

**Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «Технічні системи інформаційного та кібернетичного захисту»**
(назва)

Освітнього рівня «Магістр»

Спеціальності 125 Кібербезпека

Галузь знань 12 Інформаційні технології

1. Назва освітньої компоненти Аналіз та оптимізація процесів і систем технічного захисту інформації

2. Тип основна

3.Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
			8	--	10		72
4.Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	<ol style="list-style-type: none"> 1. Вища математика 2. Інформаційна безпека держави 3. Фізичні основи захисту інформації 4. Політика безпеки 5. Програмне забезпечення інформаційної безпеки 6. Кібернетичне право 7. Виявлення загроз інформаційній безпеці 8. Теорія ризиків 9. Системи технічного захисту інформації 10. Комплексні системи захисту інформації 						
Освітні компоненти для яких є базовою	1.Дисципліна I є базовою для підготовки і написання дипломних кваліфікаційних робіт на відповідність кваліфікації МАГІСТР.						
5. Компетенції відповідно до ОПІ та вимог роботодавців:							
Компетенції відповідно до ОПІ							
Знати				Вміти			
1. Основні нормативні положення Законодавства України, нормативно-правові акти у галузі інформаційної безпеки;				1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника;			

<p>2. Вітчизняні та міжнародні нормативні, методичні документи з питань розробки та впровадження новітніх зразків засобів технічного захисту інформації;</p> <p>3. Стандарти, технічні умови та інші нормативні й керівні матеріали з проектування, розроблення й оформлення технологічної документації комплексних систем захисту інформації;</p> <p>4. Методи проведення випробувань комплексних систем захисту інформації на відповідність вимогам вітчизняних та міжнародних нормативних документів;</p>	<p>2. Обґрунтувати необхідність створення ТСЗІ;</p> <p>3. Оформити політику безпеки;</p> <p>4. Розробляти технічне завдання на створення ТСЗІ;</p> <p>5. Розробляти проектну, робочу та експлуатаційну документацію на КСЗІ;</p> <p>6. Організовувати та проводити аналіз ТСЗІ.</p>
--	---

Компетенції відповідно до вимог роботодавців

<p>1. Основні нормативні положення Законодавства України, нормативно-правові акти у галузі інформаційної безпеки;</p> <p>2. Вітчизняні та міжнародні нормативні, методичні документи з питань розробки та впровадження новітніх зразків засобів технічного захисту інформації;</p> <p>3. Стандарти, технічні умови та інші нормативні й керівні матеріали з проектування, розроблення й оформлення технологічної документації комплексних систем захисту інформації;</p>	<p>1. Проводити аналіз і атестацію комплексу технічного захисту інформації від витоків технічними каналами;</p> <p>2. Проводити оптимізацію засобів захисту від несанкціонованого доступу, налагодження всіх механізмів розмежування доступу користувачів до інформації та апаратних ресурсів ІТС, контроль за діями користувачів, формування та актуалізація баз даних захисту, а також контроль цілісності програмного забезпечення та баз даних захисту;</p> <p>3. Проводити аналіз працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії;</p> <p>4. Проводити аналіз та оптимізацію експлуатації систем КСЗІ;</p>
--	--

6. Результати навчання відповідно до ОПП

7. План вивчення освітньої компоненти

Змістовний розділ дисципліни	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
Тема Загальні положення та вимоги в частині організації робіт із оптимізації СТЗІ	Лекція 1	Загальні положення та вимоги в частині організації робіт із захисту інформації	1. Загальні положення та вимоги в частині організації робіт із захисту інформації 2. Національні нормативні документи з технічного захисту інформації	1. Вміти проводити пошук необхідних норм, методик, інструкцій, положень, загальних вимог до систем захисту інформації.		
	Лекція 2	Складові оптимізації СТЗІ.	1. Заходи та засоби, які реалізують захист інформації	1. В залежності від властивостей		

