

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ  
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ВНУТРІШНІХ СПРАВ**

**Кафедра кібербезпеки та DATA-технологій, факультет №6**

**РОБОЧА ПРОГРАМА**

**навчальної дисципліни «Комплексні системи захисту інформації:  
проектування, впровадження, супровід»  
вибіркових компонент освітньої програми  
першого (бакалаврського) рівня вищої освіти**

**125 «Кібербезпека»**

**Харків 2023**

**ЗАТВЕРДЖЕНО**

Науково-методичною радою  
Харківського національного  
університету внутрішніх справ  
Протокол від 30.08.2023 № 7

**СХВАЛЕНО**

Вченою радою факультету № 6  
Протокол від 25.08.2023 № 7

**ПОГОДЖЕНО**

Секцією Науково-методичної ради  
ХНУВС з технічних дисциплін  
Протокол від 29.08.2023 № 7

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій  
факультету № 6 (протокол від 15.08.2023 № 8)

**Розробник:**

*Доцент кафедри кібербезпеки та DATA-технологій факультету № 6, к.т.н.,  
доцент Хавіна І.П.;*

**Рецензенти:**

- 1. Професор кафедри комп'ютерних наук та інформаційних технологій  
Національного аерокосмічного університету ім. М. Є. Жуковського  
«Харківський авіаційний інститут» д. т. н., професор Прохоров О. В.*
- 2. Провідний науковий співробітник Науково-дослідної лабораторії з проблем  
розвитку інформаційних технологій ХНУВС, к.т.н., доцент Мордвинцев М.В.*

## 1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, спеціалізації, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 5 Загальна кількість годин – 150 Кількість тем - 9	12 Інформаційні технології; 125 Кібербезпека  перший (бакалаврський) рівень вищої освіти	Навчальний курс – 4 Семестр – 7 Види контролю – залік
<b>Розподіл навчальної дисципліни за видами занять:</b>		
денна форма навчання		заочна форма навчання
Лекції – $\frac{30}{\text{(години)}}$ ;		Лекції – $\frac{8}{\text{(години)}}$ ;
Практичні заняття – $\frac{20}{\text{(години)}}$ ;		Практичні заняття – $\frac{6}{\text{(години)}}$ ;
Лабораторні заняття – $\frac{24}{\text{(години)}}$ ;		Лабораторні заняття – $\frac{6}{\text{(години)}}$ ;
Самостійна робота – $\frac{76}{\text{(години)}}$ ;		Самостійна робота – $\frac{130}{\text{(години)}}$ ;
Курсовий проект - 1		

## 2. Мета та завдання навчальної дисципліни

**Мета:** метою викладання дисципліни «Комплексні системи захисту інформації: проектування, впровадження, супровід» є забезпечити теоретичну та практичну підготовку здобувачів вищої освіти щодо принципів створення, організації та порядку проведення робіт з проектування, впровадження та супроводу комплексних систем захисту інформації (КСЗІ) в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах (далі – ІТС) підприємств, організацій, установ тощо; набуття практичних навичок аналізу, побудови та використання комплексних систем захисту від несанкціонованого доступу до інформації.

**Завдання:** надання здобувачам вищої освіти необхідних знань щодо загальних питань порядку проведення робіт із створення КСЗІ в ІТС, здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно – правовими актами та нормативними документами у сфері захисту інформації; набуття практичних навичок аналізу, побудови та використання, захисту від несанкціонованого доступу до інформації.

**Міждисциплінарні зв'язки :** викладання дисципліни «Комплексні системи захисту інформації: проектування, впровадження, супровід» базується на знаннях дисциплін «Комп'ютерні основи систем кібербезпеки», «Інформаційні

технології», «Електроніка та схемотехніка», «Операційні системи та комп'ютерні мережі», «Прикладна криптологія», «Методи та засоби захисту інформації».

**Очікувані результати навчання:** дисципліна формує компетенції з проблем теорії та практики створення КСЗІ в ІТС. У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

**знати:**

- принципи створення КСЗІ в ІТС;
- організацію та порядок проведення робіт з проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах;

**вміти:**

- здійснювати заходи щодо проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційних, комунікаційних та інформаційно – телекомунікаційних системах.

