

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

**Освітнього рівня «Бакалавр»**

**Спеціальності 125 Кібербезпека**

**Галузь знань 12 Інформаційні технології**

**1. Назва освітньої компоненти **Методи та засоби технічного захисту інформації****

(назва дисципліни)

**2. Тип основна**

3.Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	3,7	112	12	-	18	12	70
<b>4. Взаємозв'язок у структурно-логічній схемі</b>							
Освітні компоненти, які передують вивченню	1. Фізика. 2. Вища математика. 1. Схемотехніка систем технічного захисту інформації. 2. Електромагнітна сумісність. 3. Теорія інформації та кодування. 4. Комплексні системи захисту інформації. 5. Системи технічного захисту інформації.						
Освітні компоненти для яких є базовою	Комплексні системи захисту інформації						
<b>5. Компетенції відповідно до ОПП та вимог роботодавців:</b>							
<b>Компетенції відповідно до ОПП</b>							
<b>Знати</b>				<b>Вміти</b>			
1. Основні нормативні положення Законодавства України, нормативно-правові акти у галузі інформаційної безпеки; 2. Вітчизняні та міжнародні нормативні, методичні документи з питань розробки та впровадження новітніх зразків засобів технічного захисту інформації;				1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника; 2. Обґрунтувати необхідність створення ТСЗІ; 3. Оформити політику безпеки; 4. Розробляти технічне завдання на створення ТСЗІ;			

<p>3. Стандарти, технічні умови та інші нормативні й керівні матеріали з проектування, розроблення й оформлення технологічної документації технічних систем захисту інформації;</p> <p>4. Методики проведення робіт по пошуку та блокуванню засобів негласного отримання інформації</p>	<p>5. Розробляти проектну, робочу та експлуатаційну документацію на ТЗІ;</p> <p>6. Організовувати та проводити роботи по пошуку та блокуванню засобів негласного отримання інформації.</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 пусконаладжувальні роботи, монтаж обладнання і атестацію комплексу технічного захисту інформації від витоку технічними каналами;</p> <p>2. Проводити інсталяцію та ініціалізацію комплексу 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 перевірку працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії;</p> <p>4. Проводити дослідну експлуатацію 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 захисту інформації КСЗІ	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. Державні нормативні документи з технічного захисту інформації	1. Вміти проводити пошук необхідних норм, методик, інструкцій, положень, загальних вимог до систем захисту інформації.		
	Лекція 2	Склад та методи ТЗІ	1. Заходи та засоби, які реалізують захист інформації в ІТС.	1. В залежності від властивостей оброблюваної інформації визначати необхідні профілі захисту, склад, структуру та вимоги до		

				ТЗІ.		
Лекція 3	Основні положення про службу захисту інформації. План захисту інформації в ІТС.	1. Порядок створення, структуру служби технічного захисту інформації. 2. Завдання, функції та повноваження служби захисту інформації. 3. Порядок Оформлення політики безпеки;	Розробляти план робіт з проектування, реалізації, оцінювання, впровадження, технічного обслуговування, експлуатації ТЗІ та інших питань; Визначати: 1. Перелік об'єктів захисту. 2. Потенційні загрози для інформації.			
Практичне заняття 1	Нормативно-правові акти та НД у сфері технічного захисту інформації.	1. Загальні положення та вимоги в частині організації робіт із захисту інформації 2. Державні 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 застосування ТЗЗІ	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 ТЗІ.			
Практичне заняття 3	Положення про службу захисту інформації. План захисту.	1. Склад служби захисту, права та обов'язки посадових осіб, завдання СЗ. 1. Функції СЗ під час створення комплексної системи захисту інформації:	Розробляти: 1. Календарний план робі, проектування, впровадження, технічного обслуговування, ТЗІ; 2. План заходів з забезпечення безпеки інформації.			
Самостійна	Тема 1. Загальні	Загальні положення та	Формулювати вимоги в			

	робота	положення та вимоги в частині організації робіт із захисту інформації та порядку створення ТЗІ в ІТС	вимоги в частині організації робіт із захисту інформації та порядку створення ТЗІ в ІТС	частині організації робіт із захисту інформації та порядку створення ТЗІ в ІТС		
Розділ 2						
Тема. Етапи створення КСЗІ. Передпроектні роботи	Лекція 4	Формування завдання на створення ЗІ, технічними засобами	Критерії, норми, порядок, вимоги до захисту інформації в ІТС Порядок формування завдання на створення ЗІ.	Формувати загальні вимоги до ТЗІ в ІТС. Формувати завдання на створення ТЗІ.		
	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 ТЗІ	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 КСЗІ. Передпроектні роботи	Етапи створення КСЗІ. Передпроектні роботи	Проводити передпроектні роботи		
Розділ 3						
Тема. Етапи створення КСЗІ. Розробка проекту КСЗІ	Лекція 6	Розробка проекту тЗІ.	1. Етапи розробки проекту тЗІ, їх зміст. 2. Склад і зміст документації робочого проекту ТЗІ; 3. Порядок розробки робочого проекту ТЗІ	Формулювати вимоги до складу проекту ТЗІ Формулювати вимоги до змісту документації робочого проекту ТЗІ		
	Лекція 7	Впровадження комплексу ТЗІ.	Основи організації та етапи виконання робіт щодо створення комплексу ТЗІ на ОІД. Технічні канали витоку інформації, засоби захисту від витоку технічними каналами, їх технічні характеристики	Визначати вимоги до 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 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 ТЗІ. Розробка проекту ТЗІ	Етапи створення ТЗІ. Розробка проекту ТЗІ	Контролювати розробку проекту		
Розділ 4						
Тема . Етапи створення ТЗІ. Впровадження ТЗІ 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 побічних випромінювань і наведень ПЕОМ. Засоби контролю захищеності інформації від витоку технічними каналами.	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		
	Практичне заняття 8	Оцінка рівня побічних випромінювань і наведень ПЕОМ. Контроль захищеності інформації від витоку через мережі живлення і заземлення.	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		

