МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки, факультет №4

РОБОЧА ПРОГРАМА

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

125 «Кібербезпека»

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол № 10 від 22.10.2020___

СХВАЛЕНО
Вченою радою факультету № 4
Протокол № 6 від 21.10.2020___

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС _____
Протокол № 6 від 22.10.2020___

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (*протокол від 20.10.2020 № 19*)

Розробники:
1. *Доцент кафедри, к. т. н., доцент Соляник Т. М.*

Рецензенти:
1. Професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» д. т. н., професор Малєєва О. В.

2. Професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н., доцент Носов В. В.

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступень вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 5 Загальна кількість годин – 150 Кількість тем – 9	12 Інформаційні технології; (шифр галузі) (назва галузі знань) 125 – Кібербезпека бакалавр (назва СВО)	Навчальний курс – 4 Семестр – 7 Види підсумкового контрою: – залік
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання		заочна форма навчання
Лекції – 30 годин; Практичні заняття – 20 годин; Лабораторні заняття – 24 години; Самостійна робота – 76 годин; Індивідуальні завдання: Курсова робота – 1		Лекції – 8 години; Практичні заняття – 8 години; Лабораторні заняття – 10 годин; Самостійна робота – 124 годин; Індивідуальні завдання: Курсова робота – 1

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної 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.

Основними завданнями вивчення дисципліни „Комплексні системи захисту інформації: проектування, впровадження, супровід” є отримання студентами 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.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	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.	
Загальні компетентності (ЗК)	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.
Фахові Компетентності (ФК)	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 обґрунтовування 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. ФК 6. Здатність прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави та дестабілізуючі чинники.

3. Програма навчальної дисципліни

Тема № 1. Загальні питання організації та функціонування систем технічного захисту інформації.

Захист інформації: основні терміни та визначення. Класифікація інформації. Властивості інформації. Захист інформації в інформаційно-комунікаційних системах. Вимоги до захисту інформації.

Тема № 2. Нормативно-правова база України у сфері технічного захисту інформації.

Нормативні документи системи технічного захисту інформації. Поняття державного регулювання. Основні складові державного регулювання технічного захисту інформації.

Тема № 3. Комп’ютерні системи захисту інформації як об’єкт дослідження.

Об’єкт критичної інформаційної інфраструктури. Загальні положення інформаційних систем. Склад, структура та основні вимоги до комп’ютерних систем захисту інформації. Комплекси технічного захисту інформації. Комплекс

засобів захисту інформації в інформаційно-телекомунікаційних системах.

Тема № 4. Побудова комплексних систем захисту інформації.

Основні етапи створення комплексних систем захисту інформації. Передпроектні роботи зі створення КСЗІ. Обстеження середовищ функціонування ІТС. Аналіз ризиків та джерел загроз інформаційної безпеки. Оцінка захищеності інформації в інформаційно-комунікаційних системах. Модель загроз та модель порушника в ІТС.

Тема № 5. Процес створення комплексних систем захисту інформації.

Розробка Політики безпеки інформації в ІТС. Нормативно-методичні матеріали з організації захисту інформації. Розробка технічного завдання (ТЗ) на створення КСЗІ. Склад і отримання розділів ТЗ. Вимоги до засобів захисту інформації від несанкціонованого доступу та витоку інформації технічними каналами. Функціональні профілі захищеності. Вимоги до проектної та експлуатаційної документації

Тема № 6. Розробка проекту комплексних систем захисту інформації.

Стадії проектування. Ескізний проект, Технічний проект, Робоча документація. Нормативні документи та стандарти, що регламентують проектування КСЗІ в ІТС. Склад документів, що розробляються при проектуванні КСЗІ. Види документів на програмні засоби, що використовуються при створенні КСЗІ. Робоча та експлуатаційна документація КСЗІ. Управління проектами. Система розроблення та поставлення продукції на виробництво

Тема № 7. Введення комплексних систем захисту інформації в дію та оцінка захищеності інформації в ІТС.

