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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

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

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

1. АНОТАЦІЯ ДО КУРСУ

Основи захисту інформації 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. Вона має на меті формування у здобувачів уявлення про принципи захисту інформації від порушення її конфіденційності, цілісності та доступності.

Метою викладання навчальної дисципліни «Основи захисту інформації» є забезпечення здобувачів початковими знаннями з проблем захисту інформації у системах комунікацій від порушення властивостей інформації, що захищається та розгляд основних методів захисту інформації.

Передумови для вивчення дисципліни – знання і вміння, отримані здобувачем при вивченні навчальних дисциплін*:* Офісні технології, Вступ до спеціальності, Програмне забезпечення комп'ютерних технологій.

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
ЗК8	Здатність вчитися і оволодівати сучасними знаннями
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
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
СК7	Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи
СК10	Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення
СК12	Здатність створювати, впроваджувати, адмініструвати бази даних і знань з використанням сучасних методів, технологій та систем керування базами даних
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
РН7	Застосовувати знання для формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей
РН9	Розробляти, тестувати, впроваджувати, експлуатувати програмне забезпечення для вбудованих і розподілених систем
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**
5	150	48	32	70	2 (на основі БЗСО) 1 (на основі ПЗСО)	4 (на основі БЗСО) 2 (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. Основи захисту інформації у комп'ютерних системах				
Тема 1. **Актуальність захисту інформації у комп'ютерних системах.** Правила безпечного користування мережею Інтернет. Інформаційні загрози національній безпеці держави.	12	4	2	6
Тема 2. **Модель безпеки даних.** Поняття конфіденційності, цілісності та доступності.	12	4	2	6
Тема 3. **Базови поняття.** Загроза. Атака. Вразливість. Вразливості у системі захисту через людський фактор. Порушники. Принципи побудови комплексної системи захисту інформації.	12	4	2	6
Тема 4. **Класифікація** загроз. Класифікація атак. Модель порушника.	12	4	2	6
Тема 5. **Безпека мережі.** Шкідливе програмне забезпечення. Шпигунські програми. Шахрайські дії. Фішинг. Скімінг. Соціальна інженерія. Програми-вимагачі. DDoS-атаки. Способи забезпечення безпеки мережі.	12	4	2	6
Тема 6. **Процедури ідентифікації, автентифікації, авторизації** користувачів мережі.	12	4	2	6
Тема 7. **Біометричні методи ідентифікації та автентифікації.** Статичні та динамічні біометричні методи. Поняття багатофакторної автентифікації.	12	4	2	6
Змістовий модуль 2 . Основи криптографічного захисту інформації в інфокомунікаціях.				
Тема 8. **Класифікація криптографічних методів за призначенням**.	12	4	2	6
Тема 9. **Методи та засоби захисту конфіденційної інформації**. Поняття шифрування, розшифрування, ключ шифрування.	14	4	4	6

Тема 10. **Класичні методи шифрування.** Історичні шифри заміни та перестановки. Принцип каскадування у складному шифрі.	14	4	4	6
Тема 11. **Методи та засоби захисту цілісності інформації**. Поняття автентифікації документів. Захист документообігу.	14	4	4	6
Тема 12. **Основи стеганографічного захисту інформації.** Призначення стеганографії. Види та методи стеганографії.	12	4	4	4
Загалом	**150**	**48**	**32**	**70**
Підсумковий контроль – екзамен				

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 захисту інформації у комп'ютерних системах	6
2	Тема 2. Модель безпеки даних	6
3	Тема 3. Базови поняття	6
4	Тема 4. Класифікація загроз	6
5	Тема 5. Безпека мережі.	6
6	Тема 6. Процедури ідентифікації, автентифікації, авторизації користувачів.	6
7	Тема 7. Біометричні методи ідентифікації та автентифікації	6
8	Тема 8. Класифікація криптографічних методів за призначенням.	6
9	Тема 9. Методи та засоби захисту конфіденційної інформації	6
10	Тема 10. Класичні методи шифрування	6
11	Тема 11. Методи та засоби захисту цілісності інформації	6
12	Тема 12. Основи стеганографічного захисту інформації	4
	Загалом	**70**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю		Складові оцінювання
Поточний контроль та тестування, які здійснюються у ході проведення практичних занять, консультацій та відпрацювань		50%
Підсумковий контроль, який здійснюється у ході проведення екзамен		50%
Методи діагностики знань (контролю)	Фронтальне опитування, тестові завдання, робота у групах, розв`язання практичних завдань, екзамен	

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	20
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування	Відповідно до робочої програми та розкладу занять	Перевірка результатів виконання тесту	20
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			**50**
Підсумковий контроль – екзамен			**50**
Загалом балів			**100**

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ ЗДОБУВАЧІВ

Рівень знань оцінюється:

– «відмінно» / «зараховано» A – 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 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. 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 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. 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., Бєлова 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/Zatverdzheni.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/