<b>Програмні компетентності, які формуються при вивченні навчальної дисципліни:</b>		
<b>Інтегральна компетентність</b>	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі створення, впровадження та супроводу комплексних систем захисту інформації, що передбачає використання нормативної бази, спеціалізованих методів та засобів побудови таких систем.	
<b>Загальні компетентності (ЗК)</b>	ЗК1.	Здатність до абстрактного мислення, аналізу та синтезу.
	ЗК2.	Здатність застосовувати знання на практиці.
	ЗК3.	Знання та розуміння предметної області та розуміння професії.
	ЗК5.	Навички використання інформаційних і комунікаційних технологій.
	ЗК6.	Здатність до пошуку, обробки та аналізу інформації з різних джерел.
	ЗК8.	Здатність провадити дослідницьку та/або інноваційну діяльність.
<b>Спеціальні (фахові, предметні) компетентності (ФК)</b>	ФК2.	Здатність до використання інформаційних і комунікаційних технологій з метою пошуку нової інформації, створення баз даних, аналізу розподілених інформаційно-телекомунікаційних систем (ІТС), каналів зв'язку, систем управління процесами, оперативного планування роботи систем на основі аналізу інформаційних потоків та їх оптимізації.
	ФК3.	Здатність здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки, що включає: прогнозування та оцінювання стану інформаційної безпеки об'єктів і систем: виконання спеціальних досліджень технічних і програмно-апаратних засобів захисту

		обробки інформації в ІТС; проведення техніко-економічного аналізу й обґрунтування проектних рішень з забезпечення кібербезпеки; формування комплексу заходів (правил, процедур, практичних прийомів та ін.) для управління інформаційною безпекою.
	ФК4.	Здатність управляти системами, технологіями і засобами забезпечення інформаційної безпеки, що включає: відновлення нормального функціонування ІТС після здійснення кібератак, збоїв та відмов; управління інцидентами та ризиками інформаційної та кібербезпеки.
	ФК5.	Здатність проводити техніко-економічного аналіз й обґрунтовувати проектні рішення з забезпечення кібербезпеки.
	ФК6.	Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.
<b>Програмні результати навчання (ПРН)</b>	ПРН 2.	Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність
	ПРН 3.	Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел щодо ефективного розв'язання спеціалізованих задач професійної діяльності
	ПРН 4.	. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення
	ПРН 5.	Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат
	ПРН 6.	Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
	ПРН 8.	Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки
	ПРН 9.	Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки
	ПРН 10.	Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем
	ПРН 11.	Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах
	ПРН 12.	Розробляти моделі загроз та порушників

	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 15.	Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій
	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 із відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент
	ПРН 18.	Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів
	ПРН 19.	Застосовувати теорії та методи захисту щодо забезпечення безпеки інформації в інформаційно-телекомунікаційних системах
	ПРН 20.	Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів у інформаційно-телекомунікаційних системах
	ПРН 21.	Вирішувати задачі забезпечення та супроводу (зокрема: огляд, тестування, підзвітність) системи управління доступом згідно зі встановленою політикою безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах
	ПРН 22.	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки
	ПРН 23.	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах

ПРН 24.	Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових)
ПРН 25.	Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів
ПРН 26.	Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем
ПРН 27.	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах
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 30.	Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем
ПРН 31.	Застосовувати теорії та методи захисту щодо забезпечення безпеки елементів інформаційно-телекомунікаційних систем
ПРН 32.	Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем із використанням процедур резервування згідно встановленої політики безпеки
ПРН 33.	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків
ПРН 34.	Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації
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 та\або кібербезпеки
ПРН 41.	Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур
ПРН 42.	Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та\або кібербезпеки
ПРН 43.	Застосовувати національні та міжнародні регулюючі акти у сфері інформаційної безпеки та\або кібербезпеки для розслідування інцидентів
ПРН 44.	Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами
ПРН 45.	Застосовувати різні класи політик інформаційної безпеки та\або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів
ПРН 46.	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах
ПРН 47.	Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації
ПРН 48.	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах
ПРН 49.	Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах
ПРН 50.	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних)
ПРН 51.	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах
ПРН 52.	Використовувати інструментарій щодо моніторингу процесів в інформаційно-телекомунікаційних системах



## **1. Програма навчальної дисципліни.**

### **ТЕМА № 1. «Сутність комплексної системи захисту інформації і принципи її організації».**

Методологічні та концептуальні засади комплексної системи захисту інформації. Проведення робіт зі створення КСЗІ. Методологічні та концептуальні засади комплексної системи захисту інформації. Етапи створення КСЗІ. Правові підстави для створення КСЗІ.

