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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ ТЕХНІЧНОГО 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
Викладач **Швець Оксана Володимирівна**	+380673051784	ovshvets@ukr.net

1. АНОТАЦІЯ ДО КУРСУ

Обов'язкова навчальна дисципліна «Основи технічного захисту інформації» знайомить здобувачів із базовою програмною та апаратною частиною засобів технічного захисту.

Завдання дисципліни полягає у формуванні розуміння основних напрямків технічного захисту інформації, архітектури комп'ютерів, навичок з програмування, володіння основами забезпечення захисту комп'ютерних мереж. Особлива увага приділяється вивченню сучасних засобів кібербезпеки та захисту інформації, хмарній безпеці та криптографії.

Мета викладання дисципліни – формування основ знань стосовно роботи програмних та апаратних засобів захисту інформації в телекомунікаційних мережах, необхідних майбутнім фахівцям в області комп'ютерної інженерії.

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
РН6	Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп'ютерної інженерії
РН8	Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності
РН11	Ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів комп'ютерної інженерії
РН12	Поєднувати теорію і практику, знаходити та обґрунтовувати шляхи рішення типових задач у професійній діяльності з урахуванням виробничих інтересів
РН14	Використовувати сучасні інтегровані середовища, методи і технології розробки, впровадження, адміністрування комп'ютерних систем та мереж, баз даних і знань

РН15	Проводити інсталяцію та налаштування системного та прикладного програмного забезпечення, у тому числі програмних засобів захисту інформації з метою реалізації встановленої політики інформаційної безпеки
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**
6	180	28	56	96	4 (на основі БЗСО) 3 (на основі ПЗСО)	8 (на основі БЗСО) 6 (на основі ПЗСО)	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	**Кількість годин**			
	Загалом	**Лекційні заняття**	**Практичні заняття**	**Самостійна робота**
Тема 1. Основні цілі та задачі забезпечення захисту інформації	44	6	14	24
Тема 2. Міжмережеве екранування	46	8	14	24
Тема 3. Сучасні технології захисту мереж	46	8	14	24
Тема 4. Хмарні технології та віртуальні машини.	44	6	14	24
Загалом	**180**	**28**	**56**	**96**
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. Основні цілі та задачі забезпечення захисту інформації** 1. Ключові визначення та поняття 2. Історія розвитку IT та техніки 3. Розвиток суспільства та основні потреби захисту інформації 4. Задачі забезпечення захисту інформації 5. Модель OSI 6. Модель TCP/IP	24
2	**Тема 2. Міжмережеве екранування** 7. Основні протоколи захисту 8. Атаки типу DOS 9. Еволюція міжмережних екранів 10. Методи сегментації мережі. 11. Визначення та призначення DMZ. 12. Відмінності хостових та мережевих екранів.	24
3	**Тема 3. Сучасні технології захисту мереж** 13. Ризики та вразливості пов’язані з технологіями віддаленого доступу. 14. Сучасні протоколи VPN. 15. Програмні та апаратні засоби захисту інформації, представлені на українському ринку. 16. Антивіруси, міжмережні екрани, системи виявлення та протидії вторгненням. 17. Протокол DNS. Захист протоколу DNS за допомогою цифрового підпису. 18. Питання шифрування та авторизації при організації тунельних протоколів.	24
4	**Тема 4. Хмарні технології та віртуальні машини.** 19. Визначення у сфері віртуалізації. 20. Типи віртуальних машин. 21. Авторизація та автентифікація у віртуальних приватних мережах. 22. Моделі хмарних обчислень. 23. Керування даними у хмарі.	24
	Загалом	**96**

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 екзамену		50%
Методи діагностики знань (контролю)	Фронтальне опитування, тестові завдання, робота у групах, розв`язання практичних завдань, екзамену	

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. CISSP – Переклад книги Shon Harris "CISSP All-In-One Exam Guide". Електронний ресурс http://dorlov.blogspot.com/2011/05/issp-cissp-all-in-one-exam-guide.html
2. Omar Santos, Samer Salam, Hazim Dahir. Ehe ai revolution in networking, cybersecurity,and emerging technologies. ISBN-10: 0-13-829369-4. Pearson Education, Inc,Hoboken, NJ / 2024 – 185p.
3. Li Wang. Physical Layer Security in Wireless Cooperative Networks. ISSN 2366-1445 (electronic). Springer International Publishing AG 2018 https://t.me/learningnets/15086

Допоміжна

1. Barker K. CCNA Security 640-554 Official Cert Guide / Barker K., Morris S.., 2012. – 700 с.
2. Криптографічний захист інформації: Навч. посіб./ Йона Л.Г., Онацький О.В., Бєлова Ю.В.. - Одеса: ДУІТЗ, 2023. – 250 с., ел.вар.

Інформаційні ресурси

1 Національна бібліотека ім. В.І.Вернадського. URL: http://www.nbuv.gov.ua/
2 Одеська обласна універсальна наукова бібліотека ім. М.С. Грушевського. URL: https://biblioteka.od.ua/
3 Портал «Electronic Design». URL: https://www.electronicdesign.com/
4 Платформа https://learn.microsoft.com/ru-ru/training/browse/?roles=ai-engineer%2Csecurity-engineer&skip=30