ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплексні системи захисту інформації

Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека
Обсяг дисципліни – 6 кредитів ЄКТС
Шифр дисципліни – ОПП.16
Мова навчання – Українська
Статус дисципліни – Обов'язкова (професійної підготовки)
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	4	7	6	180	66	32	34	-	-	114	+	-	-	+
Разом ДФН			**6**	**180**	**66**	**32**	**34**	**-**	**-**	**114**	**1**	**-**	**-**	**1**

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» за спеціальністю 125 «Кібербезпека»

Робоча програма складена _____ канд. техн. наук, доцент Віктор ЧЕШУН
Підпис автора(ів)

Олена ЗАРИЦЬКА
Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3. Пояснювальна записка

Дисципліна «Комплексні системи захисту інформації» є однією із дисциплін фахової підготовки здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека» в межах спеціальності 125 «Кібербезпека ».

Пререквізити: компонентна база і схемотехніка систем захисту; нормативно-правове забезпечення кібербезпеки; адміністрування та захист баз і сховищ даних; системи контролю доступу; безпека безпроводових технологій та інтернету речей; технічний і криптографічний захист інформації; захист інформації в інформаційно-комунікаційних системах; безпека вебресурсів; управління інформаційною безпекою; технології виявлення вразливостей та вторгнень; проектно-технологічна практика; моделювання систем захисту даних, оцінка ризиків і прийняття рішень.

Кореквізити: переддипломна практика.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов; ЗК 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; ЗК 5 Здатність до пошуку, оброблення та аналізу інформації; ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; ФК 3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки; ФК 7 Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.); ФК 12 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

***програмних результатів навчання*:** ПРН 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності; ПРН 11 Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах; ПРН 12 Розробляти моделі загроз та порушника; ПРН 13 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних; ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень; ПРН 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів; ПРН 17 Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; ПРН 28 Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки; ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки; ПРН 39 Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах; ПРН 53 Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

Мета дисципліни. Формування системи знань та розуміння предметної області необхідних для формалізованого опису, аналізу й синтезу комплексних систем захисту інформації; розв'язування складних спеціалізованих задач; застосування методів та засобів проектування, випробування, впровадження та супроводу комплексних систем захисту інформації.

Предмет дисципліни. Методи, методики, інформаційно-комунікаційні технології, програмно-апаратне забезпечення комплексних систем захисту інформації, їх впровадження та супроводу.

Завдання дисципліни. Формування практичних навичок проєктування, впровадження та супроводу захищених інформаційних систем, забезпечення конфіденційності, цілісності та доступності інформації в них, а також підготовка фахівців, здатних розробляти та застосовувати комплексні системи захисту інформаціївідповідно до нормативної бази України.

Результати навчання. Після вивчення дисципліни студент повинен: *аналізувати, виявляти та оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам та *проводити оцінку* ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики

