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 – F Інформаційні технології
Спеціальність – F5 Кібербезпека та захист інформації
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека та захист інформації
Обсяг дисципліни – 16 кредитів ЄКТС
Шифр дисципліни – ОФП.12
Мова навчання – Українська
Статус дисципліни – Обов'язкова (фахової 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	3	6	5	150	50	16	34	-	-	100	-	-	+	-
Д	4	7	5	150	50	16	34	-	-	100	-	-	+	-
Д	4	8	6	180	66	32	-	**34**	-	114	-	-	-	+
Разом ДФН			**16**	**480**	**166**	**64**	**68**	**34**	**-**	**314**		**-**	**2**	**1**

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

Робоча програма складена _____ канд. техн. наук, доцент Ігор МУЛЯР
_____ 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) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності F5 «Кібербезпека та захист інформації».

Пререквізити: ОФП.04 Сигнали і процеси в системах захисту інформації; ОФП.05 Захист інформації в інформаційно-комунікаційних системах; ОФП.06 Захист інформації в інформаційно-комунікаційних системах (курсовий проєкт); ОФП.08 Нормативно-правове забезпечення кібербезпеки; ОФП.09 Прикладна криптологія; ОФП.10 Адміністрування та захист баз і сховищ даних; ОФП.11 Адміністрування та захист баз і сховищ даних (курсовий проєкт).

***Постреквізити*:** ОФП.16 Виробнича практика 2.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** ІК Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації; ЗК01 Здатність застосовувати знання у практичних ситуаціях; ЗК02 Знання та розуміння предметної області і розуміння професійної діяльності; ЗК06 Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні; ФК01 Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності; ФК02 Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації; ФК04 Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації; ФК06. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо); ФК09 Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності; ФК10 Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

***програмних результатів навчання*:** ПРН04 Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН05 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; ПРН09 Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації; ПРН10 Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності; ПРН13 Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому; ПРН16 Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах; ПРН20 Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації; ПРН21 Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

***Мета дисципліни*.** Формування у здобувачів системних знань і практичних навичок для реалізації комплексного підходу у побудові систем захисту інформації відповідно до вимог законів та нормативних документів України та з урахуванням передових світових практик.

***Предмет дисципліни*.** Вимоги нормативно-правового забезпечення, методи, технології та засоби розробки, реалізації, впровадження, атестації, експлуатації і супроводу систем безпеки для реалізації комплексного підходу у захисті інформаційних ресурсів.

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 інформації відповідно 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

VI семестр

Назва теми	Кількість годин, відведених на:		
	лекції	**практичні заняття**	**СРС**
Тема 1. Архітектура та програмно-апаратне забезпечення систем контролювання доступу (СКД)	8	16	48
Тема 2. Інтеграція СКД в системи захисту	8	18	52
Разом:	**16**	**34**	**100**

VII семестр

Назва теми	Кількість годин, відведених на:		
	лекції	**лабораторні роботи**	**СРС**
Тема 1. Теоретичні основи та нормативна база технічного захисту інформації	4	4	16
Тема 2. Канали витоку, методи їх виявлення та перекриття	8	24	64
Тема 3. Технічні аспекти забезпечення цілісності та доступності	2	6	16
Тема 4. Атестація об'єктів та державна експертиза у сфері технічного захисту інформації	2	-	4
Разом:	**16**	**34**	**100**

VIII семестр

Назва теми	Кількість годин, відведених на:		
	лекції	**практичні заняття**	**СРС**
Тема 1. Теоретичні основи та нормативна база технічного захисту інформації	8	8	28
Тема 2. Канали витоку, методи їх виявлення та перекриття	14	14	48
Тема 3. Технічні аспекти забезпечення цілісності та доступності	4	4	14
Тема 4. Атестація об'єктів та державна експертиза у сфері технічного захисту інформації	6	8	24
Разом:	**32**	**34**	**114**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Перелік лекцій (VI семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Архітектура та програмно-апаратне забезпечення систем контролювання доступу		**8**
1	**Вступ у системи контролювання доступу (СКД)** Поняття доступу, цілі та класифікація систем контролювання доступу; огляд загроз і вимог до систем (конфіденційність, цілісність, доступність); історія і сучасні тренди (ідентифікація, аутентифікація, авторизація, аудит). Визначення, позначення та скорочення. Поняття та призначення СКД. Класифікація СКД за типами, архітектурою та сферами застосування. Практичні приклади з реальних IT/фізичних систем. СКД для критичної інфраструктури. Літ.: [1] с. 8-25; [2] с. 207-275; [3] с. 3-69; [5] с. 5-62; [6] с. 11-69; [8] с. 7-19; 202-211, 214-246; [24]	2
2	**Технології ідентифікації та аутентифікації в СКД** Методи ідентифікації користувачів: картки proximity, смарт-карти, біометрія Технології RFID: низькочастотні (125 кГц), високочастотні (13,56 МГц), UHF. Біометричні методи: відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки. Багатофакторна аутентифікація в системах фізичного доступу. Мобільні технології ідентифікації (NFC, Bluetooth, смартфони як ключі). Стандарти ідентифікаційних технологій (MIFARE, DESFire, iClass) Літ.: [1] с. 133-157; [2] с. 571-639; [3] с. 127-149; [7] с. 115-135; [8] с. 139-149; [17, 18]; [20]; [23]	2
3	**Програмно-апаратна архітектура систем контролювання доступу** Апаратні компоненти СКД: контролери, зчитувачі, замки, турнікети. Програмне забезпечення для управління СКД: серверне та клієнтське ПЗ. Протоколи обміну даними між компонентами системи (Wiegand, OSDP, RS-485). Мережева інфраструктура СКД: топології, кабельні системи, безпровідні рішення. Інтелектуальні контролери доступу та їх функціональні можливості. Розподілені та централізовані архітектури СКД. Пожежна та охорона сигналізація. Літ.: [1] с. 61-111; [2] с. 315-570; [4] с. 8-27; 125-175, 211-260; [24]	2
4	**Проєктування та впровадження фізичних систем контролювання доступу** Методологія проєктування СКД для різних об'єктів. Аналіз ризиків та визначення рівнів безпеки. Зонування об'єктів та політики контролювання доступу. Вибір обладнання відповідно до умов експлуатації. Організація проходів: турнікети, шлюзові кабіни, обертові двері. Електроживлення та резервування систем. Літ.: [2] с. 114-123; [11]; [2] с. 965-1015; [3] с. 127-161; [6] с. 211-245	2
Тема 2. Інтеграція СКД в системи захисту		**8**
5	**Інтеграція СКД з системами відеоспостереження** Архітектура та загальні особливості операційних центрів безпеки (SOC). Команда реагування на комп'ютерні надзвичайні події. CERT-UA. Архітектура інтегрованих систем безпеки. Протоколи інтеграції: ONVIF, SDK виробників, API. Синхронізація подій контролювання доступу з відеопотоками. Відеоверифікація проходів та розпізнавання обличчя. Інтелектуальна відеоаналітика для СКД. Системи управління відео (VMS) у складі інтегрованих рішень Зберігання та архівування даних з камер та СКД Літ.: [12]; [19]; [22];	2
6	**Інтеграція СКД з IoT та розумними будинками** Концепція Internet of Things та її застосування в СКД. Протоколи IoT: MQTT, CoAP, BACnet, KNX для систем контролювання доступу. Бездротові технології: Zigbee, Z-Wave, LoRaWAN в контексті СКД. Інтеграція з системами управління будівлями (BMS). Розумні замки та автоматизація приміщень на основі даних СКД. Edge computing та туманні обчислення в розподілених СКД. Кібербезпека IoT-компонентів систем контролювання доступу Літ.: [1] с. 25-60, 172-221; [10]; [13]; [15]; [19];	2
7	**Хмарні технології та мобільні рішення в СКД** Хмарні платформи для управління контролем доступу. Архітектура SaaS-рішень для СКД. Мобільні додатки для користувачів та адміністраторів. Віддалене управління та моніторинг систем. Безпека даних у хмарних СКД: шифрування, авторизація, аудит. Гібридні рішення: локальне та хмарне управління. Масштабованість та економічна ефективність хмарних СКД Літ.: [1] с. 224-259; [7] с. 166-117; [10]; [11]; [16];	2
8	**Кібербезпека, захист даних та майбутнє систем контролювання доступу** Загрози інформаційної безпеки для СКД. Матриця атак MITRE ATT&CK® Matrix for ICS. Захист від несанкціонованого доступу та кібератак. Відповідність вимогам GDPR та захист персональних даних. Аудит та моніторинг безпеки систем контролювання доступу. Штучний інтелект та машинне навчання в СКД. Блокчейн-технології для систем контролювання доступу. Правові і етичні аспекти. Літ.: [1] с. 111-131; [10]; [13, 14]; [21];	2
	Разом за семестр:	**16**

