентність

ІК. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

Фахові компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та

критичної інфраструктури.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

Заплановані результати навчання за навчальною дисципліною

У результаті вивчення цієї навчальної дисципліни студент має набути такі компетентності.

Знати:

- Основні поняття криптографії: конфіденційність, цілісність, доступність;
- Правові та етичні аспекти застосування криптографії в Україні;
- Види криптографічних систем: симетричні, асиметричні, гібридні криптосистеми;
- Основи теорії чисел, математичний апарат криптографії;
- Алгоритми симетричного шифрування;
- Режими роботи блокових шифрів;
- Потокові шифри: принципи роботи та застосування.
- Генерація та керування ключами в симетричних системах.
- Основи шифрування з відкритим ключем;
- Протоколи узгодження ключів;
- Криптографічні методи цифрового підпису;
- Принципи побудови інфраструктури відкритих ключів;
- Атаки на симетричні та асиметричні криптосистеми;
- Методи аналізу стійкості шифрів;
- Використання хешування для забезпечення цілісності даних та цифрових підписів;
- Протоколи автентифікації;
- Використання криптосистем для захисту конфіденційної інформації в різних галузях (електронна комерція, банківські системи, захист персональних даних);
- Сучасні тенденції у криптографії (основи квантової криптографії);

Вміти:

- Здійснювати аналіз існуючих криптографічних систем і оцінювати їхню стійкість до атак;
- Розуміти та порівнювати різні типи криптосистем (симетричні,

асиметричні, гібридні);
- Розробляти та впроваджувати симетричні та асиметричні криптографічні алгоритми;
- Вибирати відповідні криптографічні алгоритми та протоколи для різних задач і систем;
- Генерувати, зберігати, розповсюджувати та керувати криптографічними ключами в різних системах.
- Застосовувати протоколи узгодження ключів (Diffie-Hellman, ECDH) для безпечного обміну ключами;
- Використовувати криптографічні хеш-функції для забезпечення цілісності даних та створення цифрових підписів;
- Реалізовувати протоколи аутентифікації користувачів і вузлів мережі (TLS, SSL, Kerberos);
- Виявляти потенційні слабкі місця криптосистем і здійснювати оцінку стійкості до атак;
- Інтегрувати криптографічні рішення в сучасні інформаційні системи та програми;
- Слідкувати за новітніми розробками у сфері криптографії та впроваджувати сучасні рішення для підвищення безпеки інформаційних систем.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1.Актуальність питань методів побудови криптосистем для забезпечення надійного захисту інформації. Аналіз погроз інформації при передачі по каналах зв'язку. Вимоги до принципів побудови криптосистем.

Тема 2. Симетричні криптосистеми. Шифри на базі мережі Фейстеля. Дослідження алгоритму шифрування DES. Режими роботи. Недоліки алгоритму шифрування DES. Методи підвищення криптостійкості криптосистеми. Алгоритм 3-DES.

Тема 3. Європейський стандарт шифрування IDEA. Особливості побудови блокової криптосистеми.

Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі. Схема SP-мережі. Реалізація SP-мережі в криптосистемах AES. Режими роботи стандарту. Вимоги щодо побудови криптосистеми AES.

Тема 5. Стандарт шифрування України ДСТУ 7624:2014 «Калина». Режими роботи криптосистеми.

Тема 6. Порівняльний аналіз сучасних криптоалгоритмів за призначенням.

Тема 7. Асиметричні алгоритми шифрування.Особливості побудови систем з відкритим ключем.

Тема 8. Принципи керування ключовою системою. Генерування та розподілення ключів методом Діффі-Хеллмана.

Тема 9. Криптосистема Ель Гамаля. Процедури шифрування в криптосистемі Ель–Гамаля.

Тема 10. Алгоритм шифрування в криптосистемі RSA. Процедури генерування ключів та шифрування.

Тема 11. Системи ідентифікації та автентифікації. Біометричні методи автентифікації.

Тема 12. Методи побудови схем електронного підпису. Різновиди ЕП.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	практ.	сам. роб.		лекц.	прак	сам. роб.
Змістовий модуль 1. Архітектура симетричних систем ЗІ								
Тема 1. Актуальність питань методів побудови криптосистем для забезпечення надійного захисту інформації. Типи й класифікація алгоритмів шифрування.	10	2		8	10			10
Тема 2. Шифри на базі мережі Фейстеля. Недоліки алгоритму шифрування DES. Алгоритм 3-DES	10	2	2	6	10	2		8
Тема 3. Європейський стандарт шифрування IDEA. Особливості побудови блокової криптосистеми.	10		2	8	10			10
Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі. Стандарт шифрування AES.	10	2	2	6	10		2	8
Тема 5. Стандарт шифрування України ДСТУ 7624:2014 «Калина».	10	2	2	6	10			10
Тема 6. Порівняльний аналіз сучасних криптоалгоритмів за призначенням	10	2	2	6	10	2		8
Змістовий модуль 2 . Криптосистеми з відкритим ключем.								
Тема 7. Асиметричні алгоритми шифрування.	10	2	2	6	10	2		8
Тема 8. Принципи керування ключовою системою.	10	2	2	6	10			10
Тема 9. Процедури шифрування в	10	2	2	6	10		2	8