інформаційної та\або кібербезпеки, *здійснювати* оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.), *реалізовувати* комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів, *вирішувати* задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, *вирішувати* задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; *використовувати* програмні та програмно-апаратні комплекси засобів захисту інформаційних ресурсів в інформаційно-телекомунікаційних (автоматизованих) системах, *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень, *застосовувати* методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки, *вирішувати* задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах, *виконувати* моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки, *виявляти* небезпечні сигнали технічних засобів і *вимірювати* параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації, *інтерпретувати* результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; *виконувати* пошук, оброблення, аналіз та синтез інформації з різних джерел державною та іноземними мовами і *використовувати* отримані результати для ефективного рішення спеціалізованих задач дисципліни і професійної діяльності; *забезпечувати* введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту, ефективність професійної комунікації в задачах проєктування, впровадження та супроводу комплексних систем захисту інформації.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:		
	лекції	**лабораторні роботи**	**СРС**
Тема 1. Проєктування комплексних систем захисту інформації	6	8	24
Тема 2. Технічні засоби захисту інформації	20	16	66
Тема 3. Випробування та впровадження комплексної системи захисту інформації	4	4	16
Тема 4. Супровід комплексної системи захисту інформації	2	6	8
Разом:	**32**	**34**	**114**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Тема 1. Проектування комплексних систем захисту інформації	**6**
1	**Загальні положення про комплексні системи захисту інформації** Структура та зміст дисципліни і методичні рекомендації щодо її вивчення. Місце дисципліни у навчальному процесі. Вимоги до знань та вмінь тих, хто навчається. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки. Визначення, позначення та скорочення. Поняття та призначення комплексної системи захисту інформації. Основні вимоги до КСЗІ. Принципи та етапи захисту від загроз при побудові КСЗІ. Літ.:[1] с.6-8; [2] с.81-86	2
2	**Основні принципи організації комплексних систем захисту інформації** Принципи організації КСЗІ. Концептуальні підходи до проєктування систем захисту. Порядок проведення робіт із створення КСЗІ в інформаційно-телекомунікаційній системі (ІТС). Етапи створення КСЗІ в ІТС. Формування технічного завдання на створення КСЗІ в ІТС. Базові розділи ТЗ. Нормативний супровід розробки ТЗ. Вимоги НД ТЗІ 3.7-001-99 до змісту, послідовності та викладення розділів ТЗ на створення КСЗІ в ІКС. Розробка ескізного проєкту КСЗІ. Представлення схем, структур, елементів КСЗІ. Оформлення та представлення текстової документації. Розробка комплекту документації для етапу проєктування КСЗІ. КСЗІ в критичній інфраструктурі. Літ.:[1] с.6-16; [2] с.189-199; [10] с.19-49	2
3	**Класифікація загроз інформаційній безпеці. Аналіз загроз на об'єкті захисту** Класифікація загроз інформаційній безпеці, ознаки класифікації. Ознаки моделі порушника, як етапу побудови КСЗІ. Категорії порушників. Класифікація порушника. Поняття контрольована зона. Модель загроз для ідентифікації каналів витоку інформації. Джерело загрози. Перелік загроз з визначенням порушень властивостей інформації та ІТС. Літ.:[3] с.19-27; [4] с.20-37	2
	Тема 2. Технічні засоби захисту інформації	**20**
4	**Джерела та носії інформації** Характеристика захищеної інформації. Захист інформації як інтегральна проблема та шляхи її вирішення. Специфіка застосування програмно-апаратних засобів захисту в СКЗІ, оцінка результативності якості прийнятих рішень щодо їх застосування. Умови безпеки інформації. Небезпечні сигнали і їх джерела. Класифікація джерел та носіїв інформації. Сутність запису і знімання інформації з носія. Джерела сигналів. Джерела функціональних сигналів. Побічні електромагнітні випромінювання (ПЕМВ) та наведення. Програмні та програмно-апаратні комплекси виявлення вторгнень. Літ.:[1] с.11-22; [2] с.79-86; [11] с.66-88	2
5	**Типова структура та види технічних каналів витоку інформації (ТКВІ).** Загальна характеристика технічного каналу витоку інформації. Класифікація та характеристика технічних каналів витоку інформації. Особливості витоку інформації технічними каналами. Типова структура та види технічних каналів витоку інформації. Схема можливих каналів витоку і несанкціонованого доступу до інформації. Літ.:[1] с.17-26; [2] с. 18-34	2
6	**Методи та засоби захисту від витоку інформації** Використання програмних та програмно-апаратних комплексів захисту інформаційних ресурсів Заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. Принципи блокування ТКВІ. Заходи щодо блокування ТКВІ з використанням активних та пасивних засобів. Заходи щодо виявлення портативних електронних пристроїв перехоплення інформації.Заходи щодо перетворення сигналів у каналах зв'язку. Літ.:[2] с.148-186; [3] с.31-38; [6] с.70-86	2
7	**Електричні канали витоку інформації** Класифікація електричних каналів витоку інформації. Забезпечення захисту інформації від ненавмисної дії технічними засобами. Виявлення небезпечних сигналів технічних засобів. Екранування технічних засобів. Заземлення. Літ.:[1] с.26-44; [2] с. 46-63	2