### **ТЕМА № 2. «Технічне завдання на створення КСЗІ в ІС»**

Загальні вимоги до розробки технічного завдання на створення КСЗІ в ІТС. Вимоги до змісту розділів технічного завдання.

### **ТЕМА № 3. «Оцінка захищеності інформації в ІС від несанкціонованого доступу»**

Побудова і структура критеріїв захищеності інформації. Оцінка коректності реалізації послуг безпеки (критерії гарантій).

### **ТЕМА № 4. «Особливості проектування КСЗІ для ІТС різних класів»**

Класифікація АС. Функціональні профілі захищеності ІТС. Особливості стандартних функціональних профілів захищеності ІТС. Особливості захисту службової інформації від НСД в ІС класу 2. Загальні вимоги із захисту службової інформації. Характеристика типових умов функціонування та вимог із захисту інформації в ІТС класу 2. Політика реалізації послуг безпеки інформації в ІТС класу 2.

### **ТЕМА № 5. «Планування захисту інформації в ІС»**

Призначення та структура Плану захисту інформації в ІС. Зміст Плану захисту інформації в ІТС.

### **ТЕМА № 6. «Випробування комплексу технічного захисту інформації та його атестація»**

Випробування комплексу технічного захисту інформації. Атестація комплексів захисту інформації. Порядок розроблення та оформлення паспорта на комплекс ТЗІ.

### **ТЕМА № 7. «Управління комплексною системою захисту інформацією в ІС»**

Призначення, структура і зміст управління КСЗІ. Служба захисту інформації в ІТС: призначення, завдання, функції, повноваження та відповідальність.

### **ТЕМА № 8. «Введення КСЗІ в дію»**

Застосування КСЗІ за призначенням. Технічна експлуатація КСЗІ.

### **ТЕМА № 9. «Моделювання КСЗІ»**

Методи моделювання КСЗІ. Вибір показників ефективності та критеріїв оптимальності КСЗІ.

#### 4. Структура навчальної дисципліни

##### 4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни					Вид контролю	
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття		Самостійна робота
Семестр № 7							
ТЕМА № 1. Сутність комплексної системи захисту інформації і принципи її організації	16	4		2	2	8	залік
ТЕМА № 2. Технічне завдання на створення КСЗІ в ІС	16	4		2	2	8	
ТЕМА № 3. Оцінка захищеності інформації в ІС від несанкціонованого доступу	22	4		4	4	10	
ТЕМА № 4. Особливості проектування КСЗІ для ІТС різних класів	16	4		2	2	8	
ТЕМА № 5. Планування захисту інформації в ІС	18	4		2	4	8	
ТЕМА № 6. Випробування комплексу технічного захисту інформації та його атестація	14	2		2	2	8	
ТЕМА № 7. Управління комплексною системою захисту інформацією в ІС	20	4		2	4	10	
ТЕМА № 8. Введення КСЗІ в дію	14	2		2	2	8	
ТЕМА № 9. Методи моделювання КСЗІ	14	2		2	2	8	
Всього за семестр № 7:	150	30		20	24	76	

#### 4.1.2. Розподіл часу навчальної дисципліни за темами (заочна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 7							
ТЕМА № 1. Сутність комплексної системи захисту інформації і принципи її організації	11,5	0,5		0,5	0,5	10	залік
ТЕМА № 2. Технічне завдання на створення КСЗІ в ІС	12	1		0,5	0,5	10	
ТЕМА № 3. Оцінка захищеності інформації в ІС від несанкціонованого доступу	13	1		1	1	10	
ТЕМА № 4. Особливості проектування КСЗІ для ІТС різних класів	12	1		0,5	0,5	10	
ТЕМА № 5. Планування захисту інформації в ІС	13	1		1	1	10	
ТЕМА № 6. Випробування комплексу технічного захисту інформації та його атестація	22	1		0,5	0,5	20	
ТЕМА № 7. Управління комплексною системою захисту інформацією в ІС	23	1		1	1	20	
ТЕМА № 8. Введення КСЗІ в дію	22	1		0,5	0,5	20	
ТЕМА № 9. Методи моделювання КСЗІ	21,5	0,5		0,5	0,5	20	
Всього за семестр № :	150	8		6	6	130	