Перелік лекцій (VII семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Теоретичні основи та нормативна база технічного захисту інформації		**4**
1	**Теоретична та нормативна база технічного захисту інформації** 1. Поняття технічного захисту інформації (ТЗІ). Мета, завдання та об'єкти ТЗІ. 2. Роль ТЗІ в державній системі кібербезпеки. 3. Нормативно-правова база ТЗІ(законодавче регулювання ТЗІ, державні стандарти у сфері ТЗІ, система нормативних документів ТЗІ). 4. Основні терміни і визначення (згідно з ДСТУ 3396.0–96). 5. Суб'єкти діяльності у сфері ТЗІ. 6. Повноваження Держспецзв'язку України. 7. Ліцензування діяльності у сфері ТЗІ. Літ.: [1]; [2]; [4]; [6]	2
2	**Класифікація інформації, що підлягає захисту, загроз і каналів витоку інформації** 1. Класифікація інформації, що підлягає захисту. 2. Загальні характеристики витоку інформації. 3. Вплив зовнішніх факторів на безпеку інформації. 4.Класифікація загроз і каналів витоку інформації (Класифікація за фізичною природою сигналів. Електромагнітні, акустичні, оптичні та вібраційні канали.) 5.Оцінка потенційних загроз. Літ.: [12]; [14]	2
Тема 2. Канали витоку, методи їх виявлення та перекриття		**8**
3	**Акустичні та віброакустичні канали витоку** 1.Механізм утворення акустичних каналів. 2. Механізм утворення віброакустичних каналів. 3. Технічні засоби акустичної розвідки (мікрофони, диктофони, стетоскопи) та їх характеристики. 4. Канали витоку через архітектурно-будівельні конструкції. 5. Методи пасивного захисту акустичної інформації (екранування, звукоізоляція). 6. Вимоги до захищених приміщень. 7. Засоби контролю акустичної захищеності. 3. Використання активних та пасивних засобів для захисту від акустичної розвідки. Літ.: [3]; [5]; [6]; [7]	2
4	**Оптичні та лазерні канали витоку** 1. Принцип дії оптичних каналів спостереження. 2. Витік через відбиття світла, лазерні мікрофони. 3. Методи захисту від лазерного знімання. 4. Використання оптичних фільтрів та екранів. 5. Методи та засоби виявлення лазерних каналів витоку. Літ.: [13]; [14]	2
5	**Електромагнітні канали витоку інформації** 1. Радіоканали витоку. 2. Виявлення закладних пристроїв. 3. Захист бездротових мереж. 4. Визначення та фізична природа побічних електромагнітних випромінювань і наведень (ПЕМВН). 5. Джерела побічних електромагнітних випромінювань (особливості комп'ютерної техніки). 6. Технічні засоби контролю та виявлення ПЕМВН. 7. Методи та засоби пасивного захисту (екранування)./Методи екранування та фільтрації. 8. Засоби активного захисту. Літ.: [3]; [6]; [7]; [8]	2
6	**Канали витоку через провідні лінії** 1. Канали витоку через провідні лінії зв'язку (телефонні; локальні мережі). 2. Методи перехоплення (індуктивний; ємнісний; гальванічний). 3. Технічні засоби захисту ліній: фільтрація; гальванічна розв'язка; високочастотне зашумлення; шифрування каналів. 4. Захист волоконно-оптичних ліній зв'язку. Літ.: [3]; [5]; [6]; [9]	2
Тема 3. Технічні аспекти забезпечення цілісності та доступності		**2**
7	**Технічні аспекти забезпечення цілісності та доступності** 1. Захист від електромагнітного імпульсу (ЕМІ). 2. Системи безперебійного живлення (ДБЖ) та їхнє застосування. 3. Технічні засоби резервування та відновлення даних. 4. Вимоги до стійкості обладнання до зовнішніх впливів. 5. Захист від промислового шпигунства (фізична безпека серверних). Літ.: [4]; [5]; [9]	2

Тема 4. Атестація об'єктів та державна експертиза у сфері технічного захисту інформації		**2**
8	**Атестація об'єктів та державна експертиза у сфері технічного захисту інформації** 1. Порядок проведення атестації об'єктів, де обробляється інформація з обмеженим доступом. 2. Вимоги до експлуатаційної документації. 3. Роль державної експертизи у сфері ТЗІ. 4. Особливості сертифікації засобів ТЗІ. Літ.: [1]; [6]	2
	Разом за семестр:	**16**

Перелік лекцій (VIII семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Концептуальні та нормативні основи комплексних систем захисту інформації		**8**
1	**Нормативно-правове регулювання комплексних систем захисту інформації в Україні** 1. Вимоги Законів України щодо застосування комплексних систем захисту інформації (КСЗІ). 2. Постанови КМУ щодо КСЗІ. 3. Роль Держспецзв'язку як уповноваженого органу. 4. Регламентація КСЗІ в системі нормативних документів технічного захисту інформації (НД ТЗІ). 5. Наказ СБУ № 1132 від 22.07.2019. Літ.: [1]; [2]; [5]	2
2	**Концептуальні основи комплексних систем захисту інформації** 1. Визначення та завдання комплексних систем захисту інформації. 2. Основні властивості інформації: конфіденційність, цілісність, доступність. 3. Життєвий цикл ІКС та місце ЗІ в ньому. 4. Класифікація загроз та їхні джерела. Літ.: [1]; [2]; [4]; [7]	2
3	**Етапи створення комплексних систем захисту інформації** 1. Етап обстеження та формування вимог. 2. Етап проєктування. 3. Етап впровадження (Створення). 4. Етап атестації та введення в дію. 5. Етап супроводження та модернізації. Літ.: [1]; [2]; [4]; [7]	2
4	**Класифікація інформаційно-комунікаційних систем та вимоги до комплексних систем захисту інформації** 1. Методика класифікації ІКС за рівнем важливості інформації. 2. Визначення та обґрунтування класу захищеності КСЗІ відповідно до НД ТЗІ. 3. Загальні вимоги до КСЗІ різних класів. 4. Об'єкти, що обов'язково потребують КСЗІ. Літ.: [3]; [4]; [5]	2
Тема 2. Документальний супровід робіт зі створення та експлуатації комплексних систем захисту інформації		**14**
5	**Організаційно-розпорядча документація** 1. Наказ про створення КСЗІ та робочої групи (або комісії з КСЗІ). 3. Положення про службу (підрозділ) захисту інформації (або призначення Адміністратора безпеки). 4. Протокол (Рішення) про введення КСЗІ в дію. Літ.: [15]	2
6	**Технічне завдання на створення КСЗІ** 1. Технічне завдання (ТЗ) на створення (модернізацію) КСЗІ. 2. Акт класифікації ІКС (як обґрунтування вимог до класу захищеності). 3. Модель загроз і порушника. Літ.: [15]	2
7	**Політика інформаційної безпеки** 1. Політика інформаційної безпеки (ПІБ). 2. Концепція захисту інформації. Літ.: [15]	2
8	**План захисту інформації (ПЗІ)** 1. План захисту інформації (перелік заходів, терміни, відповідальні). 2. План управління ризиками (RMP) або План обробки ризиків. Літ.: [15]	2