8	**Електромагнітні канали витоку інформації** Види побічних електромагнітних випромінювань. Канал побічних електромагнітних випромінювань основних та додаткових технічних засобів. Підходи до зняття інформації через електромагнітні випромінювання. Канал "паразитної" модуляції сигналів ВЧ генераторів. Канал "паразитної" ВЧ генерації підсилювачів. Канал побічних електромагнітних наведень на лінії електроживлення (заземлення) та комунікації. Канал ВЧ нав'язування (для зняття інформації, що обробляється. Літ.:[1] с.34-46; [2] с.83-90; [4] с.28-43	2
9	**Радіоканали втрат інформації** Структура радіоканалів втрат інформації. Класифікація технічних каналів витоку акустичної (мовної) інформації. Акустичні канали витоку інформації. Віброакустичні канали витоку інформації. Акустоелектричні канали. Акустооптоелектронні (лазерні акустичні) канали витоку інформації. Канали ВЧ нав'язування (для зняття мовної інформації). Перехоплення акустичних сигналів. Літ.:[1] с.45-76, 132-148; [2] с.34-46, с.117-142	2
10	**Технічні канали витоку інформації на основі закладних пристроїв** Сутність та класифікація засобів несанкціонованого перехоплення інформації (закладних пристроїв). Загальні характеристики та особливості деяких типів закладних пристроїв. Пристрої прослуховування приміщень. Радіозакладні пристрої. Заходи захисту інформації від витоку каналами на основі закладних пристроїв Літ.:[1] с.56-76, 132-148; [2] с.117-142	2
11	**Системи блокування відеоспостереження** Методи та засоби відеоспостереження. Принципи протидії засобам відеорозвідки. Класифікація візуально-оптичних каналів витоку інформації. Методи . захисту інформації від витоку по візуально-оптичному каналу. Методи і засоби пошуку прихованих відеокамер. Пошук і блокування прихованих пристроїв відеоспостереження, що використовують радіоканал для передачі інформації Літ.:[1] 126-128; [2] с.63-67; [3] с.506-527	2
12	**Канали витоку інформації при експлуатації ЕОМ** Види і природа каналів витоку інформації при експлуатації ЕОМ. Способи і методи ЗІ, оброблюваної засобами електронної техніки, від витоку радіочастотним каналу. Механізм виникнення ПЕМВ засобів цифрової електронної техніки. Технічна реалізація пристроїв маскування. Оцінка рівня ПЕМВ. Прилади виявлення ПЕМВ. Літ.: [1] с.70-81; [2] с.79-109; [3] с.536-551	2
13	**Методи та засоби забезпечення систем фізичного доступу та охорони території** Системи фізичного захисту об'єктів. Типова система фізичного доступу. Доглядові системи.. Ручні та арочні металошукачі. Автономні та мережеві системи доступу. Сигналізації. Літ [2] с.199-250; [3] с.557-568; [10] с.67-101	2
	Тема 3. *Випробування та впровадження комплексної системи захисту інформації*	**4**
14	**Організація випробувань КСЗІ** Реалізація КСЗІ відповідно до вимог нормативно-правових документів. Введення КСЗІ в дію. Аналіз та оцінка ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. Підготовка КСЗІ до введення в дію. Комплектування КСЗІ. Монтажно-пусковий період. Пуско-налагоджувальні роботи. Попередні випробування та дослідна експлуатація. Оцінка ефективності та рівня захищеності ресурсів в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки. Літ.: [1] с.81-91; [2] с.189-198; [3] с.568-572	2
15	**Державна експертиза КСЗІ в ІТС** Положення про державну експертизу в сфері ТЗІ. Порядок організації та проведення експертизи. Порядок надання Експертного висновку та Атестату. Особливості проведення експертиз КСЗІ державними органами. Особливості проведення експертизи шляхом декларації Літ.: [1] с.91-99; [5] с.124-123	2
	Тема 4. Супровід комплексної системи захисту інформації	**2**
16	**Супровід КСЗІ** План робіт із захисту інформації в ІТС. Контрольно-профілактичні заходи. Інженерно-технічні заходи. Задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем. Кадрові заходи. Забезпечення супроводу КСЗІ в ІКС. Контроль встановленого порядку оброблення інформації в ІКС. Основні вимоги до КЗЗ від НСД. НД ТЗІ 1.1-00299: безперервний захист, атрибути та диспетчер доступу, реєстрація дій, функції та механізми захисту, забезпечення послуг безпеки та гарантій їх реалізації. Вирішення задачі супроводу КСЗІ. Особливості супроводу КСЗІ в ІТС державних установ. Державний контроль за станом ТЗІ Літ.: [3] с.562-566; [6] с.134-154	2
	Разом:	**32**

5.2 Зміст лабораторних занять

№ з/п	Тема лабораторного заняття	Кількість годин
1	Аналіз структури об'єкту захисту та оцінка можливих загроз, уразливостей та дестабілізуючих чинників. Літ.:[1] с.6-16; [2] с.189-199; [3] с.19-27	4
2	Розроблення моделі порушника та загроз і реалізація політики інформаційної безпеки як етап проєктування КСЗІ. Літ.:[3] с.19-27; [6] с.12-22	4
3	Дослідження характеристик технічних засобів прослуховування інформації. Використання генераторів шуму для блокування витоку інформації. Літ.:[1] с.17-44; [2] с. 18-63, 83-90; [3] с.328-343, 516-527	4
4	Організація та використання систем відеомоніторингу контрольованої території. Літ.:[1] с.70-81, 126-128; [2] с.63-67	4
5	Утворення системи контролю і захисту приміщень на основі IoT пристроїв Xiaomi (модулів розумного будинку) та давачів охоронної сигналізації. Літ.: [2] с.199-250; [3] с. 527-548	4
6	Виявлення і вимірювання параметрів небезпечних сигналів та локалізація їх джерел. Методика та засоби виявлення закладних пристроїв. Літ.: [1] с.60-76; [2] с.87-138	4
7	Оцінка ефективності та рівня захищеності КСЗІ, документальний супровід КСЗІ (протокол випробувань комплексних систем захисту інформації, документація на етапі експлуатації КСЗІ) Літ.: [1] с.81-99; [2] с.189-198; [3] с.548-562	4
8	Впровадження та забезпечення функціонування комплексних систем захисту інформації, моніторинг роботи та технічний супровід. Літ.: [3] с.562-566; [11] с.134-154	4
9	Підсумкове заняття. Тестування	2
	Разом:	**34**