криптосистемі Ель–Гамаля.								
Тема 10. Шифрування в криптосистемі RSA.	10	2	2	6	10			10
Тема 11. Системи ідентифікації та автентифікації.	10	2	2	6	10			10
Тема 12. Методи побудови схем електронного підпису	10	2	2	6	10		2	8
Усього годин	**120**	**22**	**22**	**76**	**120**	**6**	**6**	**108**
ПІДСУМКОВИЙ КОНТРОЛЬ – Залік								

5. ПРАКТИЧНІ ЗАНЯТТЯ

№ з/п	Назва теми	Кількість годин	
		Денна форма	Заочна форма
1	Принципи побудови криптосистем за призначенням.	2	
2	Дослідження симетричних криптосистем, що побудовані на мережі Фейстеля. (DES; 3-DES; ДСТУ-28147-2009; IDEA)	4	2
3	Дослідження стандартів шифрування, що побудовані на SP-мережі. Стандарт шифрування AES.	2	
4	Дослідження стандарту шифрування України ДСТУ 7624:2014 «Калина».	4	
5	Дослідження асиметричних алгоритмів. Алгоритм шифрування RSA та Ель Гамаля.	4	2
6	Дослідження алгоритмів генерування та розподілення ключів. Алгоритм Діффі-Хеллмана.	2	
7	Дослідження алгоритмів електронного підпису RSA, Ель Гамаля та DSA.	4	2
	Всього	22	6

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «**Інформаційна безпека інноваційної діяльності»** включаються наступні тематики завдання.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	**Назва теми**	**Кількість годин**	
		денна форма	**заочна форма**
1	**Тема 1. Актуальність питань методів побудови криптосистем для забезпечення надійного захисту інформації.** Аналіз погроз інформації при передачі по каналах зв'язку. Вимоги до принципів побудови криптосистем	8	10

2	**Тема 2. Шифри на базі мережі Фейстеля.** Дослідження алгоритму шифрування DES. Режими роботи. Недоліки алгоритму шифрування DES. Методи підвищення криптостійкості криптосистеми. Алгоритм 3-DES.	6	8
3	**Тема 3. Європейський стандарт шифрування IDEA**. Особливості побудови криптосистеми.	8	10
4	**Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі.** Схема SP-мережі. Реалізація SP-мережі в криптосистемах AES Режими роботи стандарту. Вимоги щодо побудови криптосистеми AES.	6	8
5	**Тема 5. Стандарт шифрування України ДСТУ 7624:2014 «Калина»**. Порівняльний аналіз симетричних криптосистем.	6	10
6	**Тема 6.** Порівняльний аналіз сучасних криптоалгоритмів за призначенням	6	8
7	**Тема 7. Асиметричні алгоритми шифрування.** Особливості побудови систем з відкритим ключем.	6	8
8	**Тема 8. Принципи керування ключовою системою**. Генерування та розподілення ключів методом Діффі-Хеллмана.	6	10
9	**Тема 9. Криптосистема Ель Гамаля.** Процедури шифрування в криптосистемі Ель–Гамаля.	6	8
10	**Тема 10. Алгоритм шифрування в криптосистемі RSA.** Процедури генерування ключів та шифрування.	6	10
11	**Тема 11. Системи ідентифікації та автентифікації.** Біометричні методи автентифікації.	6	10
12	**Тема 12. Методи побудови схем електронного підпису.** Різновиди ЕП.	6	8
	Всього	**76**	**108**

8. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю	Складові оцінювання
Поточний контроль, який здійснюється у ході: проведення практичних та лабораторних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань.	50%
Підсумковий контроль, який здійснюється у ході проведення іспиту (заліку).	50%

Методи діагностики знань (контролю)	Фронтальне опитування, лабораторні завдання, індивідуальні завдання, робота у групах, розв`язання практичних завдань, залік

Питання до заліку

1. Що таке конфіденційність інформації?

2. Чим забезпечується захист конфіденційної інформації?

3. Що таке цілісність інформації?

4. Чим забезпечується захист цілісності інформації?

5. Що таке доступність інформації?

6. Дати поняття процесу шифрування інформації.

7. Ключ шифрування. Різновиди ключів шифрування.

8. Класичні методи шифрування. Поясніть сутність методів шифрування: підставляння, переставляння та гамування.

9. З яких простих перетворювань складається складний шифр?

10. Які вимоги до захисту персональних даних існують у рамках законодавства України?