			в ІТС. 2. Вплив властивостей оброблюваної інформації, класу автоматизованої системи та умов експлуатації ІТС на склад, структуру та вимоги до ТСЗІ. 3. Особливості побудови інтегрованих систем.	оброблюваної інформації визначати для АС класу 1,2 і 3 необхідні профілі захисту, склад, структуру та вимоги до ТСЗІ.		
Лекція 3	Основні положення про службу захисту інформації. План захисту інформації в ІТС.		1. Порядок створення, структуру служби захисту інформації. 2. Завдання, функції та повноваження служби захисту інформації. 3. Порядок Оформлення політики безпеки; 4. Порядок розробки Моделі загроз і Моделі порушника.	Розробляти план робіт з проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації КСЗІ та інших питань; Визначати: 1. Перелік об'єктів захисту. 2. Потенційні загрози для інформації. Розробляти: 3. Модель загроз. 4. Модель порушника.		
Практичне заняття 1	Нормативно-правові акти та НД у сфері захисту інформації.		1. Загальні положення та вимоги в частині організації робіт із захисту інформації 2. Національні нормативні документи з технічного захисту інформації	1. Вміти проводити пошук необхідних норм, методик, інструкцій, положень, загальних вимог до систем захисту інформації.		
Практичне заняття 2	Обґрунтування необхідності аналізу ТСЗІ.		1. Загальні положення та вимоги в частині організації робіт із захисту інформації 2. Національні нормативні документи з технічного захисту інформації	1.Визначати потенційні загрози для інформації; 2. Проводити обґрунтування необхідності створення КСЗІ.		
Практичне	Положення про службу		1. Склад служби захисту,	Розробляти:		

	заняття 3	захисту. План захисту.	права та обов'язки посадових осіб, завдання СЗ. 1. Функції СЗ під час створення комплексної системи захисту інформації:	1. Календарний план робі, проектування, впровадження, технічного обслуговування, ТСЗІ; 2. План заходів з забезпечення безпеки інформації.		
	Самостійна робота	Тема 1. Загальні положення та вимоги в частині організації робіт із захисту інформації та порядку створення ТСЗІ в ІТС	Загальні положення та вимоги в частині організації робіт із захисту інформації та порядку створення КСЗІ в ІТС	Формулювати вимоги в частині організації робіт із захисту інформації та порядку створення ТСЗІ в ІТС		
Розділ 2						
Тема. Етапи створення КСЗІ. Передпроектні роботи	Лекція 4	Формування завдання на оптимізацію ТСЗІ.	Критерії, норми, порядок, вимоги до атестації у ТСЗІ Порядок формування завдання на створення ТСЗІ.	Формувати загальні вимоги до ТСЗІ в ІТС. Формувати завдання на створення ТСЗІ.		
	Лекція 5	Політики безпеки інформації в ІТС.	Порядок розробки політики безпеки інформації в ІТС	Розробляти Політику безпеки інформації в ІТС		
	Практичне заняття 4	Розробка технічного завдання на створення ТСЗІ	Порядок розробки ТЗ щодо захисту інформації в ІТС	Розробляти ТЗ щодо захисту інформації в ІТС		
	Практичне заняття 5	Розробка політики безпеки інформації в ІТС.	Порядок розробки політики безпеки інформації в ІТС	Розробляти Політику безпеки інформації в ІТС		
	Самостійна робота	Етапи створення аналізу ТСЗІ. Передпроектні роботи	Етапи створення ТСЗІ. Передпроектні роботи	Проводити передпроектні роботи		
Розділ 3						
Тема. Етапи створення КСЗІ. Розробка проекту КСЗІ	Лекція 6	Розробка проекту ТСЗІ.	1. Етапи розробки проекту КСЗІ, їх зміст. 2. Склад і зміст документації робочого проекту КСЗІ; 3. Порядок розробки робочого проекту КСЗІ	Формулювати вимоги до складу проекту ТСЗІ Формулювати вимоги до змісту документації робочого проекту ТСЗІ		
	Лекція 7	Комплекс ТСЗІ.	Основи організації та етапи	Визначати вимоги до		