5.4 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів усіх форм здобуття освіти полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, тестування тощо. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. Крім цього, до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу. Отримання завдання на КП, підготовка до виконання ЛР1	5
2	Опрацювання теоретичного матеріалу, робота над КП, підготовка до захисту ЛР1.	7
3	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР2	7
4	Опрацювання теоретичного матеріалу, робота над КП, підготовка до захисту ЛР2	7
5	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР3	7
6	Опрацювання теоретичного матеріалу, робота над КП, підготовка до захисту ЛР3	7
7	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР4	7
8	Опрацювання теоретичного матеріалу, робота над КП, підготовка до захисту ЛР №4	7
9	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР5	7
10	Опрацювання теоретичного матеріалу, робота над КП, підготовка до захисту ЛР5	7
11	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР6	7
12	Опрацювання теоретичного матеріалу, робота над КП, підготовка до захисту ЛР6	7
13	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР7	7
14	Опрацювання теоретичного матеріалу, робота над КП, підготовка до захисту ЛР7	7
15	Опрацювання теоретичного матеріалу, робота над КП, підготовка до виконання ЛР8	7
16	Опрацювання теоретичного матеріалу, підготовка до захисту ЛР8. Підготовка до захисту КП	7
17	Опрацювання теоретичного матеріалу. Тестування.	4
	Разом:	**114**

***Примітки*:** КП – курсовий проєкт

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів. Зокрема, лекції проводяться з використанням словесних, наочних, інтерактивних та проблемних методів з супроводом мультимедійних технологій та презентаційних матеріалів; лабораторні роботи – з використанням практичних та частково-пошукових методів, методів проєктної діяльності із застосуванням сучасних інформаційно-комп'ютерних технологій; самостійна робота – з використанням пояснювально-ілюстративних та частково-пошукових методів.

7. Методи контролю

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

– оцінювання результатів захисту лабораторних робіт;

– тестовий контроль засвоєння теоретичного та практичного матеріалу дисципліни.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, ***не допускається*** до семестрового контролю, поки не виконає обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) з усіх видів поточного контролю і не склав іспит, вважається таким, який ***має*** академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних занять та захисту лабораторних робіт (вивчення теоретичного матеріалу з теми роботи, попередню підготовку протоколу роботи, підготовку до усного опитування для допуску до заняття), активно працювати на лабораторних заняттях, якісно підготувати звіт (схемні рішення і протокол роботи відповідно до теми), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами завдань тощо. Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо студент захистив її на наступному після виконання роботи занятті. Пропущене лабораторне заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час лабораторних занять, тестуванням, під час захисту курсового проєкту та семестрового контролю.

Здобувач вищої освіти, виконуючи завдання лабораторних занять і курсового проєкту з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах, які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	Узагальнений зміст критерія оцінювання
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними приладами та інструментами, прикладними програмами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів

Аудиторна робота								Контрольні заходи	Семестровий контроль	
Лабораторні роботи:								Тестовий контроль:	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т 1-4		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100**
24-40								**12-20**	**24-40**	

Примітки: *За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Навчальним планом дисципліни передбачено курсовий проект, на виконання якого виділяється 2 кредити ЄКТС (60 год.) самостійної роботи студента під керівництвом викладача та з консультуванням за графіком.

Згідно з навчальним планом підготовки бакалаврів за спеціальністю «Кібербезпека» курсовий проєкт виконується у 7 семестрі поетапно, відповідно до календарного плану.

Завдання на курсовий проєкт базується на матеріалі, який опрацьовується під час лекційних, лабораторних та самостійних занять в ході вивчення дисципліни. Тематика курсового проєкту пов'язана з майбутньою спеціальністю студентів. В курсовому проєкті студент повинен показати свої знання в галузі проєктування комплексних систем захисту інформації в кіберпросторі. Крім того, в якості об'єкту для курсового проєкту можуть бути дослідження та впровадження відомих технології проєктування засобів захисту, реалізація тестових програм тощо.

Об'єктом дослідження для курсового проєкту рекомендується обрати підприємство, на якому студент проходив проєктно-технологічну практику. Заохочуються пропозиції студентів щодо самостійного, за узгодженням з викладачем, вибору теми курсового проєкту. Самостійний вибір предметної області, в якій доцільно створювати КСЗІ, дозволяє зробити висновок щодо рівня творчої активності студента, його вміння самостійно здійснити попередній аналіз предметної області і розробити технічне завдання.