Практичне заняття 9	Оцінка рівня магнітної складової побічних випромінювань ПЕОМ. Контроль захищеності інформації від витоків через електромагнітні випромінювання ПЕОМ.	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		
Практичне заняття 10	Оцінка рівня електричної складової побічних випромінювань ПЕОМ. Контроль захищеності інформації від витоків через електромагнітні випромінювання ПЕОМ.	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		
Практичне заняття 11	Пристрій «СРМ-700»-	Профілі захисту, реалізовані в засобах захисту, порядок налагоджування пристрій «СРМ-700»-	Проводити інсталяцію та налагоджування - Пристрій «СРМ-700»-		
Практичне заняття 12	Пристрій ST-31	Профілі захисту, реалізовані в засобах захисту, порядок налагоджування пристрій «ST-31»-	Проводити інсталяцію та налагоджування - Пристрій «ST-31»-		
Практичне заняття 13	Скануючий приймач AOR 8200	Профілі захисту, реалізовані в засобах захисту, порядок налагоджування пристрій «AOR 8200»-	Проводити інсталяцію та налагоджування - Пристрій «AOR 8200»-		
Практичне заняття 14	Скануючий приймач IC-R20	Профілі захисту, реалізовані в засобах захисту, порядок налагоджування пристрій «IC-R20»-	Проводити інсталяцію та налагоджування - Пристрій «IC-R20»-		
Практичне заняття 15	Пристрій Protect	Профілі захисту, реалізовані в засобах захисту, порядок налагоджування пристрій «Protect»-	Проводити інсталяцію та налагоджування - Пристрій «Protect»-		
Практичне заняття 16	АПК Digi Scan	Профілі захисту, реалізовані в засобах захисту, порядок	Проводити інсталяцію та налагоджування - Пристрій		

			налагоджування пристрій АПК Digi Scan	АПК Digi Scan		
	Самостійна робота	Тема 4. Етапи створення ТЗІ. Введення ТЗІ в дію.	Етапи створення ТЗІ. Введення ТЗІ в дію.	Контролювати введення ТЗІ в дію.		
<b>Розділ 5</b>						
Тема 5. Атестація пристроїв ТЗІ	Лекція 9	Порядок проведення експертизи засобів захисту інформації від несанкціонованого доступу	Порядок організації та проведення експертизи захисту інформації. Порядок надання	Організувати роботи по проведенню експертизи ТЗІ		
	Практичне заняття 17	АПК Digi Scan	Профілі захисту, реалізовані в засобах захисту, порядок налагоджування пристрій для роботи по аудіоканалу АПК Digi Scan	Проводити інсталяцію та налагоджування – робота по виявленню аудіоканалів витоку інформації за допомогою АПК Digi Scan		
	Практичне заняття 18	АПК Digi Scan	Профілі захисту, реалізовані в засобах захисту, порядок налагоджування пристрій для роботи по ІЧ каналу АПК Digi Scan	Проводити інсталяцію та налагоджування – робота по виявленню ІЧ каналів витоку інформації за допомогою АПК Digi Scan		
	Самостійна робота	Тема 5. Атестація пристроїв ТЗІ.	Порядок організації та проведення атестації пристроїв ТЗІ	Організувати роботи по проведенню атестації пристроїв ТЗІ		
<b>8. Мова вивчення освітньої компоненти</b>						
Українська, англійська технічна- вивчення інструкцій пристроїв пошуку та блокування засобів негласного отримання інформації на практичних заняттях 6, 11 та 13						
<b>9. Інформаційне забезпечення освітньої компоненти</b>						
<ol style="list-style-type: none"> <li>1. Основи інформаційної безпеки автори В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест</li> <li>2. Лабораторний практикум з теорії кіл і сигналів в інформаційному та кіберпросторах автори Ю.О. Тихонов, В.А. Савченко, А.М. Котенко, А.М. Зідан</li> <li>3. Методика пошуку засобів негласного отримання інформації Державного Університету телекомунікацій 2019</li> <li>4. Методичні рекомендації до виконання дипломної роботи першого рівня вищої освіти «БАКАЛАВР» для студентів спеціальності 125 «Кібербезпека», 2019р.</li> <li>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</li> </ol>						

Спеціальною літературою наданою компаніями- партнерами-
1. Методика пошуку засобів негласного отримання інформації ТОВ Квірін,2017р.
2. Методика пошуку засобів негласного отримання інформації ТОВ DAS.2015р.
<b>10. Методи оцінювання, підсумкові звітності за освітньою компонентою</b>
Заліки, екзамени, курсові проекти, тестування
<b>11. Матеріально-технічне забезпечення освітньої компоненти</b>
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