9	**Техноробочий проєкт КСЗІ** 1. Технічний проєкт КСЗІ. 2. Порядок розробки проекту КСЗІ. 3. Ескізний проект КСЗІ. 4. Технічний проект КСЗІ. 5. Робочий проєкт КСЗІ. 6. Техноробочий проект КСЗІ. 7. Специфікація засобів захисту (повний перелік технічних і програмних засобів). 8. Програма і методики випробувань (ПМВ) КСЗІ. Літ.: [15]	2
10	**Експлуатаційна документація** 1. Положення про КСЗІ (як комплексний документ, що охоплює правила експлуатації та супроводу). 2. Інструкція адміністратора безпеки (ІАБ). 3. Інструкція користувача захищеної ІКС. 4. Інструкції щодо резервного копіювання, відновлення та реагування на інциденти. Літ.: [15]	2
11	**Заходи захисту (як окрема категорія документів)** 1. Декларація про застосовність (SoA, Statement of Applicability) (частіше вимога ISO, але корисна для обліку). 2. Протоколи вимірювань ПЕМВН та акустичних шумів (для ТЗІ). 3. Протоколи випробувань КСЗІ (за результатами виконаних ПМВ). 4. Архівування та зберігання документації. 5. Підтримка КСЗІ на етапі експлуатації. Літ.: [16]	2
	Тема 3. Експлуатація та супровід комплексних систем захисту інформації	**4**
12	**Управління конфігурацією та змінами в КСЗІ** 1. Необхідність управління конфігурацією (CM). 2. Процедури реєстрації та контролю змін у компонентах КСЗІ. 3. Оцінка впливу змін на безпеку системи. 4. Підтримка актуальності документації КСЗІ. 5. Використання систем CMDB (Configuration Management Database). Літ.: [3]; [5]	2
13	**Реагування на інциденти інформаційної безпеки** 1. Визначення інциденту, критерії класифікації. 2. Етапи реагування: локалізація, відновлення, аналіз. 3. Взаємодія з CERT-UA та галузевими центрами. 4. Формування Плану реагування та звітності про інциденти. Літ.: [2]; [5]; [7]	2
	Тема 4. Авторизація з безпеки	**6**
14	**Нормативно-правові основи авторизації з безпеки та перехід до ризик-орієнтованої моделі** 1. Закон України № 4336-IX (2025 р.) та нова архітектура кіберзахисту. 2. Гармонізація українського законодавства з ISO/IEC 27001 та NIST SP 800-5.3. 3. Постанова КМУ № 712 (1.8.0.6.2025): визначення та мета авторизації з безпеки (АЗБ); сфера застосування Постанови та об'єкти АЗБ; принципи та етапи процедури АЗБ; відповідальність керівників за рішення про АЗБ. Літ.: [18]	2
15	**Профілі безпеки** 1. Визначення та призначення Профілю безпеки. 2. Структура Профілю безпеки, компоненти та їх опис. 3. Базовий Профіль безпеки – сфера застосування та мінімальні вимоги. 4. Галузевий Профіль безпеки. Особливості формування для критичних секторів (енергетика, фінанси). 5. Цільовий Профіль безпеки: формування для конкретних систем. Літ.: [18]	2
16	**Процедура Авторизації з безпеки** 1. Розробка системи з безпеки та документації. 2. Оцінка (аудит) системи з безпеки. 3. Прийняття рішення про Авторизацію з безпеки. 4. Термін дії Авторизації та умови її продовження/скасування. 5. Формування та ведення Переліку авторизованих систем. Літ.: [18]	2
	Разом за семестр:	**32**

5.2 Зміст лабораторних робіт/практичних занять

Перелік лабораторних робіт (VI семестр)

№ з/п	Теми лабораторних робіт	Кількість годин
Тема 1. Архітектура та програмно-апаратне забезпечення систем контролювання доступу		**16**
1	Організація захисту інформації від несанкціонованого доступу в системах контролювання доступу із застосуванням програмного засобу ЛОЗА™-1	4
2	Застосування ЛОЗА™-1 як засобу неперервного автоматизованого ведення журналів реєстрації подій та інцидентів та аналіз журналів	4
3	Проєктування системи контролю доступом (апаратна частина)	4
4	Проєктування системи контролю доступом (програмна частина)	4
Тема 2. Інтеграція СКД в системи захисту		**12**
5	Організація та використання систем відеомоніторингу контрольованої території	4
6	Утворення системи контролю і захисту приміщень на основі IoT пристроїв Xiaomi (модулів розумного будинку) та давачів охоронної сигналізації	4
7	Створення IP-телефонної системи з використанням вільного програмного забезпечення (VoIP) на базі операційної системи Ubuntu та програмного забезпечення Asterisk	4
8	Дослідження та практичне застосування методології MITRE ATT&CK для аналізу і покращення безпеки систем контролювання доступу, а також розробка та оцінка вартості впровадження таких систем на підприємстві з використанням ZKTeco та інструментів для проектування IP-відеосистем	4
9	Підсумкове заняття. Тестування.	2
	Разом за семестр:	**34**

Перелік лабораторних робіт (VII семестр)

№ з/п	Теми лабораторних робіт	Кількість годин
	Тема 1. Теоретичні основи та нормативна база технічного захисту інформації	**4**
1	**Аналіз й ідентифікація каналів витоку та класифікація загроз** Складання матриці загроз та каналів витоку для типового офісного приміщення згідно вимог нормативно-технічної документації. Літ.: [1]; [6]	4
	Тема 2. Канали витоку, методи їх виявлення та перекриття	**24**
2	**Утворення та оцінка ефективності акустичного зашумлення** Вимірювання рівня природного та штучного акустичного фону у приміщенні. Налаштування та застосування генератора акустичного шуму. Вимірювання рівня перешкод у контрольованій зоні та оцінка ефективності захисту. Літ.: [5]; [7]	4
3	**Утворення та оцінка ефективності віброакустичного зашумлення** Вимірювання рівня природного та штучного акустичного фону у приміщенні. Налаштування та застосування генератора акустичного та вібраційного шумів. Оцінка ефективності захисту.	4
4	**Виявлення та перекриття оптичних та лазерних каналів витоку** Виявлення оптичних закладних пристроїв детектором відеокамер. Виявлення лазерних каналів витоку. Перекриття лазерних каналів витоку. Літ.: [15]	4
5	**Виявлення закладних пристроїв детекторами** Застосування детектора закладних пристроїв для виявлення прихованих засобів зйому інформації. Виявлення прихованих засобів зйому інформації металодетектором. Літ.: [15]	4
6	**Виявлення закладних пристроїв аналізатором спектра сигналів** Робота з аналізатором спектра. Виявлення активних частот та джерел їх походження. Оцінка екранів. Літ.: [15]	4
7	**Утворення зони контролю та захисту від побічних електромагнітних випромінювань** Вимірювання рівня електромагнітних випромінювань. Проведення розрахунку мінімально допустимої відстані до межі контрольованої зони на прикладі робочої станції. Застосування генератора шуму "БАЗАЛЬТ - 5ГЕШ" для захисту від побочних електромагнітних випромінювань. Літ.: [3]; [7]; [8]	4