При виконанні курсового проєкту обов'язково повинні бути використані такі елементи:

- аналіз об'єкта захисту відповідно до НД ТЗІ 3.7-001-2005;
- розробка моделі загроз;
- розробка моделі порушника;
- розробка політики безпеки;
- аналіз інженерно-технічних, апаратних та програмних засобів захисту інформації;
- синтез оптимальної КСЗІ;
- розробка документації на етапах впровадження і супроводу.

Календарний план виконання курсового проєкту

Зміст етапу	Термін виконання
1 Вибір та затвердження теми курсового проєкту; розробка завдання на курсовий проєкт; складання календарного графіка виконання курсового проєкту	1-2 тиждень
2 Аналіз об'єкта захисту та аналіз захищеності його інформації від несанкціонованого втручання	3-4 тиждень
3 Аналіз та опис наявної системи захисту інформації	5-8 тиждень
4 Проєктування пропонованої КСЗІ	9-12 тиждень
5 Написання тексту пояснювальної записки та розробка графічних матеріалів	13-14 тиждень
6 Остаточне коригування курсового проєкту з урахуванням зауважень керівника; оформлення курсового проєкту, як документа відповідно до вимог	15 тиждень
7 Підготовка до захисту та захист курсового проєкту	16 тиждень

Розробка повинна бути представлена у вигляді моделі КСЗІ і супроводжуватись пояснювальною запискою, яка б повинна бути обсягом ***50-60 сторінок*** і рекомендовано містила в собі такі елементи:

- загальний аналіз об'єкта захисту, аналіз концептуальних вимог та інформаційних потреб для конкретної предметної області;
- виявлення інформаційних об'єктів та зв'язків між ними;
- побудова концептуальної схеми предметної області;
- аналіз загроз та ризиків для інформаційно-комунікаційної системи підприємства, оцінка ступеню загрози інформації, що захищається;
- моделювання можливих каналів витоку інформації;
- аналіз інженерно-технічних, апаратних та програмних засобів захисту інформаційних ресурсів підприємства та вибір оптимальних;
- розробка технічного завдання для системи захисту
- технічний проєкт системи захисту щодо розробки загальних рішень по системі та її частинах, функціональній і організаційних структурах, функціях персоналу, по структурі та складу технічних засобів, постановках і алгоритмах розв'язання задач, мовах, які застосовуються, по організації та веденню бази даних, системі класифікації та кодування інформації, програмному забезпеченню, розробці плану організаційних заходів щодо підготовки об'єкта до введення системи в дію, по правовому забезпеченню;
- робочий проєкт системи захисту, який включає програмно-апаратну реалізацію системи захисту та оформлення відповідної робочої документації;
- розробка заходів з технічного захисту інформації на об'єкті захисту;
- розробка моделі охоронної та пожежної сигналізації об'єкта (приміщення), систтеми відеоспостереження, тощо;
- розрахунок зон поширення акустичних і електромагнітних хвиль з об'єкта захисту з масштабною прив'язкою на місцевості;
- аналіз роботи та випробовування розробленої системи захисту та доведення ефективності та коректності її функціонування;
- оцінка ступеня захисту інформації на об'єкті;
- розробку відповідної документації на етапі впровадження і супроводу;
- формулювання рекомендацій по роботі з засобом (інструкції з технічного обслуговування, інструкції системному адміністратору, інструкції користувачу- оператору).

Вибір необхідних розділів курсового проєкту узгоджується з керівником і повинен бути адаптований до тематики курсового проєкту.

Як результат виконання курсового проєкту є розробка графічної частини, яка демонструє основні результати виконаної розробки ***(5 креслень)***

В курсовому проєкті обов'язковими є два креслення:

1) Схема інформаційних потоків;
2) Схема структурна КСЗІ ІТС підприємства.

Інші вибираються довільно, щоб розкрити суть проєкту, напрклад:

- схему структурну мережі підприємства;
- модель загроз;
- модель порушника;
- алгоритм захисту мережі підприємства;
- схему роботи системи захисту;
- рівні інтеграції різних елементів інтегрованої КСЗІ;
- алгоритми обчислень в системі;
- архітектуру системи захисту
- структурну схема охоронно-пожежної сигналізації:
- структурну схему системи відеонагляду, тощо.

