Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(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. Вища математика 2. Основи інфокомунікаційних технологій 3. Стандарти інформаційної та кібербезпеки						
Освітні компоненти для яких є базовою	1. Теорія ризиків 2.						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. Загальнонаукова компетентність – здатність до накопичення наукових і педагогічних вмінь та навичок (діагностування й інтерпретування ситуацій, планування та здійснення наукових досліджень, викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційних технологій та захисту інформації);			1. Аналізувати ризики та джерела загроз, розробляти модель загроз, розробляти модель порушника				
2. здатність до генерування нових знань з теорії захисту інформації та			2. На основі інформації, одержаної у ході дослідження об'єкта				

інформаційної безпеки, з проблем алгоритмізації та програмування процесів в системах кібербезпеки; тощо.	інформаційної діяльності замовника та результатів аналізу ризиків, розробляти рекомендації щодо удосконалення системи управління інформаційною безпекою, застосування яких дозволить мінімізувати ризики та формулювати перелік уразливостей
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, оцінювання уразливостей інформаційних систем, необхідні для аналізу, та управління інформаційною безпекою підприємства;	
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: Технічний аудит інформаційних систем. Суть, види, зміст. Відповідальність за порушення законодавта у сфері кібернетичної безпеки.	1. Знати Загальні положення АОУІС. 2. Основні терміни та поняття ІБ та ПТ 3. Характеристику порушників кібернетичної безпеки 4. Методології та підходи до оцінювання захищеності інформаційних систем			

	Лекція 2	Тема: Віртуальне середовище для тестової лабораторії. VirtualBox, Kali Linux, Metasploit/Debian/Labs	1. Засвоїти VirtualBox 2. Kali Linux 3. Безпечне застосування інструментів для тестування захищеності			
	Лекція 3	Тема: Розвідка. Збір інформації з відкритих джерел.	1. Знати Основні поняття та суть розвідки у тестуванні захищеності 2. Активни та пасивний види розвідки 3. Методології та програмні засоби			
	Практичне заняття 1	Тема: Технічний аудит інформаційних систем. Суть, види, зміст.		1. Класифікація порушників кібернетичної безпеки		
	Практичне заняття 2	Тема: Віртуальне середовище для тестової лабораторії. VirtualBox, Kali Linux, Metasploit/Debian/Labs		1. Налаштування тестової лабораторії. VirtualBox, Kali Linux, Metasploit/Debian/Labs		
	Практичне заняття 3	Тема: Збір інформації з відкритих джерел.		1. Активни та пасивний види розвідки 2. Вибирати Методології та програмні засоби		
	Лабораторне заняття 1	Тема: Технічний аудит інформаційних систем. Суть, види, зміст.		1. Характеризувати порушників кібернетичної безпеки		
	Лабораторне заняття 2	Тема: Тестова лабораторія. VirtualBox, Kali Linux, Metasploit/Debian/Labs		1. Створення тестової лабораторії. VirtualBox, Kali Linux, Metasploit/Debian/Labs		
	Лабораторне заняття 3	Тема: Збір інформації з відкритих джерел.		1. Проведення Активного та пасивного видів розвідки		
Розділ 2						

	Лекція 4	Тема: Аналіз та оцінка вразливостей мережевих ресурсів (NETWORK)	1. Пошук цілей та вразлвостей. 2. Перехоплення трафіку та MITM 3. Експлуатація знайдених вразливостей 4. Можливі дії після успішної експлуатації			
	Лекція 5	Тема: Аналіз та оцінка уразливостей систем (System security)	1. Суть та основні поняття System security 2. Криптографія та парольні атаки 3. Переповлення буферу та інші види вразливостей систем			
	Лекція 6	Тема: Аналіз та оцінка уразливостей WEB ресурсів	1. Суть та основні поняття WEB pentesting 2. Збір інформації та розвідка 3. Оцінка уразливостей WEB ресурсів 4. Ін’єкції, інші види вразливостей та способи атак на WEB ресурси			
	Лекція 7	Тема: Аналіз та оцінка уразливостей бездротових мереж Wi-Fi	1. Необхідне обладнання та налаштування середовища 2. Стандарти бездротових мереж 3. Дослідження Wi-Fi мереж, аналіз трафіку, атаки на бездротові мережі			
	Лекція 8	Тема: Документування дій щодо аналізу та оцінюванню уразливостей інформаційних систем.	1. Документування дій аудитора 2. Написання звіту на основі проведеного аналізу інформаційних систем			

		Звіт				
	Лекція 9	Тема: Документування дій щодо аналізу та оцінюванню уразливостей інформаційних систем. Звіт	1. Документування дій аудитора 2. Написання звіту на основі проведеного аналізу інформаційних систем			
	Практичне заняття 4	Тема: Аналіз та оцінка вразливостей мережевих ресурсів (NETWORK)		1. Пошук цілей та вразлвостей. 2. Перехоплення трафіку та MITM 3. Експлуатація знайдених вразливостей 4. Можливі дії після успішної експлуатації		
	Практичне заняття 5	Тема: Аналіз та оцінка уразливостей систем (System security)		1. Криптографія та парольні атаки 2. Переповлення буферу та інші види вразливостей систем		
	Практичне заняття 6	Тема: Аналіз та оцінка уразливостей WEB ресурсів		1. Збір інформації та розвідка 2. Оцінка уразливостей WEB ресурсів 3. Ін’єкції, інші види вразливостей та способи атак на WEB ресурси		
	Практичне заняття 7	Тема: Аналіз та оцінка уразливостей бездротових мереж Wi-Fi		1. Стандарти бездротових мереж 2. Дослідження Wi-Fi мереж, аналіз трафіку, атаки на бездротові мережі		
	Практичне заняття 8	Тема: Документування дій щодо аналізу та оцінюванню уразливостей.		1. Документування дій аудитора		

	Практичне заняття 9	Тема: Документування дій щодо аналізу та оцінюванню уразливостей		1. Написання звіту на основі проведеного аналізу інформаційних систем		
	Лабораторне заняття 4			1. Пошук цілей та вразлвостей. 2. Перехоплення трафіку та MITM 3. Експлуатація знайдених вразливостей		
	Лабораторне заняття 5			1. Криптографія та парольні атаки		
	Лабораторне заняття 6			1. Оцінка уразливостей WEB ресурсів 2. Ін’єкції, інші види вразливостей та способи атак на WEB ресурси		
	Лабораторне заняття 7			1. Дослідження Wi-Fi мереж, аналіз трафіку, атаки на бездротові мережі		
	Лабораторне заняття 8			1. Документування дій аудитора		
	Лабораторне заняття 9			1. Написання звіту на основі проведеного аналізу інформаційних систем		
8. Мова вивчення освітньої компоненти						
українська, англійська						
9. Інформаційне забезпечення освітньої компоненти						
Common Vulnerability Scoring System version 3.1						
Georgia Weidman Penetration Testing: A Hands-On Introduction to Hacking: навчальний посібник.						
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.