	Тема 3. Технічні аспекти забезпечення цілісності та доступності	**6**
8	**Захист електроживлення** Моделювання каналу витоку через мережу 220В. Практичне застосування та оцінка ефективності гальванічної розв'язки. Дослідження принципів роботи мережевих фільтрів. Налагодження і захист системи безперебійного живлення. Літ.: [18]	6
9	Підсумкове заняття. Тестування.	2
	Разом за семестр:	**34**

Перелік практичних занять (VIII семестр)

№ з/п	Теми практичних занять	Кількість годин
	Тема 1. Концептуальні та нормативні основи комплексних систем захисту інформації	**8**
1	**Аналіз вимог нормативно-правового забезпечення комплексних систем захисту інформації** Літ.: [1]; [2]; [5]	2
2	**Обстеження середовищ функціонування інформаційно-комунікаційних систем** Обстеження обчислювальної системи. Обстеження інформаційного середовища. Обстеження фізичного середовища. Обстеження середовища користувачів. Літ.: НД ТЗІ 3.7-003 -2005	2
3	**Аналіз та класифікація загроз** Визначення та ранжування загроз для обраної ІКС . Класифікація загроз за моделями. Літ.: [4]; [7]	2
4	**Класифікація інформаційно-комунікаційних систем та визначення вимог до комплексних систем захисту інформації** Обґрунтування необхідності створення КСЗІ. Визначення класу захищеності ІКС Практичне застосування методики класифікації ІКС. Обґрунтування та визначення необхідного класу захищеності КСЗІ. Літ.: [3]; [4]	2
	Тема 2. Документальний супровід робіт зі створення та експлуатації комплексних систем захисту інформації	**14**
5	**Підготовка базової організаційно-розпорядчої документації** Підготовка наказів про створення КСЗІ та робочої групи (або комісії з КСЗІ). Розробка положення про службу (підрозділ) захисту інформації (або призначення Адміністратора безпеки). Літ.: [15]	2
6	**Формування технічного завдання на створення комплексної системи захисту інформації** Технічне завдання (ТЗ) на створення (модернізацію) КСЗІ. Акт класифікації ІКС (обґрунтування вимог до класу захищеності). Модель загроз і порушника. Літ.: [15]	2
7	**Розробка політики безпеки інформації в інформаційно-комунікаційній системі** Складання структури та ключових розділів ПІБ для організації. Визначення політик використання ресурсів. Літ.: [15]	2
8	**Складання плану захисту інформації (ПЗІ)** План захисту інформації (перелік заходів, терміни, відповідальні). План управління ризиками (RMP) або План обробки ризиків. Літ.: [15]	2
9	**Розробка технічного проєкту** Розробка технічного проєкту КСЗІ (схеми розміщення, логічна структура, специфікація обладнання). Розробка специфікації засобів захисту (повного переліку технічних і програмних засобів). Програма і методики випробувань (ПМВ) КСЗІ. Літ.: [15]	2
10	**Розробка експлуатаційної документації (накази і положення)** Підготовка наказу про введення КСЗІ в експлуатацію. Розробка положення про КСЗІ. Літ.: [15]	2
11	**Розробка експлуатаційної документації (інструкції)** Інструкція адміністратора безпеки (ІАБ). Інструкція користувача захищеної ІКС. Інструкції щодо резервного копіювання, відновлення та реагування на інциденти. Літ.: [16]	2
	Тема 3. Експлуатація та супровід комплексних систем захисту інформації	**4**
12	**Управління конфігурацією та змінами в КСЗІ** Реєстрація та контроль змін у компонентах КСЗІ. Оцінка впливу змін на безпеку системи. Підтримка актуальності документації КСЗІ. Літ.: [3]; [5]	2

13	**Реагування на інциденти інформаційної безпеки** Формування Плану реагування та звітності про інциденти. Літ.: [2]; [5]; [7]	2
	Тема 4. Авторизація з безпеки	**6**
14	**Аналіз вимог нормативно-правового забезпечення авторизації з безпеки** Літ.: [18]	2
15	**Формування профілю безпеки** Визначення Базового Профілю безпеки. Формування Цільового Профілю безпеки Літ.: [18]	2
16	**Формування пакету авторизаційної документації** Розробка плану управління ризиками Формування звіту про оцінку безпеки. Підготовка заяви про відповідність. Літ.: [18]	2
17	Підсумкове заняття. Тестування.	
	Разом за семестр:	**32**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, підготовці до практичних занять, 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.

Планування самостійної роботи на VI семестр

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №1.	6
2	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	6
3	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №2.	6
4	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	6
5	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №3.	6
6	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	6
7	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №4.	6
8	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	6
9	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №5.	6
10	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	6
11	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №6.	6
12	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	6
13	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №7.	6
14	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	6
15	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №8.	6
16	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	6
17	Узагальнення пройденого матеріалу. Підготовка до тестування.	4
	Разом за семестр:	100

Планування самостійної роботи на VII семестр

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №1.	6
2	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	6
3	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №2.	6
4	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	6
5	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №3.	6
6	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	6
7	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №4.	6
8	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	6
9	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №5.	6
10	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	6
11	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №6.	6
12	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	6
13	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №7.	6
14	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	6
15	Опрацювання теоретичного матеріалу. Підготовка до лабораторної роботи №8.	6
16	Опрацювання теоретичного матеріалу. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	6
17	Узагальнення пройденого матеріалу. Підготовка до тестування.	4
	Разом за семестр:	100

Планування самостійної роботи на VIII семестр

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №1, робота над завданнями практичного заняття.	6
2	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №2, робота над завданнями практичного заняття.	6
3	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №3, робота над завданнями практичного заняття.	7
4	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №4, робота над завданнями практичного заняття.	7
5	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №5, робота над завданнями практичного заняття.	7
6	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №6, робота над завданнями практичного заняття.	7
7	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №7, робота над завданнями практичного заняття.	7
8	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №8, робота над завданнями практичного заняття.	7
9	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №9, робота над завданнями практичного заняття.	7
10	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №10, робота над завданнями практичного заняття.	7
11	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №11, робота над завданнями практичного заняття.	7
12	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №12, робота над завданнями практичного заняття.	7
13	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №13, робота над завданнями практичного заняття.	7
14	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №14, робота над завданнями практичного заняття.	6
15	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №15, робота над завданнями практичного заняття.	7
16	Опрацювання теоретичного матеріалу. Підготовка до практичного заняття №16, робота над завданнями практичного заняття.	7
17	Узагальнення пройденого матеріалу. Підготовка до тестування.	5
	Разом за семестр:	114

6. Технології та методи навчання

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

7. Методи контролю

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

- оцінювання результатів захисту лабораторних робіт;
- тестовий контроль;
- оцінювання результатів виконання практичних завдань.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, 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 весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) 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 та формування фахових компетентностей і

програмних результатів навчання передбачає необхідність підготовки до практичних занять (вивчення теоретичного матеріалу з теми заняття) та активно працювати на практичних заняттях і вирішувати завдання, підготовки до 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 (рішення завдань, результати експериментів 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 зобов'язані дотримуватися термінів виконання усіх видів робіт, передбачених Робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене лабораторне або практичне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час практичних та лабораторних занять, а також за результатами тестування і підсумкового контролю.