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; повнота відповіді та знання методів проєктування комплексних систем захисту інформації тощо.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів тестового контролю

Тест, передбачений робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	0-59	60	65	70	75	80	85	90	95	100
Кількість отриманих балів	0	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали*** **(середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	6	8	10
Теоретичне питання № 2	6	8	10
Практичне завдання	12	16	20
Разом:	**24**		**40**

Примітка. *Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна оцінка** (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом ***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
C	73-82		
D	66-72		
E	60-65		
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

10. Питання для самоконтролю результатів навчання

1. Організаційні основи розробки проектів, реалізації та модернізації захищених інформаційних і комунікаційних систем.
2. Соціальні та морально етичні норми колективного розроблення проектів.
3. Правові норми організації роботи колективу для розробки проектів.
4. Оптимізація співробітництва у колективі при розробці проектів.
5. Загальна технологія розробки комплексів засобів захисту інформаційно-комунікаційних систем.
6. Індикатори електромагнітних випромінювань.
7. Радіочастотоміри.
8. Автоматизовані пошукові комплекси.
9. Мобільні пошукові комплекси.
10. Скануючі приймачі.
11. Спеціалізоване програмне забезпечення.
12. Тепловізорні засоби.
13. Стаціонарні комплекси автоматичного виявлення радіомікрофонів.
14. Типові методи та прийоми проектування захищених інформаційних та комунікаційних систем.
15. Засоби захисту для складових КСЗІ.
16. Класифікація джерела загроз та загроз ~~и~~ інформації.
17. Сутність технічного каналу витоку інформації.
18. Загальна класифікація каналів витоку інформації.
19. Електромагнітні канали витоку інформації.
20. Електричні канали витоку інформації.
21. Параметричні канали витоку інформації.
22. Повітряні канали витоку акустичної інформації.
23. Вібраційні канали витоку акустичної інформації.
24. Електроакустичні канали витоку акустичної інформації.
25. Оптико-електронний канал витоку акустичної інформації, його характеристика, методи блокування.
26. Індукційний метод перехоплення інформації при її передачі по каналах зв'язку.
27. Класифікація, принцип роботи акустичних закладок.
28. Класифікація, принцип роботи віброакустичних закладок.
29. Класифікація, принцип роботи спрямованих мікрофонів.
30. Класифікація, принцип роботи панорамних скануючих приймачів.
31. Класифікація, принцип роботи аналізаторів спектру та пеленгаторів.
32. Програмно-апаратні комплекси радіо-, радіотехнічної розвідки.
33. Засоби візуальної розвідки.
34. Системи спостереження за транспортними засобами. Радіомаяки. Радіонавігаційний приймач.
35. Класифікація методів та засобів захисту інформації від витоку технічними каналами.
36. Засоби виявлення, локалізації і нейтралізації закладних пристроїв.
37. Основні вимоги до структури і параметрів засобів радіомоніторингу при захисті мовної інформації.
38. Пасивні методи та засоби захисту інформації.
39. Активні методи та засоби захисту інформації.
40. Методи та засоби виявлення та подавлення диктофонів.
41. Методи і засоби пошуку електронних закладних засобів.
42. Методи пошуку закладок з використанням індикаторів поля, інтерсепторів і радіочастотомірів.
43. Методи пошуку закладок з використанням нелінійних локаторів, виявлячі порожнеч (пустот), металошукачів і рентгенівських апаратів
44. Засоби пошуку пристроїв перехоплення інформації. Сканерні приймачі й аналізатори спектру.
45. Програмно-апаратні та спеціальні комплекси контролю сигналів.
46. Засоби пошуку пристроїв перехоплення інформації, що використовують фізичні властивості навколишнього середовища.
47. Методи пошуку закладок з використанням металошукачів.
48. Види спеціальних перевірок виділених приміщень.
49. Державне ліцензування діяльності в області захисту інформації.
50. Сертифікація засобів захисту інформації. Основні поняття.
51. Атестування об'єктів інформатизації. Основні поняття.
52. Основні рекомендації щодо захисту інформації від витоку технічними каналами на об'єктах ТЗПІ при розробці технічного проекту
53. Етапи розробки проекту комплексу засобів захисту інформаційно-комунікаційної системи.
54. Принципи адаптації можливостей комплексу засобів захисту до вимог стандартів.
55. Вимоги нормативних документів щодо створення КСЗІ в ІТС
56. Етапи побудови комплексної системи захисту інформації
57. Комплексні системи захисту інформації: призначення, принципи, стратегії
58. Середовища функціонування ІТС. Вміст передпроєктних робіт щодо створення КСЗІ. Порядок розробки і вміст нормативно-розпорядчої документації передпроєктної стадії робіт.
59. Порядок розробки і вміст документів ескізного проекту, робочого та технічного проекту КСЗІ
60. Порядок створення комплексу технічного захисту інформації в ІТС.
61. Принципи розробки та методики випробувань КСЗІ.
62. Практика введення в дію КСЗІ.
63. Види експертизи та її проведення на реальних об'єктах.
64. Процедура впровадження КСЗІ.
65. Супровід КСЗІ в ІТС
66. Складання програм випробувань КСЗІ та розробка методик проведення випробувань.
67. Методи оцінки захищеності інформаційно-комунікаційних систем

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Компонентна база і схемотехніка систем захисту» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Компонентна база і схемотехніка систем захисту». https://msn.khmnu.edu.ua/course/view.php?id=6709

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК або ноутбук, проєктор. Програмне забезпечення: пакет схемотехнічного моделювання цифрових, аналогових та аналогово-цифрових електронних схем Electronics Workbench.

