Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «Комплексні системи захисту інформації»
(назва)

Освітнього рівня «Бакалавр»

Спеціальності 125 Кібербезпека

Галузь знань 12 Інформаційні технології

1. Назва освітньої компоненти Комплексні системи захисту інформації
(назва дисципліни)

2. Тип основна

3.Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	4,2	**126**	**18**	**--**	**18**	**18**	**72**
4.Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Вища математика 2. Фізика 3. Інформаційна безпека держави 4. Фізичні основи захисту інформації 5. Політика безпеки 6. Програмне забезпечення інформаційної безпеки 7. Кібернетичне право 8. Безпека інформації в інформаційно-комунікаційних системах 9. Виявлення загроз інформаційній безпеці 10. Захищені інформаційні технології 11. Теорія ризиків 12. Системи технічного захисту інформації						
Освітні компоненти для яких є базовою	1.Дисципліна КСЗІ є базовою для підготовки і написання дипломних кваліфікаційних робіт на відповідність кваліфікації БАКАЛАВР, а також для подальшого навчання за програмою МАГІСТР.						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ОПП							

Знати	Вміти
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; 3. Стандарти, технічні умови та інші нормативні й керівні матеріали з проектування, розроблення й оформлення технологічної документації комплексних систем захисту інформації; 4. Методики проведення випробувань комплексних систем захисту інформації на відповідність вимогам вітчизняних та міжнародних нормативних документів;	1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника; 2. Обґрунтувати необхідність створення КСЗІ; 3. Оформити політику безпеки; 4. Розробляти технічне завдання на створення КСЗІ; 5. Розробляти проектну, робочу та експлуатаційну документацію на КСЗІ; 6. Організовувати та проводити державну експертизу КСЗІ.
Компетенції відповідно до вимог роботодавців	
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; 3. Стандарти, технічні умови та інші нормативні й керівні матеріали з проектування, розроблення й оформлення технологічної документації комплексних систем захисту інформації;	1. Проводити пусконалагоджувальні роботи, монтаж обладнання і атестацію комплексу технічного захисту інформації від витоку технічними каналами; 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; 3. Проводити перевірку працездатності засобів захисту інформації в автономному режимі та при їх комплексній взаємодії; **4.** Проводити дослідну експлуатацію КСЗІ;
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	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	1.Вміти проводити пошук необхідних норм, методик, інструкцій, положень, загальних вимог до систем		

організації робіт із захисту інформації та порядку створення КСЗІ в ІТС			документи з технічного захисту інформації	захисту інформації.		
	Лекція 2	Склад КСЗІ.	1. Заходи та засоби, які реалізують захист інформації в ІТС. 2. Вплив властивостей оброблюваної інформації, класу автоматизованої системи та умов експлуатації ІТС на склад, структуру та вимоги до КСЗІ. 3.Особливості побудови інтегрованих систем.	1. В залежності від властивостей оброблюваної інформації визначати для АС класу 1,2 і 3 необхідні профілі захисту, склад, структуру та вимоги до КСЗІ.		
	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 створення КСЗІ.	1. Загальні положення та вимоги в частині організації робіт із захисту інформації	1.Визначати потенційні загрози для інформації; 2. Проводити		

			2. Національні нормативні документи з технічного захисту інформації	обґрунтування необхідності створення КСЗІ.		
	Практичне заняття 3	Положення про службу захисту. 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, КСЗІ; 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 КСЗІ 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 КСЗІ в ІТС		
Розділ 2						
Тема. Етапи створення КСЗІ. Передпроектні роботи	Лекція 4	Формування завдання на створення КСЗІ.	Критерії, норми, порядок, вимоги до захисту інформації в ІТС Порядок формування завдання на створення КСЗІ.	Формувати загальні вимоги до КСЗІ в ІТС. Формувати завдання на створення КСЗІ.		
	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 КСЗІ	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	Лекція 6	Розробка проекту КСЗІ.	1.Етапи розробки проекту КСЗІ, їх зміст. 2. Склад і зміст документації	Формулювати вимоги до складу проекту КСЗІ Формулювати вимоги до		

