



Міжнародний гуманітарний університет
Факультет Кібербезпеки, програмної інженерії та комп'ютерних наук
Комп'ютерної інженерії та інноваційних технологій

СИЛАБУС 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

Розробники і викладачі	Контактний тел.	E-mail
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій Йона Лариса Григорівна	+380677463777	yonalarysa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

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

Інтегральна компетентність

ІК1. 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.

Спеціальні (фахові, предметні) 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. Проводити 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.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		Вид заняття (денне відділення / заочне відділення)			Ознаки курсу		
ЄКТС	годин	Лекційні заняття	Практичні заняття	Самостійна робота	Курс, (рік навчання)	Семестр	Обов'язкова / вибіркова
4	120	22 / 6	22 / 6	76 / 108	1	1 /	Обов'язкова

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.	практ.	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.	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 криптосистемі Ель–Гамала.	10	2	2	6	10		2	8
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

<i>Усього годин</i>	120	22	22	76	120	6	6	108
ПІДСУМКОВИЙ КОНТРОЛЬ – Залік								

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Здобувачі отримують теми та питання дисципліни, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання, зокрема

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Методи побудови криптографічних систем» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання теоретичного матеріалу, здобутого під час семестру.
3. Виконання практичних та індивідуальних завдань, сформованих викладачем.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю знань.

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

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю		Складові оцінювання
Поточний контроль , який здійснюється під час проведення практичних занять, виконання індивідуального завдання, проведення консультацій та відпрацювання пропущених здобувачем занять.		50%
Підсумковий контроль , який здійснюється під час проведення екзамену.		50%
Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, тези доповіді, наукова стаття, індивідуальне опитування, тестування, екзамен.	

8. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ СТУДЕНТІВ З ПІДСУМКОВИМ КОНТРОЛЕМ У ФОРМІ ЕКЗАМЕНУ.

Денна та заочна форми навчання			
Поточний контроль			
Види роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання

Систематичність і активність роботи на базі практики			
1.1. Підготовка до практичних занять.	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	25
Виконання завдань для самостійного опрацювання			
1.2. Підготовка програмного матеріалу (тем, питань) для самостійного вивчення	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або індивідуально-консультативна робота (ІКР) викладача зі здобувачами.	10
Виконання індивідуальних завдань (науково-дослідна робота студента)			
1.3. Підготовка реферату за заданою тематикою.	Відповідно до розкладу занять і графіку ІКР	Обговорення (захист) матеріалів реферату.	10
1.4. Інші види індивідуальних завдань, зокрема, підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до розкладу занять і графіку ІКР	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	5
Разом балів за поточний контроль			50
<i>Підсумковий контроль – Залік</i>			50
Всього балів			100

Заочна форма навчання

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ (для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та практичних заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» В - від 82 до 89 балів. Здобувач 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 та практичних заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» С - від 74 до 81 балів. Здобувач 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 конспекту з виконаними завданнями до самостійної роботи, реферату та активність у

науково-дослідній роботі;

- «задовільно» / «зараховано» D - від 64 до 73 балів. Здобувач 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 конспекту з виконаними завданнями до самостійної роботи, рефератів;

- «задовільно» / «зараховано» E - від 60 до 63 балів. Здобувач 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, має неповний конспект з завданнями 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 0 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 (10-12)	A	Відмінно	Зараховано
82-89 (8-9)	B	Добре	
74-81(6-7)	C		
64-73 (5)	D		
60-63 (4)	E	Задовільно	
35-59 (3)	Fx		
1-34 (2)	F	Незадовільно	Не зараховано

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, Мічиганський університет та інші. [Coursera.org](https://www.coursera.org)
- 6 Cryptography Stack Exchange. crypto.stackexchange.com
- 7 MIT OpenCourseWare. ocw.mit.edu
- 8 IEEE Xplore Digital Library. ieeexplore.ieee.org