13. Рекомендована література

Основна

1. Системи захисту інформації : підручник / Ю.В. Костюк, П.М. Складанний, Г.М. Гулак, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 887 с. URL: https://elibrary.kubg.edu.ua/id/eprint/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf (дата звернення: 22.08.2025)
2. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с. URL: https://elartu.tntu.edu.ua/handle/lib/42625 (дата звернення: 22.08.2025)
3. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк та ін. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с. URL: https://elibrary.kubg.edu.ua/id/eprint/51358/1/Kostiuk_Y_Skladannyi_P_Bebeshko_B_Khorolska_K_Rzaieva_S_Vorokhob_M_BIKS_2025_FITM.pdf (дата звернення: 22.08.2025)
4. Хлапонін Ю.І. Комплексні системи захисту інформації: конспект лекцій. Київ: КНУБА, 2022. 84 с. URL: https://repositary.knuba.edu.ua/server/api/core/bitstreams/6b05fa85-b573-4300-ad40-45b63e198ffa/content (дата звернення: 22.08.2025)
5. Комплексні системи захисту інформації : Навчальний посібник [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. URL: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/ (дата звернення: 22.08.2025)
6. Технічний захист інформації: Навч. погіб. в 2 ч. Ч. 1: Основи технічного захисту інформації / В.М.Богуш, В. Д. Бровко, О.С.Кобус, В.Д. Козюра. Київ: Видавництво Ліра-К, 2022. 286с.
7. Методи та засоби технічного захисту інформації. Опорний конспект лекцій навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека» / уклад.: В. М. Луценко, Д. О. Прогонов. Київ : КПІ ім. Ігоря Сікорського, 2021. 289 с. URL: https://ela.kpi.ua/handle/123456789/42397 (дата звернення: 22.08.2025)
8. Технічні засоби захисту інформації: Опорний конспект лекцій з дисципліни для студентів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Яцків В.В., Кулина С.В. Тернопіль 2023. 88 с. URL: https://dspace.wunu.edu.ua/bitstream/316497/49114/1/Технічні%20засоби%20захисту%20інформації.pdf (дата звернення: 22.08.2025)

Додаткова

9. Campbell T. Practical Information Security Management: A Complete Guide to Planning and Implementation. Australia: Burns Beach, 2016. 253 p.
10. Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice / Elias G. Carayannis, David F. J. Campbell, Marios Panagiotis Efthymiopoulos. New York : Springer, 2014. 360 p.
11. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.
12. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар - Чернівці: Чернівецький національний університет, 2018. 252 с
13. Інформаційна безпека: навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.
14. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. Хмельницький: ХмНУ, 2021. 196 с.
15. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. Cham, Switzerland : Springer, 2018. 174 p.
16. Інформаційна безпека держави: навчальний посібник/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
17. Fundamentals of InformationSystems Security / Editors : David Kim, Michael G. Solomon. Burlington, Massachusetts : Jones & Bartlett Learning, 2018. 548 p.
18. Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software Level / Editors : Michael Schwartz, Maciej Machulak. Apress, 2018. 377 p.

19. Security and Privacy inInternet of Things (IoTs): Models, Algorithms, and Implementations / Edited by Fei Hu**.** Taylor & Francis Group, 2016**.** 564 p.

20. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level / Editors : Robert M. Clark, Simon Hakim. Cham, Switzerland : Springer, 2016. 360 p.

21. Гребенніков В.В. Комплексні системи захисту інформації: проєктування, впровадження, супровід. / В.В. Гребенніков Ужгород: Ужгородський національний університет, 2013. 161 с.

22. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Чинний від 28 квітня 1999 р. Київ : ДСТСЗІ СБ, 1999. 35с.

23. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Чинний від 20 грудня 2000 р. Київ : ДСТСЗІ СБ, 2000. 8с.

24. НД ТЗІ 3.7-003 -2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Чинний від 28 листопада 2005 р. Київ : ДСТСЗІ СБ, 2005. 22с.

25. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. Чинний від 12 грудня 2007 р. Київ : ДСТСЗІ СБ, 2007. 7с.

26. НД ТЗІ 3.3-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. Чинний від 12 грудня 2007 р. – Київ : ДСТСЗІ СБ, 2007. 9с.

27. НД ТЗІ 2.7-011-2012. Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. Чинний від 23 липня 2012 р. Київ : Адміністрація Держспецзв'язку, 2012. 18с.

28. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Чинний від 25 березня 2011 р. Київ : Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2011. 130с.

29. Микитишин А. Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. Тернопіль: ТНТУ, 2016. 255 с

30. Stephen Sakawa Kibwage. Role-Based Access Control Administration of Security Policies and Policy Conflict Resolution in Distributed Systems. A Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems Graduate School of Computer and Information Sciences. Nova Southeastern University, 2015. 111 p.

31. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions/ Hend K. Alkahtani. Computer and Information Science. Vol. 12, No. 2; 2019. Published by Canadian Center of Science and Education. P. 117-125.

32. The Development of an Intelligent Complex of Radiation-Technological Control of a Safety Barrier / S. Lienkov, O. Banzak, Y. Husak, I. Muliar, V. Cheshun, E. Lenkov // International Journal of Emerging Trends in Engineering Research. Volume 8. No. 7, July 2020. P. 3483–3486.

33. Методи та засоби захисту інформації / Al-Ammouri A., Dekhtyar M., Ishchenko R., Klochan E. Системи управління, навігації та зв'язку. Збірник наукових праць. 2024. №1. С. 38-44. URL: https://journals.nupp.edu.ua/sunz/article/view/3265 (дата звернення: 22.08.2025).

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=6709
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (*бакалаврський*)
Мова викладання	Українська
Семестр	Четвертий
Кількість призначених кредитів ЄКТС	6,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: *аналізувати, виявляти та оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам та *проводити оцінку* ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки, *здійснювати* оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.), *реалізовувати* комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів, *вирішувати* задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки *використовувати* інформаційно-комунікаційні технології, сучасні методи і моделі інформаційної безпеки та/або кібербезпеки, *вирішувати* задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; *використовувати* програмні та програмно-апаратні комплекси засобів захисту інформаційних ресурсів в інформаційно-телекомунікаційних (автоматизованих) системах, *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень, *застосовувати* методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки, *вирішувати* задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах, *виконувати* моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки, *виявляти* небезпечні сигнали технічних засобів і *вимірювати* параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації, *інтерпретувати* результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації; *виконувати* пошук, оброблення, аналіз та синтез інформації з різних джерел державною та іноземними мовами і *використовувати* отримані результати для ефективного рішення спеціалізованих задач дисципліни і професійної діяльності; *забезпечувати* введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту, ефективність професійної комунікації в задачах проєктування, впровадження та супроводу комплексних систем захисту інформації.

Зміст навчальної дисципліни. Визначення комплексних систем захисту інформації (КСЗІ), їх мета, задачі та принципи побудови. Вимоги законодавства України та нормативних документів щодо захисту інформації в КСЗІ. Види захисту в КСЗІ: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні) та програмні засоби й методи захисту. Етапи створення КСЗІ: обстеження інформаційних систем, розробка моделі загроз і моделі порушника, формування політики безпеки та технічного завдання. Забезпечення конфіденційності, цілісності та доступності інформації (CIA Triad). Організаційні заходи: роль політик безпеки, організаційної структури, управління персоналом та процедур безпеки. Інженерно-технічні заходи: використання спеціалізованих програмно-апаратних засобів для захисту даних та систем.

Пререквізити: компонентна база і схемотехніка систем захисту; нормативно-правове забезпечення кібербезпеки; адміністрування та захист баз і сховищ даних; системи контролю доступу; безпека безпроводових технологій та інтернету речей; технічний і криптографічний захист інформації; захист інформації в інформаційно-комунікаційних системах; безпека вебресурсів; управління інформаційною безпекою; технології виявлення вразливостей та вторгнень; проектно-технологічна практика; моделювання систем захисту даних, оцінка ризиків і прийняття рішень.

Кореквізити: переддипломна практика.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для ***першого*** (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних, інтерактивних та проблемних методів); лабораторні роботи (з використанням практичних та частково-пошукових методів, методів проєктної діяльності); самостійна робота (з використанням пояснювально-ілюстративних та частково-пошукових методів).

Форми оцінювання результатів навчання: оцінювання на практичних заняттях; оцінювання результатів захисту лабораторних робіт; тестування; оцінювання результатів захисту курсового проєкту; оцінювання результатів підсумкового семестрового контролю (іспит).

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Системи захисту інформації : підручник / Ю.В. Костюк, П.М. Складанний, Г.М. Гулак, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 887 с.
2. Комплексна безпека інформаційних мережевих систем: навчальний посібник/ Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. Тернопіль: ФОП Паляниця В.А., 2023. 324 с.
3. Безпека інформаційно-комунікаційних систем : підручник / Ю.В. Костюк та ін. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с.
4. Хлапонін Ю.І. Комплексні системи захисту інформації: конспект лекцій. Київ: КНУБА, 2022. 84 с.
5. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. Хмельницький: ХмНУ, 2021. 117 с.
6. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=6709
7. Електронна бібліотека ХНУ. Доступ до ресурсу: http://library.khmnu.edu.ua/

Викладачі: канд. техн. наук, доцент Віктор Чешун, асистент Олена Зарицька.