#### 4.1.3. Питання, що виносяться на самостійне опрацювання.

Завдання що виносяться на самостійну роботу студента			Література:
<b>Семестр №7</b>			
	Тема 1. Сутність комплексної системи захисту інформації і принципи її організації.		
	Основні види інформації.		Конспект лекцій, література [1-13]
	Основні джерела інформації.		Конспект лекцій, література [1-13]

	Інформаційна взаємодія, основні об'єкти та суб'єкти інформаційної взаємодії	Конспект лекцій, література [1-13]
	Тема 2. Методологічні та концептуальні засади комплексної системи захисту інформації.	
	Рівень забезпечення безпеки інформації. Достатність захисту інформації.	Конспект лекцій, література [1-13]
	Варіанти побудови комплексної системи захисту Внутрішньовідомчі нормативно-правові документи.	Конспект лекцій, література [1-13]
	Тема 3. Порядок здійснення захисту інформації на об'єктах інформаційної діяльності	
	Класифікація інформації за видами таємниці і ступенями конфіденційності.	Конспект лекцій, література [1-13]
	Нормативне закріплення складу інформації, що захищається.	Конспект лекцій, література [1-13]
	Тема 4. Захист інформації в комп'ютерній системі підприємства	
	Послідовність визначення об'єкта захисту.	Конспект лекцій, література [1-13]
	Значення носіїв інформації, що захищається як об'єктів захисту.	Конспект лекцій, література [1-13]
	Основні методи оцінювання захищеності інформації в ІТС.	Конспект лекцій, література [1-13]
	Нормативно-методичні матеріали з організації захисту інформації.	Конспект лекцій, література [1-13]
	Тема 5. Несанкціонований доступ до інформації і способи його здійснення	
	Визначення джерел дестабілізуючого впливу на інформацію.	Конспект лекцій, література [1-13]
	Модель формування безлічі дестабілізуючих факторів. Поняття загрози безпеки інформації.	Конспект лекцій, література [1-13]
	Функціональні профілі захищеності.	Конспект лекцій, література [1-13]
	Вимоги до проектної та експлуатаційної документації.	Конспект лекцій, література [1-13]
	Тема 6. Модель порушника безпеки інформації в ІТС	
	Класифікація, модель порушників.	Конспект лекцій, література [1-13]
	Основні напрями реалізації порушником інформаційних загроз в ІТС.	Конспект лекцій, література [1-13]
	Можливості, категорії, специфікація порушників.	Конспект лекцій, література [1-13]
	Тема 7. Методи, засоби та заходи захисту інформації в ІТС від витоку та руйнування технічними каналами	
	Технічні канали витоку інформації і їх класифікація.	Конспект лекцій, література [1-13]
	Модель технічних каналів витоку інформатизації на типовому об'єкті інформатизації.	Конспект лекцій, література [1-13]
	Канали витоку через несанкціонований вплив на системи, що використовують інформаційно-комунікаційні технології.	Конспект лекцій, література [1-13]
	Тема 8. Правові підстави та основні положення щодо створення КСЗІ та комплексу ТЗІ в Україні	
	Структура законодавства України в області захисту інформації.	Конспект лекцій, література [1-13]
	Основні положення правових норм щодо створення КСЗІ та комплексів ТЗІ.	Конспект лекцій, література [1-13]
	Тема 9. Моделювання процесів комплексної системи захисту інформації.	

