



**Міжнародний гуманітарний університет
ФАХОВИЙ КОЛЕДЖ
Циклова комісія зі спеціальності «Комп'ютерна інженерія»**

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЯХ

Галузь знань	12 – «Інформаційні технології»
Спеціальність	123 – «Комп'ютерна інженерія»
Назва освітньої програми	Комп'ютерна інженерія
Рівень передвищої освіти	Фаховий передвищий рівень

Розробники і викладачі	Контактний тел.	E-mail
кандидат технічних наук, доцент Йона Лариса Григорівна	+380677463777	yonalarysa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Дисципліна «Захист інформації в телекомунікаціях» є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 123 «Комп'ютерна інженерія», а також обов'язковим компонентом освітньої програми для здобуття освітнього рівня «фахової передвищої освіти». Ця дисципліна формує у здобувачів уявлення про принципи захисту інформації від порушення її конфіденційності, цілісності та доступності.

Метою навчальної дисципліни «Захист інформації в телекомунікаціях» 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 методів захисту інформації.

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

Інтегральна компетентність	
ІК	Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій в процесі професійної діяльності або навчання, що вимагає застосування методів і технологій комп'ютерної інженерії та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності, здійснювати контроль інших осіб у визначених ситуаціях
Загальні компетентності	
ЗК4	Здатність застосовувати знання у практичних ситуаціях
Спеціальні (фахові) компетентності	
СК1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційних технологій
СК2	Здатність застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування апаратних, програмних та інструментальних засобів комп'ютерної інженерії
СК5	Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки
СК6	Здатність брати участь у модернізації апаратних та програмних засобів комп'ютерної інженерії
СК11	Здатність здійснювати вибір, розгортати, інтегрувати, діагностувати, адмініструвати та експлуатувати комп'ютерні системи та мережі, мережеві ресурси, сервіси та інфраструктуру організації
СК13	Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їх компонентів шляхом використання аналітичних методів і методів моделювання
СК14	Здатність оцінювати і враховувати економічні, соціальні, технологічні та екологічні чинники, що впливають на сферу професійної діяльності
СК15	Здатність оцінювати рівень захисту інформації в комп'ютерних засобах та системах і обґрунтовувати вибір апаратних та програмних засобів для забезпечення його належного рівня
Програмні результати навчання	
РН2	Знати і розуміти теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп'ютерної інженерії
РН3	Знати сучасні методи та технології для розв'язання прикладних задач комп'ютерної інженерії
РН6	Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп'ютерної інженерії
РН17	Обґрунтовано обирати та використовувати методи криптографії для забезпечення необхідного рівня захисту інформації в комп'ютерних системах та мережах

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		Вид заняття			Ознаки курсу		
ЄКТС	годин	Лекційні заняття	Практичні заняття	Самостійна робота	Курс, (рік навчання)	Семестр	Обов'язкова / вибіркова
4	120	28	28	64	3 (на основі БЗСО) 2 (на основі ПЗСО)	6 (на основі БЗСО) 4 (на основі ПЗСО)	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин			
	Загалом	Лекційні заняття	Практичні заняття	Самостійна робота
Змістовий модуль 1. Архітектура систем захисту інформації				
Тема 1. Актуальність проблеми захисту інформації в сучасних системах телекомунікації.	8	2	2	4
Тема 2. Основи архітектури систем захисту інформації.	8	2	2	4
Тема 3. Алгоритми шифрування на базі мережі Фейстеля.	8	2	2	4
Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі.	8	2	2	4
Тема 5. Порівняльний аналіз симетричних криптосистем.	8	2	2	4
Тема 6. Основи стеганографічного захисту інформації	8	2	2	4
Тема 7. Сумісне використання стеганографічного та криптографічного захисту інформації в телекомунікаційних системах.				
Змістовий модуль 2 . Криптосистеми з відкритим ключем.	8	2	2	4
Тема 8. Принципи керування ключовою системою.	8	2	2	4
Тема 9. Асиметричні алгоритми шифрування	8	2	2	4
Тема 10. Односпрямовані геш-функції	10	2	2	6
Тема 11. Процедури шифрування в асиметричних криптосистемах	10	2	2	6
Тема 12. Порівняльний аналіз асиметричних криптосистем.	10	2	2	6
Тема 13. Системи ідентифікації та автентифікації.	10	2	2	6
Тема 14. Методи побудови схем електронного підпису	8	2	2	4
Загалом	120	28	28	64
Підсумковий контроль – залік				

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Здобувачі отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням платформ он-лайн навчання на основі інформаційних систем Moodle або Google Classroom. Виконання практичних робіт та проведення індивідуального тестування, забезпечується за допомогою існуючих в університеті комп'ютерних класів, бібліотеки та платформ он-лайн навчання на основі інформаційних систем Moodle або Google Classroom.