			виконання робіт щодо створення комплексу ТЗІ на ОІД. Технічні канали витоку інформації, засоби захисту від витоку технічними каналами, їх технічні характеристики	комплексу ТЗІ, склад комплексу Виявляти канали витоку інформації, рівні інформаційних сигналів, визначати параметри необхідних засобів захисту.		
	Лекція 8	Комплекс засобів захисту від несанкціонованого доступу (КЗЗ).	Міжнародні та національні критерії оцінки захищеності АС від НСД Перелік сертифікованих з заданими рівнями відповідальності засобів захисту від несанкціонованого доступу . Профілі захисту, реалізовані в засобах захисту	За міжнародними та національними критеріями проводити оцінку захищеності інформації в ІТС Проводити інсталяцію та налагоджування засобів захисту від несанкціонованого доступу		
	Самостійна робота	Тема 3. Етапи створення ТСЗІ. Розробка проекту ТСЗІ	Етапи створення ТСЗІ. Розробка проекту ТСЗІ	Контролювати розробку проекту		
Розділ 4						
Тема . Етапи створення ТСЗІ. Введення ТСЗІ в дію.	Практичне заняття 6	Засоби захисту інформації від витоку технічними каналами.	Засоби захисту, їх технічні характеристики	Користуватись засобами захисту інформації		
	Практичне заняття 7	Оцінка рівня магнітної складової побічних випромінювань ПЕОМ. Контроль захищеності інформації від витоку через електромагнітні випромінювання ПЕОМ.	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		
	Практичне заняття 8	Оцінка рівня електричної складової побічних випромінювань ПЕОМ. Контроль захищеності інформації	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		

		від витоків через електромагнітні випромінювання ПЕОМ.				
Розділ 5						
Тема 5. Атестація ТСЗІ.	Лекція 9	Порядок проведення експертизи засобів захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації	Порядок організації та проведення експертизи комплексних систем захисту інформації. Права та обов'язки суб'єктів експертизи. Порядок надання Експертного висновку та Атестації	Організувати роботи по проведенню експертизи та оформленню Атестації відповідності.		
	Практичне заняття 9	Оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.	Порядок Оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.	Проводити Оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.		
	Практичне заняття 10	Оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.	Порядок Оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.	Проводити Оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу.		
	Самостійна робота	Тема 5. Атестація КСЗІ.	Порядок організації та проведення експертизи комплексних систем захисту інформації. Права та обов'язки суб'єктів експертизи. Порядок надання Експертного висновку та Атестації	Організувати роботи по проведенню експертизи та оформленню Атестації відповідності.		
8. Мова вивчення освітньої компоненти						

Українська, англійська технічна- вивчення інструкцій пристроїв пошуку та блокування засобів негласного отримання інформації на практичних заняттях 6, 9 та 10
9. Інформаційне забезпечення освітньої компоненти
<p>1. Основи інформаційної безпеки автори В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест Лабораторний практикум з теорії кіл і сигналів в інформаційному та кіберпросторах автори Ю.О. Тихонов, В.А. Савченко, А.М. Котенко, А.М. Зідан</p> <p>3. Методика пошуку засобів негласного отримання інформації Державного Університету телекомунікацій 2019</p> <p>4. Методичні рекомендації до виконання дипломної роботи першого рівня вищої освіти «БАКАЛАВР» для студентів спеціальності 125 «Кібербезпека», 2019р.</p> <p>5. НД ТЗІ 2.6-001-11; НД ТЗІ 3.7-003-05; НД ТЗІ 2.7-010-09; НД ТЗІ 2.7-009-09</p>
<p>Спеціальною літературою наданою компаніями- партнерами-</p> <p>1. Методика пошуку засобів негласного отримання інформації ТОВ Квірін, 2017р.</p> <p>2. Методика пошуку засобів негласного отримання інформації ТОВ DAS. 2015р.</p>
10. Методи оцінювання, підсумкові звітності за освітньою компонентою
Заліки, екзамени, курсові проекти, тестування
11. Матеріально-технічне забезпечення освітньої компоненти
Лабораторія технічних систем захисту інформації на об'єктах інформаційної діяльності
Лабораторія імітаційного моделювання технічних систем захисту"

Інформаційний пакет освітньої компоненти, яка викладається англійською мовою, додатково розміщується на сторінці кафедри на англійській мові