Здобувач вищої освіти, виконуючи лабораторні роботи, практичні завдання та інші види робіт з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (із використанням мобільних девайсів тощо)). У разі виявлення плагіату 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 здобувачів освіти

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, системними та 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 здобувачів у VI семестрі

Аудиторна робота								Контрольні заходи	Семестровий контроль
Лабораторні роботи №:								Тестовий контроль:	Залік
1	2	3	4	5	6	7	8	Т 1-2	
Кількість балів за вид навчальної роботи (мінімум-максимум)									
6-10	6-10	6-10	6-10	6-10	6-10	6-10	6-10	12-20	За рейтингом
48-80								**12-20**	**60-100***

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів у VII семестрі

Аудиторна робота								Контрольні заходи	Семестровий контроль
Лабораторні роботи №								Тестовий контроль:	Залік
1	2	3	4	5	6	7	8	Т 1-4	
Кількість балів за вид навчальної роботи (мінімум-максимум)									
6-10	6-10	6-10	6-10	6-10	6-10	6-10	6-10	12-20	За рейтингом
48-80								**12-20**	**60-100***

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання здобувачів у VIII семестрі

Аудиторна робота								Контрольні заходи	Семестровий контроль	
Практичні заняття №								Тестовий контроль:	Іспит	Разом балів
1-2	3-4	5-6	7-8	9-10	11-12	13-14	15-16	Т 4-5		
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: Т – тема навчальної дисципліни;

*За набрану з будь-якого виду роботи (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».

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; якість оформлення звіту; вільне володіння здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення та отримані експериментально результати.

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 на практичних заняттях

Оцінка, яка виставляється за практичне заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми; вільне володіння студентом термінологією дисципліни, уміння обґрунтувати прийняті рішення при вирішенні завдань.

При оцінюванні практичного заняття викладач керується узагальненими критеріями, наведеними у таблиці «Критерії оцінювання навчальних досягнень здобувача вищої освіти» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

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.

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 залік вставляється на останньому занятті за умови якщо загальна сума балів, яку накопичив здобувач з дисципліни (іншого освітнього компонента) за результатами ***поточного*** контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «***зараховано***», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення. Присутність здобувача у цьому випадку не є обов'язковою.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у VIII семестрі в 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 вищої освіти (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»**)**.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав здобувач з дисципліни за результатами поточного та підсумкового 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 здобувачем сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Рейтингова шкала балів</th><th colspan="2">Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни</th></tr>
<tr><th>Залік</th><th>Іспит/диференційований залік</th></tr>
<tr><td>A</td><td>90-100</td><td rowspan="5">Зараховано</td><td>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</td></tr>
<tr><td>B</td><td>83-89</td><td rowspan="2">Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>C</td><td>73-82</td></tr>
<tr><td>D</td><td>66-72</td><td rowspan="2">Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни</td></tr>
<tr><td>E</td><td>60-65</td></tr>
<tr><td>FX</td><td>40-59</td><td rowspan="2">Незараховано</td><td>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</td></tr>
<tr><td>F</td><td>0-39</td><td>Незадовільно/Fail – Результати навчання відсутні</td></tr>
</table>

10. Питання для самоконтролю результатів навчання

VI семестр

1. Дайте визначення поняття "система контролювання доступу" та назвіть основні функції СКД.
2. Які основні завдання вирішують системи фізичного контролювання доступу?
3. Наведіть класифікацію СКД за типом архітектури.
4. У чому полягають переваги та недоліки автономних систем контролювання доступу?
5. Які нормативні документи регламентують застосування СКД в Україні?
6. Порівняйте централізовані та децентралізовані архітектури СКД.
7. Назвіть основні компоненти типової системи контролювання доступу.
8. Які критерії використовуються для вибору типу СКД для конкретного об'єкта?Поясніть різницю між поняттями "ідентифікація", "аутентифікація" та "авторизація".
9. Які технології RFID використовуються в сучасних СКД та в чому їх відмінності?
10. Опишіть принцип роботи proximity-карт на частоті 125 кГц.
11. У чому переваги смарт-карт стандарту MIFARE DESFire перед простими proximity-картами?
12. Назвіть основні біометричні методи ідентифікації, що застосовуються в СКД.
13. Які показники використовуються для оцінки якості біометричних систем (FAR, FRR)?
14. Опишіть технологію розпізнавання відбитків пальців у системах контролювання доступу.
15. У чому полягають переваги розпізнавання обличчя порівняно з іншими біометричними методами?
16. Що таке багатофакторна аутентифікація і навіщо вона потрібна в СКД?
17. Як працюють мобільні ідентифікатори на базі NFC та Bluetooth?
18. Назвіть основні апаратні компоненти системи контролювання доступу та їх призначення.
19. Які функції виконує контролер доступу в СКД?
20. Опишіть принцип роботи протоколу Wiegand для передачі даних між зчитувачем і контролером.
21. У чому переваги протоколу OSDP перед Wiegand?
22. Які типи електромагнітних та електромеханічних замків застосовуються в СКД?
23. Опишіть різницю між турнікетами, шлюзовими кабінами та обертовими дверима.
24. Які мережеві технології використовуються для з'єднання контролерів доступу?
25. Назвіть основні функції серверного програмного забезпечення СКД.
26. Які переваги дає використання інтелектуальних контролерів доступу?
27. Опишіть типову топологію мережі для багаточкової системи контролювання доступу.
28. Які етапи включає процес проєктування системи контролювання доступу?
29. Що таке аналіз ризиків і як він впливає на вибір рішень СКД?
30. Поясніть принцип зонування об'єкта при проєктуванні СКД.
31. Які рівні безпеки (security levels) можуть бути визначені для різних зон об'єкта?
32. Як здійснюється вибір обладнання для експлуатації в складних кліматичних умовах?
33. Опишіть принципи інтеграції СКД з системами охоронної сигналізації.
34. Як організується взаємодія СКД з системами пожежної безпеки (режим евакуації)?
35. Які вимоги висуваються до організації електроживлення СКД?
36. Навіщо потрібне резервне живлення для систем контролювання доступу?
37. Які особливості установки турнікетів та шлюзових кабін на об'єктах?
38. Які переваги дає інтеграція систем контролювання доступу з відеоспостереженням?
39. Опишіть протокол ONVIF та його роль в інтеграції СКД і відеосистем.
40. Що таке відеоверифікація проходів і як вона реалізується?
41. Як працює система розпізнавання облич у складі інтегрованої СКД?
42. Які події контролювання доступу можуть ініціювати запис відео або тривогу?
43. Назвіть основні функції систем управління відео (VMS).
44. Які методи синхронізації подій між СКД і системою відеоспостереження існують?
45. Які вимоги до зберігання відеоданих та журналів подій СКД?
46. Як забезпечується цілісність та захист архівів відео та даних про проходи?
47. Що таке Internet of Things (IoT) і як ця концепція застосовується до СКД?
48. Опишіть протокол MQTT та його використання в системах контролювання доступу.
49. Які переваги дає використання протоколу BACnet для інтеграції з BMS?
50. Як працюють бездротові технології Zigbee та Z-Wave у складі СКД?
51. Що таке розумний замок і які його основні можливості?
52. Як дані СКД можуть використовуватися для автоматизації роботи будівлі?
53. Поясніть концепцію Edge Computing у контексті розподілених систем контролювання доступу.
54. Які загрози кібербезпеки виникають при використанні IoT-пристроїв у СКД?
55. Опишіть архітектуру інтеграції СКД з системою управління будівлею (BMS).
56. Як технологія LoRaWAN може застосовуватися для побудови розподіленої СКД?
57. У чому полягають переваги хмарних систем контролювання доступу?
58. Опишіть модель SaaS (Software as a Service) для СКД.
59. Які функції можуть виконувати мобільні додатки для користувачів СКД?
60. Як реалізується віддалене управління та моніторинг систем контролювання доступу?
61. Що таке гібридна архітектура СКД і коли доцільно її застосовувати?
62. Порівняйте економічну ефективність локальних та хмарних рішень для СКД.
63. Які виклики виникають при масштабуванні хмарних систем контролювання доступу?
64. Назвіть основні загрози інформаційної безпеки для систем контролювання доступу.