	Моделі управління безпекою	Конспект лекцій, література [1-13]
	Архітектурна побудова комплексної системи захисту інформації	Конспект лекцій, література [1-13]
	Технологічна побудова комплексної системи захисту інформації	Конспект лекцій, література [1-13]

## 5. Індивідуальні завдання

### 5.1.1. Теми рефератів

### 5.1.2. Теми курсових робіт

1. Розробка комплексної системи захисту інформації для агентства з продажу нерухомості.
2. Розробка комплексної системи захисту інформації для кредитного відділу комерційного банку.
3. Розробка комплексної системи захисту інформації для бухгалтерії вищого навчального закладу.
4. Розробка комплексної системи захисту інформації для громадської організації.
5. Розробка комплексної системи захисту інформації для інтернет-магазину продажу електротоварів.
6. Розробка комплексної системи захисту інформації для відділу кадрів комерційного банку.
7. Розробка комплексної системи захисту інформації для відділення фірми інтернет-провайдера.
8. Розробка комплексної системи захисту інформації для відділення комерційного банку.
9. Розробка комплексної системи захисту інформації для приватної конструкторської фірми.
10. Розробка комплексної системи захисту інформації для сховища даних супермаркету.
11. Розробка комплексної системи захисту інформації для клінічної лабораторії.
12. Розробка комплексної системи захисту інформації для бібліотечного репозиторію кафедри.
13. Розробка комплексної системи захисту інформації для будівельної організації.
14. Розробка комплексної системи захисту інформації для аптеки.
15. Розробка комплексної системи захисту інформації для ректорату вищого навчального закладу.
16. Розробка комплексної системи захисту інформації для кафедри вищого навчального закладу.
17. Розробка комплексної системи захисту інформації для факультету вищого навчального закладу.

18. Розробка комплексної системи захисту інформації для ветеринарної клініки.
19. Розробка комплексної системи захисту інформації для страхової компанії.
20. Розробка комплексної системи захисту інформації для інтернет-магазину оптової продажу одягу.
21. Розробка комплексної системи захисту інформації для відділу кадрів навчального закладу.
22. Розробка комплексної системи захисту інформації для фірми інтернет-провайдера.
23. Розробка комплексної системи захисту інформації для відділення магазину мережи «Сільпо».
24. Розробка комплексної системи захисту інформації для приватної конструкторської фірми.
25. Розробка комплексної системи захисту інформації для бібліотечного порталу вищого навчального закладу.
26. Розробка комплексної системи захисту інформації для транспортної компанії (вантажні перевози).
27. Розробка комплексної системи захисту інформації для служби таксі.
28. Розробка комплексної системи захисту інформації для відділення пошти.
29. Розробка комплексної системи захисту інформації для станції пасажирських автобусних перевезень.
30. Розробка комплексної системи захисту інформації для спортивного комплексу.

### **5.1.3. Теми наукових робіт**

## **6. Методи навчання**

Навчання з дисципліни проходить у формі:

для денної форми навчання:

- лекцій (15 занять, 30 годин);
- практичних занять (10 занять, 20 години);
- лабораторних занять (12 занять, 24 години);
- самостійної роботи (76 години);

для заочної форми навчання:

- лекцій (4 заняття, 8 годин);
- практичних занять (3 заняття, 6 години);
- лабораторних занять (3 заняття, 6 години);
- самостійної роботи (130 години);

Метою лекційного курсу є отримання студентами необхідних знань та практичних навичок для розробки та створення, організації та порядку проведення робіт з проектування, впровадження та супроводу комплексних систем захисту інформації в інформаційних, комунікаційних та ІТС підприємств,

організацій, установ тощо; набуття практичних навичок аналізу, побудови та використання комплексних систем захисту від несанкціонованого доступу до інформації. Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, та опрацювання завдань до практичних занять. Індивідуальна робота передбачає виконання курсового проекту.

## **7. Перелік питань та завдань, що виносяться на підсумковий контроль**

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 пусконаладжувальних 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 забезпечення безперервності 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 типи 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?

## 8. Критерії та засоби оцінювання результатів навчання здобувачів

Контрольні заходи оцінювання результатів навчання включають в себе поточний та підсумковий контроль.

**Поточний контроль.** До форм поточного контролю належить оцінювання:

- рівня знань під час практичних занять;
- якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку набутих здобувачем вищої освіти (далі – здобувач) знань, умінь та інших компетентностей з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну роботу виставляються в журналі обліку роботи академічної групи окремою графою за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

Результат навчальних занять за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок під час навчальних занять протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

Результат самостійної роботи за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок з самостійної роботи, отриманих протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи окремою графою.