проекту КСЗІ			робочого проекту КСЗІ; 3. Порядок розробки робочого проекту КСЗІ	змісту документації робочого проекту КСЗІ		
	Лекція 7	Комплекс 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 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 КСЗІ. Розробка проекту КСЗІ	Етапи створення КСЗІ. Розробка проекту КСЗІ	Контролювати розробку проекту		
Розділ 4						
Тема . Етапи створення КСЗІ. Введення КСЗІ 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	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		

		каналами.				
	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 витоку через електромагнітні випромінювання ПЕОМ.	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		
	Практичне заняття 10	Оцінка рівня електричної складової побічних випромінювань ПЕОМ. Контроль захищеності інформації від витоку через електромагнітні випромінювання ПЕОМ.	Порядок оцінки ПЕМВН	Проводити оцінку ПЕМВН		
	Практичне заняття 11	КЗЗ від НСД «Рубіж-РСО»	Профілі захисту, реалізовані в засобах захисту, порядок установки та налагоджування КЗЗ	Проводити інсталяцію та налагоджування засобів захисту від несанкціонованого доступу		
	Практичне заняття 12	Установка та налагоджування КЗЗ від НСД "Рубіж - РСО".	Профілі захисту, реалізовані в засобах захисту, порядок установки та налагоджування КЗЗ	Проводити інсталяцію та налагоджування засобів захисту від несанкціонованого доступу		
	Практичне заняття 13	КЗЗ від НСД «Гриф».	Профілі захисту, реалізовані в засобах захисту, порядок установки та налагоджування КЗЗ	Проводити інсталяцію та налагоджування засобів захисту від несанкціонованого доступу		
	Практичне заняття 14	Установка та налагоджування КЗЗ від	Профілі захисту, реалізовані в засобах захисту, порядок	Проводити інсталяцію та налагоджування засобів		

		НСД «Гриф».	установки та налагоджування КЗЗ	захисту від несанкціонованого доступу		
	Практичне заняття 15	Установка та налагоджування КЗЗ від НСД «Лоза».	Профілі захисту, реалізовані в засобах захисту, порядок установки та налагоджування КЗЗ	Проводити інсталяцію та налагоджування засобів захисту від несанкціонованого доступу		
	Практичне заняття 16	Випробування КСЗІ. Дослідна експлуатація.	Порядок проведення випробувань і дослідної експлуатації КСЗІ	Проводити випробування і дослідну експлуатацію КСЗІ		
	Самостійна робота	Тема 4. Етапи створення КСЗІ. Введення КСЗІ в дію.	Етапи створення КСЗІ. Введення КСЗІ в дію.	Контролювати введення КСЗІ в дію.		
Розділ 5						
Тема 5. Атестація КСЗІ.	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 Атестата	Організувати роботи по проведенню експертизи та оформленню Атестата відповідності.		
	Практичне заняття 17	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 18	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	Тема 5. Атестація КСЗІ.	Порядок організації та	Організувати роботи по		

	робота		проведення експертизи комплексних систем захисту інформації. Права та обов'язки суб'єктів експертизи. Порядок надання Експертного висновку та Атестата	проведенню експертизи та оформленню Атестата відповідності.		

8. Мова вивчення освітньої компоненти

Українська, англійська технічна- вивчення інструкцій пристроїв пошуку та блокування засобів негласного отримання інформації на практичних заняттях 6, 11 та 13

9. Інформаційне забезпечення освітньої компоненти

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
3. Методика пошуку засобів негласного отримання інформації Державного Університету телекомунікацій 2019
4. Методичні рекомендації до виконання дипломної роботи першого рівня вищої освіти «БАКАЛАВР» для студентів спеціальності 125 «Кібербезпека»,2019р.
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

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.

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