11. Що таке криптографія і яку роль вона відіграє в захисті інформації?

12. Класифікація криптосистем за призначенням.

13. Привести вимоги для побудови блочних криптосистем.

14. Поясніть сутність понять “перемішування” та “розсіювання” за К.Шенноном?

15. Пояснити метод каскадування, який використовується для побудови

надійних блочних шифрів.

16. Принципи побудови симетричних криптосистем.

17. Побудова симетричних криптосистем за мережею Фейстеля.

18. Пояснити принцип побудови криптосистеми 3-DES.

19. Пояснити принцип побудови криптосистеми IDEA.

20. Порівняти відомі симетричні криптоалгоритми за параметрами: довжина ключа; кількість етапів шифрування; кількість ключів для одного етапу шифрування; реалізація мережі Фейстеля.

21. Пояснити принцип побудови алгоритму Діффі-Хеллмана.

22. Переваги та недоліки алгоритму розподілення ключів методом Діффі-Хеллмана.

23. Привести схему секретної системи зв’язку для симетричних криптосистем.

24. Привести схему секретної системи зв’язку для асиметричних криптосистем.

25. Принципи керування ключовою системою.

26. Привести алгоритм формування цифрового підпису.

27. Які існують класи криптоалгоритмів?

28. Пояснити принцип рівноміцного захисту в інформаційних системах.

29. З яких етапів складається алгоритм електронного цифрового підпису?

30. Які алгоритми називають несиметричними?

31. Призначення асиметричних криптосистем.

32. Принципи побудови асиметричних криптосистем.

33. Пояснити принцип побудови криптосистеми Ель Гамаля.

34. Пояснити принцип побудови криптосистеми AES.

35. Пояснити принцип побудови криптосистеми Калина.

36. Як вирішується питання автентифікації в телекомунікаціях?

37. Призначення хеш функції в алгоритмах електронного підпису.

38. Привести алгоритм формування цифрового підпису на базі системи RSA.

39. Пояснити принцип мультиплікативної атаки. Яка криптосистема має цей недолік?

40. Призначення Персонального ідентифікаційного номеру (PIN).

41. Призначення стеганографічного захисту інформації.

42. Як забезпечується поєднання криптографічних та стеганографічних методів захисту інформації?

43. Протоколи захисту електронних транзакцій.

44. Методи біометричної автентифікації.

45. Багатофакторна автентифікація.

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ (для заліку)

Рівень знань оцінюється:

– «відмінно» / «зараховано» A – від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» B – від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставленні завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» C – від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи та активність у науково-дослідній роботі;

– «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи;

– «задовільно» / «зараховано» E – від 60 до 63 балів. Студент був присутній не на всіх лекціях та практичних заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, виконав не всі завдання до самостійної роботи;

– «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу;

– «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів. Студент не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	Зараховано
74-81	C		
64-73	D	Задовільно	Зараховано
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. **Мартинюк, В. М., Гуменюк, О. В., & Слободянюк, В. В.** Криптографічні методи захисту інформації : навч. посіб. / В. М. Мартинюк, О. В. Гуменюк, В. В. Слободянюк. – Київ : Техніка, 2020. –304 с.
2. **Семенко, І. В., Копиленко, С. П.** Інформаційна безпека та криптологія: теорія і практика : підручник / І. В. Семенко, С. П. Копиленко. – Харків : Основа, 2021. – 352 с.
3. **Петренко, О. І., Корж, А. В.** Захист інформації в комп'ютерних системах та мережах : навч. посіб. / О. І. Петренко, А. В. Корж. – Львів : ЛНУ ім. І. Франка, 2019. – 278 с.
4. **Онацький О.В., Йона Л.Г., Бєлова Ю.В.** Криптографічний захист інформації: Навч. посіб./О.В.Онацький, Л.Г.Йона , Ю.В. Бєлова. - Одеса: ДУІТЗ, 2023. – 250 с..

Допоміжна

1. **Шевченко, В.** Прикладна криптографія : підручник / В. Шевченко. – Київ : Наукова думка, 2019. –320 с.

Інформаційні ресурси

1 Наказ МОН № 332 від 18.03.2021 року Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) рівня вищої освіти. URL: https://osvita.ua/legislation/Vishya_osvita.
2 Національна бібліотека України ім. В.І. Вернадського. URL: http://www.nbuv.gov.ua.
3 Портал кіберполіції України. URL: https://cyberpolice.gov.ua/
4 Портал урядової команди реагування на комп’ютерні надзвичайні події України (CERT-UA). URL: https://cert.gov.ua/
5 Coursera. Стенфорд, Мічіганський університет та інші.Coursera.org
6 Cryptography Stack Exchange. crypto.stackexchange.com
7 MIT OpenCourseWare. ocw.mit.edu
8 IEEE Xplore Digital Library.ieeexplore.ieee.org