65. Як захистити СКД від несанкціонованого доступу на рівні мережі?
66. Які вимоги GDPR стосуються обробки даних у системах контролювання доступу?
67. Опишіть процес аудиту безпеки системи контролювання доступу.
68. Як штучний інтелект може покращити функціональність СКД?
69. Які застосування машинного навчання можливі в системах контролювання доступу?
70. Опишіть потенційне використання блокчейн-технологій для СКД.

VII семестр

1. Положення про технічний захист інформації в Україні та контроль за його функціонуванням.
2. Положення про державну експертизу в сфері технічного захисту інформації.
3. Порядок створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності.
4. Порядок проведення перед проектних досліджень на об'єкті інформаційної діяльності.
5. Рекомендації щодо розроблення технічного завдання на виконання робіт із створення комплексу захисту на об'єкті інформаційної діяльності.
6. Система технічного захисту інформації в Україні: стан та напрями розвитку.
7. Перехоплення даних.
8. Класифікація каналів витоку інформації.
9. Технічні канали витоку інформації.
10. Методи за засоби захисту від витоку інформації.
11. Поняття інженерно-технічного захисту.
12. Апаратні засоби захисту.
13. Ключові елементи: ключові дискети, USB- та LPT-ключі.
14. Класифікація закладних пристроїв.
15. Основні характеристики закладних пристроїв.
16. Застосування закладних пристроїв.
17. Пристрої для захисту інформації у мережах.
18. Індикатори електромагнітних випромінювань.
19. Радіочастотоміри.
20. Автоматизовані пошукові комплекси.
21. Мобільні пошукові комплекси.
22. Скануючі приймачі.
23. Спеціалізоване програмне забезпечення.
24. Тепловізорні засоби.
25. Стаціонарні комплекси автоматичного виявлення радіомікрофонів.
26. Типові методи та прийоми проектування захищених інформаційних та комунікаційних систем.
27. Засоби захисту для складових КСЗІ.
28. Класифікація джерела загроз та загрози інформації.
29. Сутність технічного каналу витоку інформації.
30. Загальна класифікація каналів витоку інформації.
31. Електромагнітні канали витоку інформації.
32. Електричні канали витоку інформації.
33. Параметричні канали витоку інформації.
34. Повітряні канали витоку акустичної інформації.
35. Вібраційні канали витоку акустичної інформації.
36. Електроакустичні канали витоку акустичної інформації.
37. Оптико-електронний канал витоку акустичної інформації, його характеристика, методи блокування.
38. Індукційний метод перехоплення інформації при її передачі по каналах зв'язку.
39. Класифікація, принцип роботи акустичних закладок.
40. Класифікація, принцип роботи віброакустичних закладок.
41. Класифікація, принцип роботи спрямованих мікрофонів.
42. Класифікація, принцип роботи панорамних скануючих приймачів.
43. Класифікація, принцип роботи аналізаторів спектру та пеленгаторів.
44. Програмно-апаратні комплекси радіо-, радіотехнічної розвідки.
45. Засоби візуальної розвідки.
46. Системи спостереження за транспортними засобами. Радіомаяки. Радіонавігаційний приймач.
47. Класифікація методів та засобів захисту інформації від витоку технічними каналами.
48. Засоби виявлення, локалізації і нейтралізації закладних пристроїв.
49. Основні вимоги до структури і параметрів засобів радіомоніторингу при захисті мовної інформації.
50. Пасивні методи та засоби захисту інформації.
51. Активні методи та засоби захисту інформації.
52. Методи та засоби виявлення та подавлення диктофонів.
53. Методи і засоби пошуку електронних закладних засобів.
54. Методи пошуку закладок з використанням індикаторів поля, інтерсепторів і радіочастотомірів.
55. Методи пошуку закладок з використанням нелінійних локаторів, виявлячі порожнеч (пустот), металошукачів і рентгенівських апаратів
56. Засоби пошуку пристроїв перехоплення інформації. Сканерні приймачі й аналізатори спектру.
57. Програмно-апаратні та спеціальні комплекси контролю сигналів.

58. Засоби пошуку пристроїв перехоплення інформації, що використовують фізичні властивості навколишнього середовища.
59. Методи пошуку закладок з використанням металошукачів.
60. Види спеціальних перевірок виділених приміщень.
61. Державне ліцензування діяльності в області захисту інформації.
62. Сертифікація засобів захисту інформації. Основні поняття.
63. Атестування об'єктів інформатизації. Основні поняття.
64. Основні рекомендації щодо захисту інформації від витоку технічними каналами на об'єктах ТЗПІ при розробці технічного проекту
65. Етапи розробки проекту комплексу засобів захисту інформаційно-комунікаційної системи.
66. Принципи адаптації можливостей комплексу засобів захисту до вимог стандартів.

VIII семестр

1. У чому суть процесу і порядку створення КСЗІ?
2. У чому сенс побудови КСЗІ інтегрованою ІТС за модульним принципом?
3. З яких етапів складається процес створення КСЗІ?
4. Які рішення приймаються на етапі формування загальних вимог до КСЗІ?
5. Як обґрунтовується необхідність створення КСЗІ в ІТС?
6. У чому полягає мета обстеження середовища функціонування ІТС?
7. Що визначається в процесі формування завдання на створення КСЗІ?
8. У чому сенс розробки політики безпеки інформації в ІТС?
9. Що визначає технічне завдання на створення КСЗІ?
10. Які існують варіанти на оформлення ТЗ на КСЗІ?
11. Що визначається на етапі ескізного проектування КСЗІ?
12. Що виконується на етапі технічного проектування КСЗІ?
13. Що робиться на етапі робочого проектування КСЗІ?
14. Які роботи включені в етап введення КСЗІ в дію?
15. У чому полягає зміст пусконалагоджувальних робіт?
16. Яка мета попередніх випробувань КСЗІ?
17. Що виконується під час дослідницької експлуатації КСЗІ?
18. Яка мета державної експертизи КСЗІ і що при цьому робиться?
19. У чому сенс супроводу КСЗІ?
20. Що викладається в ТЗ на КСЗІ?
21. Що є вихідними даними для розробки ТЗ на КСЗІ?
22. Які основні роботи виконуються на етапі формування ТЗ на КСЗІ?
23. Що включається в опис політики безпеки?
24. Які вимоги рекомендується включати в ТЗ відносно вживаних способів, методів і засобів?
25. Що включається в розділ «Вимоги до складу проектної та експлуатаційної документації»?
26. Що включається в розділ «Етапи виконання робіт»?
27. Що включається в розділ «Порядок проведення випробувань КСЗІ»?
28. Які види критеріїв визначаються в НД ТЗІ 2. 5-004-99?
29. Що визначають рівні кожної послуги?
30. Що є рейтингом послуг захисту інформації, що надаються, в ІТС від НСД?
31. Поясніть структуру критеріїв конфіденційності.
32. Що означають критерії довірчої та адміністративної конфіденційності?
33. Поясніть структуру критеріїв цілісності.
34. Поясніть структуру критеріїв доступності.
35. Поясніть структуру критеріїв спостереженості.
36. Поясніть структуру критеріїв гарантій.
37. Який сенс критеріїв гарантій середовища розробки?
38. Який сенс критеріїв гарантій послідовності розробки?
39. Який сенс критеріїв гарантій випробувань КЗЗ?
40. Які загальні вимоги до процесів обробки в ІТС службової інформації?
41. Що входить до складу ІТС класу 2?
42. Чим укомплектовані обчислювальні системи ІТС?
43. Що є комплексом ПЗ обчислювальної системи?
44. У чому полягають типові вимоги до обчислювальної системи ІТС в питаннях захисту інформації?
45. У чому полягають типові вимоги до умов розміщення компонентів ІТС?
46. Що необхідно виконати для організації управління доступом до службової інформації і компонент ІТС?
47. Визначите основні характеристики оброблюваною в ІТС службової інформації.
48. Визначите характеристики технології обробки службової інформації в ІТС.
49. Які технології обробки службової інформації реалізуються в ІТС класу 2?
50. Визначите функціональні профілі захищеності оброблюваної інформації в ІТС класу 2.
51. Що є Планом захисту інформації в ІТС? На яких засадах він розробляється? Що він закріплює?
52. У яких випадках розробляється План захисту інформації в ІТС?
53. Які розділи включаються в План захисту інформації в ІТС?
54. У чому полягають завдання захисту інформації в ІТС?