6. САМОСТІЙНА РОБОТА

№ з/п	Назва теми	Кількість годин
1	Тема 1. Актуальність проблеми захисту інформації в сучасних системах телекомунікації. Аналіз погроз інформації при передачі по каналах зв'язку. Методи захисту інформації в каналах зв'язку.	4
2	Тема 2. Основи архітектури систем захисту інформації. Принципи побудови систем захисту інформації. Класичні методи шифрування. Схема побудови складного шифру.	4
3	Тема 3. Алгоритми шифрування на базі мережі Фейстеля. Дослідження алгоритму шифрування DES. Режими роботи та недоліки. Методи підвищення криптостійкості криптосистеми. Алгоритм 3-DES. Криптосистема IDEA. Особливості побудови криптосистеми.	4
4	Тема 4. Сучасні стандарти шифрування, що побудовані на SP-мережі. Схема SP-мережі. Реалізація SP-мережі в криптосистемах AES та ДСТУ 7624:2014 «Калина». Вимоги до побудови криптосистем. Режими роботи та функціональні перетворення.	4
5	Тема 5. Порівняльний аналіз симетричних криптосистем. Порівняння симетричних криптосистем за основними параметрами щодо криптостійкості.	4
6	Тема 6. Основи стеганографічного захисту інформації. Основні вимоги до побудови систем приховування факту передачі інформації. Класифікація стегосистем. Основні характеристики класичної, комп'ютерної та цифрової стеганографії.	4
7	Тема 7. Сумісне використання стеганографічного та криптографічного захисту інформації в телекомунікаційних системах. Проектування схеми системи криптографічного та стеганографічного захисту інформації.	4
8	Тема 8. Принципи керування ключовою системою. Ключова система, генерування та розподілення ключів	4
9	Тема 9. Асиметричні алгоритми шифрування. Особливості побудови систем з відкритим ключем.	4
10	Тема 10. Принципи керування ключовою системою. Генерування, накопичування, та розподілення ключів Метод генерування та розподілення ключів Діффі-Хеллмана.	4
11	Тема 11. Криптосистема Ель Гамала. Процедури шифрування в криптосистемі Ель-Гамала.	6
12	Тема 12. Алгоритм шифрування в криптосистемі С. Процедури генерування асиметричної пари ключів та система шифрування RSA.	6
13	Тема 13. Системи ідентифікації та автентифікації. Прості методи автентифікації за паролем. Біометричні методи	6

	автентифікації. Біометрико-криптографічні перетворення при підтвердженні справжності користувача. Багатофакторна автентифікація.	
14	Тема 14. Методи побудови схем електронного підпису. Процедура створення підпису в алгоритмі RSA. Різновиди ЕП.	6
	Загалом	64

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю		Складові оцінювання
Поточний контроль та тестування, які здійснюються у ході проведення практичних занять, консультацій та відпрацювань		80%
Підсумковий контроль, який здійснюється у ході проведення заліку		20%
Методи діагностики знань (контролю)	Фронтальне опитування, тестові завдання, робота у групах, розв'язання практичних завдань, залік	

8. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ ЗДОБУВАЧІВ

Поточний контроль			
Види роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи на практичних заняттях			
1.1. Підготовка до практичних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	35
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування	Відповідно до робочої програми та розкладу занять	Перевірка результатів виконання тесту	35
Виконання індивідуальних завдань (науково-дослідна робота здобувача)			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять або ІКР, наукових конференцій та круглих столів.	10
Загалом балів за поточний контроль			80
Підсумковий контроль – залік			20
Загалом балів			100

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ ЗДОБУВАЧІВ

Рівень знань оцінюється:

– «відмінно» / «зараховано» А – від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, на екзамені демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставлені 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» В – від 82 до 89 балів. Здобувач володіє знаннями матеріалу на екзамені, 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 поставлені 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» С – від 74 до 81 балів. Здобувач відтворює значну частину теоретичного матеріалу на екзамені, 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. Здобувач був присутній не на всіх лекціях та практичних заняттях, на екзамені 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. Здобувач був присутній не на всіх лекціях та практичних заняттях, на екзамені 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. Здобувач 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. Здобувач 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. Криптографічний захист інформації: Навч. посіб./ Онацький О.В., Йона Л.Г., Белова Ю.В.. - Одеса: ДУІТЗ, 2023. – 250 с., ел.вар.

Допоміжна

- 2 Сучасні криптографічні системи. Навчальний посібник. С.М. Горохов, Л.Г. Йона, О.В. Онацький, під керівництвом проф. М.В. Захарченка Одеса: ВЦ ОНАЗ ім. О.С. Попова, 2007. – 152 с.
- 3 Асиметричні методи шифрування: Навч. посіб. / Онацький О.В., Йона Л.Г., Шинкарчук Т.М.; за ред. М. В. Захарченка. – Одеса: ОНАЗ ім. О. С. Попова, 2010. – 164 с.

Інформаційні ресурси

- 1 Наказ Міністерства освіти і науки України від 20.04.2022 № 366 «Про затвердження стандарту фахової передвищої освіти за спеціальністю 123 Комп'ютерна інженерія галузі знань 12 Інформаційні технології освітньо-професійного ступеня «фаховий молодший бакалавр», URL: <https://mon.gov.ua/storage/app/media/Fakhova%20peredvyshcha%20osvita/Zatverdzeni.standarty/2022/04/20/123-Kompyuterna.inzheneriya-366-20.04.2022.pdf>.
- 2 Національна бібліотека України ім. В.І. Вернадського. URL: <http://www.nbuv.gov.ua>.
- 3 Портал кіберполіції України. URL: <https://cyberpolice.gov.ua/>