***Здобувач, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний перескласти її.***

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переведу до 100-бальної системи множиться на коефіцієнт **10**.

$$\text{Загальна кількість балів (перед підсумковим контролем)} = \left( \frac{\text{Результат навчальних занять за семестр} + \text{Результат самостійної роботи за семестр}}{2} \right) * 10$$

**Підсумковий контроль.** Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструється в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображаються у відомостях обліку успішності, навчальних картках здобувачів, залікових книжках. ***Присутність здобувачів на проведенні підсумкового контролю (екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

***Підсумковий контроль (екзамен)*** оцінюється за національною шкалою. Для переведу результатів, набраних на підсумковому контролі, з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності здобувачів, становить **50**.

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру, та балів, набраних на підсумковому контролі (екзамені).

$$\text{Підсумкові бали навчальної дисципліни} = \text{Загальна кількість балів (перед підсумковим контролем)} + \text{Кількість балів за підсумковим контролем}$$

Здобувач вищої освіти, який під час складання підсумкового контролю (екзамен) отримав незадовільну оцінку, складає його повторно. Повторне складання підсумкового заліку допускається не більше двох разів з кожної навчальної дисципліни: один раз – викладачеві, а другий – комісії, до складу якої входить керівник відповідної кафедри та 2-3 науково-педагогічних працівника.

Критерії оцінювання здобувачів вищої освіти під час поточного контролю (робота на практичних заняттях) та підсумкового контролю. Кафедрою визначені наступні вимоги до здобувачів стосовно засвоєння змісту навчальної дисципліни (кількість оцінок, яку він повинен отримати під час аудиторної роботи, самостійної або індивідуальної роботи):

Робота під час навчальних занять	Самостійна робота	Підсумковий контроль
Отримати не менше 80% позитивних оцінок	Вирішити практичне завдання.	Отримати за підсумковий контроль не менше 30 балів

## 9. Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно («зараховано»)	A	«Відмінно» – теоретичний зміст курсу засвоєний цілком, потрібні практичні навички роботи з освоєним матеріалом сформовані, усі навчальні завдання, які передбачені програмою навчання, виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою
94-96			
90-93			
85-89	Добре («зараховано»)	B	«Дуже добре» – теоретичний зміст курсу засвоєний цілком, потрібні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані, якість виконання жодного з них не оцінена мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією-двома значними помилками.
80-84			
75 – 79			
70-74	Задовільно («зараховано»)	D	«Задовільно» – теоретичний зміст курсу засвоєний частково, але прогалини не носять істотний характер, потрібні практичні

65-69			навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконана, деякі з виконаних завдань містять помилки, робота з трьома значними помилками
60-64		Е	«Достатньо» – теоретичний зміст курсу засвоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконана або якість виконання деяких з них оцінена числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки
40-59	Незадовільно («не зараховано»)	FX	«Умовно незадовільно» – теоретичний зміст курсу засвоєний частково, потрібні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконана, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки
21-40			
1-20		F	«Безумовно незадовільно» – теоретичний зміст курсу не освоєний, потрібні практичні навички роботи несформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значного підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

## 10. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

### Основна література

1. Козюра В.Д. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: навчальний посібник / В.Д. Козюра, В.О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.
2. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2018. – 476 с.
3. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

### Додаткова література

4. ДСТУ 33960-96 Захист інформації. Технічний захист інформації. Основні положення.
5. ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
6. ДСТУ 33962-97 Захист інформації. Технічний захист інформації. Терміни та визначення;
7. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

8. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
11. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
12. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в АС.
13. НД ТЗІ 1.6-004-2013. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.

### **Інформаційні ресурси в Інтернеті:**

1. Державна служба спеціального зв'язку та захисту інформації (ДСЗЗІ) [Електронний ресурс]. – Режим доступу: <https://cip.gov.ua/ua>
2. Ю.Є. Яремчук, П.В. Павловський, В.С. Катаєв, В.В. Сінюгін. Комплексні системи захисту інформації / Навчальний посібник. [Електронний ресурс]. – Режим доступу: [https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk\\_kompleksni\\_systemy\\_zahystu\\_informaciyi/](https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/)