55. На які об'єкти ІТС поширюється політика безпеки?
56. Як класифікується інформація, що обробляється в ІТС?
57. Які об'єкти ІТС підлягають інвентаризації?
58. Якими способами можуть здійснюватися загрози в ІТС?
59. Що необхідно визначити для кожної із загроз безпеки в ІТС?
60. Що є моделлю порушника інформаційної безпеки?
61. Як класифікуються порушники безпеки?
62. Що є політикою безпеки інформації в ІТС?
63. Які моменти повинні враховуватися при розробці політики безпеки?
64. На яких принципах базується політика безпеки?
65. Які моменти повинна доказово гарантувати політика безпеки?
66. Які роботи включає методологія розробки політики безпеки?
67. Що є концепція безпеки інформації в ІТС?
68. Що є аналізом ризиків?
69. Як здійснюється вибір основних рішень в забезпеченні інформаційної безпеки?
70. Що в себе включає план проведення відновних робіт і забезпеченняибезперервності функціонування ІТС?
71. У чому полягають правила розмежування доступу?
72. Що є система документів із забезпечення захисту інформації в ІТС?
73. З яких розділів складається календарний план робіт з організації заходів захисту інформації в ІТС?
74. У чому полягає зміст висновків за результатами випробувань комплексу ТЗІ?
75. Визначите склад Програми і методики випробувань комплексу ТЗІ.
76. Що є атестація комплексу ТЗІ? Які існують види атестації?
77. Визначите етапи атестації комплексу ТЗІ.
78. З яких розділів складається Паспорт на комплекс ТЗІ?
79. Що таке управління КСЗІ? У чому його сенс і мета?
80. У чому полягають особливості систем управління КСЗІ?
81. Які завдання вирішуються в процесі управління КСЗІ?
82. У чому полягають принципи управління КСЗІ?
83. Яка структура управління КСЗІ? Що виконують її основні елементи?
84. Як класифікують завдання управління КСЗІ?
85. Які розділи включає Положення про СЗІ в ІТС?
86. Що таке СЗІ в ІТС? Які правові основи її створення і діяльності?
87. У чому полягають повноваження і відповідальність СЗІ?
88. У чому сенс будівельно-монтажних робіт?
89. Які функції системи розмежування доступу?
90. Якими шляхами забезпечується цілісність і доступність інформації в ІТС на етапі експлуатації?
91. Поясніть завдання, які вирішуються в процесі технічної експлуатації КСЗІ.
92. Яка мета етапу науково-дослідної розробки КСЗІ?
93. Визначте послідовність і зміст науково-дослідної розробки КСЗІ.
94. Що є моделювання КСЗІ? Які типі моделей використовуються?
95. У чому полягають особливості моделювання КСЗІ?
96. Які основні етапи оцінювання КСЗІ?
97. Що є показники ефективності системи? Які вимоги до них?
98. Що таке критерії ефективності КСЗІ? Які концепції використовують для прийняття рішень?
99. Приклади критеріїв придатності, оптимальності й раціональності.
100. Які підходи використовують для оцінки ефективності КСЗІ

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Комплексні системи захисту інформації» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання:

1. Курс «Комплексні системи захисту інформації». https://msn.khmnu.edu.ua/course/view.php?id=6709

12. Матеріально-технічне та програмне забезпечення

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями, стенд Xiaomi Mi Home, стенд ZKTeco, RFID, стенд HikVision, IP-телефони, мережеве та інше спеціалізоване обладнання.

Спеціальне та прикладне програмне забезпечення: OS Ubuntu, OS MS Windows 10 або вище, ЛОЗА™-1, Xiaomi Mi Home, ZKTeco , IP Video System Design Tool, VoIP Asterisk, тощо.

13. Рекомендована література

Основна

1. Жураковський, Б. Ю. Технології інтернету речей [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Інформаційне забезпечення робототехнічних систем» за спеціальністю 126 «Інформаційні системи та технології» / Б. Ю. Жураковський, І. О. Зенів ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 5,1 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 271 с. – Назва з екрана.
2. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. – 3rd ed. – Indianapolis, Indiana : John Wiley & Sons, Inc., 2020. – 1212 p.
3. Yevseiev, S. Modeling of security systems for critical infrastructure facilities : monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych [et al.]. – Kharkiv : PC TECHNOLOGY CENTER, 2022. – 196 p.
4. Кушнір, А. П. Системи пожежної та охоронної сигналізації : навчальний посібник / А. П. Кушнір, Д. О. Чалий. – Львів : СПОЛОМ, 2022. – 298 с.
5. Хлапонін, Ю. І. Комплексні системи захисту інформації : конспект лекцій / Ю. І. Хлапонін. – Київ : КНУБА, 2022. – 84 с.
6. Хорошко, В. О. Проєктування комплексних систем захисту інформації : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало [та ін.] ; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». – Львів : Видавництво Львівської політехніки, 2020. – 320 с. : іл.

