Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «Управління інформаційною та кібернетичною безпекою»
(назва)

Освітнього рівня першого (бакалаврського) рівня вищої освіти

Спеціальності 125 «Кібербезпека»

Галузь знань 12 «Інформаційні технології»

1. Назва освітньої компоненти Аналіз та оцінка уразливостей інформаційних систем
(назва дисципліни)

2. Тип основна, вибіркова (вказати) основна

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	0	18	18	96
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Основи інфокомунікаційних технологій 2. Стандарти інформаційної та кібербезпеки						
Освітні компоненти для яких є базовою	1. Управління ризиками інформаційної безпеки 2.Теорія ризиків						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. Знання та розуміння предметної області та розуміння професії.			1. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.				
2. здатність до генерування нових знань з теорії захисту інформації та інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; тощо.			2. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.				

Компетенції відповідно до вимог роботодавців	
1. Знання основних принципів та концепцій інформаційної безпеки (ІБ);	1. Уміння аналізувати вразливості та загрози, оцінювати відповідні ризики, вибирати контрзаходи та здійснювати комплексні заходи по управлінню ризиками.
2. Базові знання нормативно-правових актів, стандартів і технічних умов, інструкцій та настанов управління ризиками ІБ;	2. Уміння здійснювати оцінку відповідності системи захисту своєму призначенню відповідно до вимог діючих стандартів;
3. Знання в галузі інформаційних технологій та систем, теорії ризику, економіки інвестицій та менеджменту, необхідні для аналізу, оцінки та управління ризиками інформаційної безпеки;	3. Застосування засобів автоматичного сканування уразливостей інформаційних систем підприємств.

6. Результати навчання відповідно до ОПП

1. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

2. ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

3. ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в ІТС.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
	Лекція 1	Тема: Вступ до АОУІС				
	Лекція 2	Тема: Апаратно-програмні засоби для проведення технічного аудиту ІС	1. Засвоїти основні поняття ризиків 2. Опанувати класифікацію ризиків			
	Лекція 3	Тема: Документування дій під час проведення технічного аудиту ІС	1. Засвоїти основні закономірності та моделі 2. озвитку Опанувати використання основних залежностей розвитку			
	Лекція 4	Тема: Пошук та збір інформації з відкритих джерел	1. Засвоїти основні складові системного підходу 2. Опанувати окремі методи системного підходу			

	Практичне заняття 1	Тема: Відповідальність за втручання у діяльність ІС	1. 2.	Класифікувати ризики		
	Практичне заняття 2	Тема: Принцип дії програмних засобів пошуку уразливостей ІС	1. 2.	Оперування понятійним апаратом теорії ризиків		
	Практичне заняття 3	Тема: Принципи документування дій щодо пошуку уразливостей		Вивчення підходів щодо використання прогностичних математичних моделей розвитку		
	Практичне заняття 4	Тема: Збір інформації з відкритих джерел	Вивчити теоретичні основи функціонально-вартісного підходу	Прийняття рішень за допомогою функціонально-вартісного підходу		
	Практичне заняття 5	Тема: Віртуальні лабораторії для імітації атак на ІС		Чисельний розрахунок базових показників ймовірностей		
	Лабораторна робота 1	Віртуальна лабораторія техчніного аудитора ІС		Класифікувати ризики		
	Лабораторна робота 2	Віртуальна лабораторія техчніного аудитора ІС		Оперування понятійним апаратом теорії ризиків		
	Лабораторна робота 3	Пошук та збір інформації з відкритих джерел		Вивчення підходів щодо використання прогностичних математичних моделей розвитку		
	Лабораторна робота 4	Пошук та збір інформації з відкритих джерел		Прийняття рішень за допомогою функціонально-вартісного підходу		
	Лабораторна робота 5	Документування дій під час проведення технічного аудиту ІС		Чисельний розрахунок базових показників ймовірностей		
Розділ 2						

	Лекція 5	Тема: Автоматизовані сканери для пошуку уразливостей ІС	Засвоїти основні ймовірнісні міри ризику Опанувати методи чисельного розрахунку ймовірнісних мір ризику			
	Лекція 6	Тема: Методи за засоби пошуку вразливостей ІС	Засвоїти основні ймовірнісні міри ризику Опанувати методи чисельного розрахунку ймовірнісних мір ризику			
	Лекція 7	Тема: Вразливості ВЕБ додатків та ВЕБ серверів	Засвоїти основні міри корисності Опанувати методи чисельного розрахунку мір корисності			
	Лекція 8	Тема: Парольні атаки	Засвоїти основні ризики інвестиційних проектів Опанувати методи чисельного розрахунку ризиків інвестиційних проектів			
	Лекція 9	Тема: Звіт за результатами технічного аудиту	Засвоїти сучасні підходи щодо управління ризиками в межах менеджменту проектів			
	Практичне заняття 6	Тема: Сканування мереж та автоматичні сканери вразливостей		Чисельний розрахунок ймовірнісних мір ризику		
	Практичне заняття 7	Тема: Парольні атаки на інформаційні системи		Здобути та закріпити практичні навички щодо застосування одно етапних процедур прийняття рішень		
	Практичне заняття 8	Тема: Пошук вразливостей ВЕБ серверів та ВЕБ додатків		застосування одно етапних процедур прийняття рішень		

	Практичне заняття 9	Тема: Звіт по аудиту ІС		застосування одно етапних процедур прийняття рішень		
	Лабораторна робота 6			Чисельний розрахунок ймовірнісних мір ризику		
	Лабораторна робота 7	Сканування мереж та автоматичні сканери вразливостей		Здобути та закріпити практичні навички щодо застосування одно етапних процедур прийняття рішень		
	Лабораторна робота 8	Вразливості ВЕБ додатків та ВЕБ серверів		застосування одно етапних процедур прийняття рішень		
	Лабораторна робота9	Парольні атаки		застосування одно етапних процедур прийняття рішень		

8. Мова вивчення освітньої компоненти
(українська)
Розділ 2 частково англійською
9. Інформаційне забезпечення освітньої компоненти
Common Vulnerability Scoring System version 3.1
Методы и средства тестирования на проникновение веб-приложений и сетей
OWASP Testing Guide v4
10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(екзамен)
11. Матеріально-технічне забезпечення освітньої компоненти
Перелік питань для самостійної підготовки, перелік навчальної літератури та доступ до тексту лекцій та слайдів до лекцій через систему MOODLE для підготовки до практичних занять. Для роботи з документами використовується комп’ютерна техніка лабораторії кафедри.