Додаткова

7. Терлецький, Т. В. Системи пожежної сигналізації : навчальний підручник для студентів технічних спеціальностей / Т. В. Терлецький, В. І. Федорчук-Мороз, О. Л. Кайдик ; за заг. ред. Т. В. Терлецького. – Луцьк : ІВВ ЛНТУ, 2022. – 130 с.
8. Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software / ed. M. Schwartz, M. Machulak. – Berkeley, CA : Apress, 2018. – 377 p.
9. Гулак, Г. М. Методологія захисту інформації. Аспекти кібербезпеки : навчальний посібник / Г. М. Гулак [та ін.]. – Київ : Видавництво НА СБ України, 2020. – 256 с.
10. Rashid, N. N. A Comprehensive Framework for Harnessing IoT and 5G for Enhanced Disaster Response / N. N. Rashid, Z. Ghanim Ali, A. Hussein Ali, N. Adnan Taher, S. Khdhaer Mukhlif, I. V. Muliar, H. Muthanna Noori // Proceeding of the 36th Conference of FRUCT Association. – 2024. – P. 655–663. – ISSN 2305-7254.
11. Муляр, І. В. Використання сучасних децентралізованих технологій для розмежування доступу в хмарному середовищі / І. В. Муляр, В. В. Гавронський, І. В. Гурман, А. Р. Віхтюк, В. О. Пістолюк // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2022. – № 4. – С. 81–86. – DOI: 10.31891/2219-9365-2022-72-4-10.
12. Cabanillas-Carbonell, M. Artificial intelligence in video surveillance systems for suspicious activity detection and incident response: A systematic literature review / M. Cabanillas-Carbonell, J. Sallari Rivera, J. Santivañez Muñoz // Advances in Science and Technology Research Journal. – 2025. – Vol. 19, No. 3. – P. 389–405. – DOI: 10.12913/22998624/196795.
13. Lienkov, O. The Development of an Intelligent Complex of Radiation-Technological Control of a Safety Barrier / O. Lienkov, Y. Banzak, I. Husak, I. Muliar, V. Cheshun, E. Lenkov // International Journal of Emerging Trends in Engineering Research. – 2020. – Vol. 8, No. 7. – P. 3483–3486. – DOI: 10.30534/ijeter/2020/97872020.
14. Муляр, І. В. Використання моделі GPT для автоматизації тестування IoT-пристроїв / І. В. Муляр, В. С. Гловюк, К. О. Зацепін, В. С. Чернов // Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XX міжнар. наук.-практ. конф., Київ, 29 листоп. 2024 р. – Київ : ВІКНУ, 2024. – Т. 1. – С. 49–50.
15. Бобровнікова, К. Ю. Метод та алгоритми виявлення кібератак у мережах інтернету речей на основі аналізу енергоспоживання / К. Ю. Бобровнікова, І. В. Гурман, В. І. Чорненький, І. В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2025. – Вип. 88. – С. 82–95.
16. Комплексна безпека інформаційних мережевих систем : навчальний посібник / уклад. А. Г. Микитишин, М. М. Митник, О. С. Голотенко, В. В. Карташов. – Тернопіль : ФОП Паляниця В. А., 2023. – 324 с.
16. Гулак, Г. М. Методологія захисту інформації. Аспекти кібербезпеки : навчальний посібник / Г. М. Гулак [та ін.]. – Київ : Видавництво НА СБ України, 2020. – 256 с.
17. Li, Q. Design and Performance Evaluation of an RFID and Machine Learning-Based Intelligent Security System for Smart Buildings / Q. Li, J. Liu // 2025 2nd International Conference on Intelligent Computing and Robotics (ICICR), 2025. – P. 193–198.

18. Kanagamalliga, S. Arduino-Powered Fingerprint Authentication for Door Access Control / S. Kanagamalliga, S. Rajalingam, M. Karthikeyan, A. Kannan // 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), 2024. – P. 131–135.

19. Lam, K. H. Smart Building Management System (SBMS) for Commercial Buildings – Key Attributes and Usage Intentions from Building Professionals' Perspective / K. H. Lam, W. M. To, P. K. C. Lee // Sustainability. – 2023. – Vol. 15, No. 1. – P. 80. – DOI: 10.3390/su15010080.

20. Al-Doori, V. S. Securing Smart Buildings Using RFID and Fingerprint Technologies / V. S. Al-Doori, M. A. J. Maktoof, A. F. Abdulqader, S. Lienkov // 2024 35th Conference of Open Innovations Association (FRUCT), 2024. – P. 71–81.

21. Uddin, M. N. Engineering a multi-sensor surveillance system with secure alerting for next-generation threat detection and response / M. N. Uddin, H. Nyeem // Results in Engineering. – 2024. – Vol. 22. – Article 101984. – DOI: 10.1016/j.rineng.2024.101984.

22. ДСТУ IEC 62676-1-1:2017 (IEC 62676-1-1:2013, IDT). Системи відеоспостереження охоронного призначення. Частина 1-1. Вимоги до систем. Загальні вимоги. – Чинний від 2017-12-15. – Київ : ДП «УкрНДНЦ», 2017. – IV, 33 с. – (Національний стандарт України).

23. ISO/IEC 30137-1:2019. Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification. – Published 2019-02. – Geneva : ISO, 2019. – 28 p.

24. ДСТУ IEC 60839-11-1:2017 (IEC 60839-11-1:2013, IDT). Системи тривожної сигналізації та електронні системи безпеки. Частина 11-1. Електронні системи контролювання доступу. Вимоги до системи та її складників. – Чинний від 2017-12-15. – Київ : ДП «УкрНДНЦ», 2017. – IV, 51 с. – (Національний стандарт України).

25. MITRE ATT&CK® Matrix for ICS. URL: https://attack.mitre.org/matrices/ics/ (дата звернення: 25.08.2025).

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://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Шостий, сьомий, восьмий
Кількість встановлених кредитів ЄКТС	16
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. Вступ у системи контролювання доступ. Поняття доступу, цілі та класифікація систем контролювання доступу; огляд загроз і вимог до систем. СКД для критичної інфраструктури. Методи ідентифікації користувачів. Протоколи. Інтерфейси. Апаратні компоненти СКД. Проєктування та впровадження фізичних систем контролювання доступу**.** Інтеграція СКД з системами відеоспостереження, IoI, розумним будинком. Хмарні технології та мобільні рішення в СКД**.** Тенденції розвитку СКД. Використання ШІ. Матриця атак MITRE ATT&CK® Matrix for ICS. Теоретичні основи та нормативна база технічного захисту інформації. Канали витоку, методи їх виявлення та перекриття. Технічні аспекти забезпечення цілісності та доступності. Атестація об'єктів та державна експертиза у сфері технічного захисту інформації. Теоретичні основи та нормативна база технічного захисту інформації. Канали витоку, методи їх виявлення та перекриття. Технічні аспекти забезпечення цілісності та доступності. Атестація об'єктів та державна експертиза у сфері технічного захисту інформації.

Пререквізити: сигнали і процеси в системах захисту інформації; захист інформації в інформаційно-комунікаційних системах; захист інформації в інформаційно-комунікаційних системах (курсовий проєкт); нормативно-правове забезпечення кібербезпеки; прикладна криптологія; адміністрування та захист баз і сховищ даних; адміністрування та захист баз і сховищ даних (курсовий проєкт).

Постреквізити: виробнича практика 2.

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 та проблемних методів із застосуванням

мультимедійних технологій та презентаційних матеріалів); практичні заняття (з використанням практичних та частково-пошукових методів); лабораторні роботи (з використанням практичних, частково-пошукових методів та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій та спеціалізованого обладнання, методів проєктної діяльності, комп'ютерного моделювання); самостійна робота (з використанням пояснювально-ілюстративних, практичних та частково-пошукових методів).

Форми оцінювання результатів навчання: оцінювання на практичних заняттях; оцінювання результатів захисту лабораторних робіт; тестовий контроль; оцінювання результатів підсумкового семестрового контролю (іспит).

Вид семестрового контролю: залік**,** іспит.

Навчальні ресурси:

1. 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.
2. Інформаційна безпека в комп'ютерних мережах: навч. посіб./ О.А. Смірнов, Конопліцька-О.К. Слободенюк, С.А. Смірнов, К.О. Буравченко, Т.В. Смірнова, Л.І. Поліщук. Кропивницький: Видавець Лисенко В. Ф., 2020. 295 с.
3. Information Security Handbook/ Noor Zaman Jhanjhi, Khalid Hussain, Mamoona Humayun, Azween Bin Abdullah, João Manuel R.S. Tavares. CRC Press, 2022. 250 p.
4. Інформаційна безпека. Підручник/ В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.:Видавництво Ліра-К, 2021. 412 с.
5. Інформаційні мережі: навчальний посібник / Ю. В. Коваль, А. Б. Ставровський. Київ, 2021. 84 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/

Викладач: канд. техн. наук, доцент Ігор Муляр; канд. техн. наук, доцент Віктор Чешун; асистент Олена Зарицька.