Роботи з підготовки організаційної структури (Служба захисту інформації) та розробка розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС. Комплектування КСЗІ. Будівельно – монтажні та пусконалагоджувальні роботи. Випробування та атестація комплексу технічного захисту інформації. Програми та методики випробувань

Тема № 8. Експертиза комплексних систем захисту інформації.

Суб’єкти та об’єкти експертизи. Порядок організації та проведення експертизи. Програма та методика проведення експертизи. Приймальні випробування ІТС при функціонуючій в її складі КСЗІ.

Тема № 9. Впровадження та супровід КСЗІ.

Роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації (відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ). Гарантійне і післягарантійне технічне обслуговуванню засобів захисту інформації

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. Загальні питання організації та функціонування систем технічного захисту інформації.	**10**	**4**		**2**		**4**	
Тема № 2. Нормативно-правова база України у сфері технічного захисту інформації.	**16**	**2**		**2**		**12**	
Тема № 3. Комп'ютерні системи захисту інформації як об'єкт дослідження.	**18**	**4**		**2**		**12**	
Тема № 4. Побудова комплексних систем захисту інформації.	**18**	**4**		**2**	**4**	**8**	
Тема № 5. Процес створення комплексних систем захисту інформації.	**20**	**4**		**4**	**4**	**8**	
Тема № 6. Розробка проекту комплексних систем захисту інформації.	**18**	**4**		**2**	**4**	**8**	
Тема № 7. Введення комплексних систем захисту інформації в дію та оцінка захищеності інформації в ІТС.	**16**	**2**		**2**	**4**	**8**	
Тема № 8. Експертиза комплексних систем захисту інформації.	**18**	**4**		**2**	**4**	**8**	
Тема № 9. Впровадження та супровід КСЗІ.	**16**	**2**		**2**	**4**	**8**	
Всього по дисципліні	**150**	**30**		**20**	**24**	**76**	**Залік**

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. Загальні питання організації та функціонування систем технічного захисту інформації.	**41**	**2**		**2**	**4**	**33**	
Тема № 5. Побудова комплексних систем захисту інформації.	**58**	**4**		**4**	**4**	**46**	
Тема № 9. Впровадження та супровід КСЗІ.	**51**	**2**		**2**	**2**	**45**	
Всього по дисципліні	**150**	**8**		**8**	**10**	**124**	**Залік**

4.2. Завдання на самостійну роботу

Завдання що виносяться на самостійну роботу студента			Література:
Семестр №7			
	Тема № 1. Загальні питання організації та функціонування систем технічного захисту інформації.		
		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. Нормативно-правова база України у сфері технічного захисту інформації.		
		Міжвідомчі нормативно-правові документи.	Конспект лекцій, література [1-13]
		Внутрішньовідомчі нормативно-правові документи.	Конспект лекцій, література [1-13]
	Тема № 3. Комп’ютерні системи захисту інформації як об’єкт дослідження.		
		Основні види інформаційних систем.	Конспект лекцій, література [1-13]

		Типові класифікації інформаційних систем.	Конспект лекцій, література [1-13]
		Загальні вимоги до систем захисту інформації.	Конспект лекцій, література [1-13]
		Основні засоби захисту інформації.	Конспект лекцій, література [1-13]
	Тема № 4. Побудова комплексних систем захисту інформації.		
		Передпроектні роботи зі створення КСЗІ.	Конспект лекцій, література [1-13]
		Загальні принципи обстеження середовищ функціонування ІТС.	Конспект лекцій, література [1-13]
		Основні методи оцінювання захищеності інформації в ІТС.	Конспект лекцій, література [1-13]
		Основні ризики та джерела загроз в ІТС.	Конспект лекцій, література [1-13]
	Тема № 5. Процес створення комплексних систем захисту інформації.		
		Нормативно-методичні матеріали з організації захисту інформації.	Конспект лекцій, література [1-13]
		Основні положення технічного завдання на створення КСЗІ.	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. Розробка проекту комплексних систем захисту інформації.		
		Основні стадії проектування.	Конспект лекцій, література [1-13]
		Склад документів, що розробляються при проектуванні КСЗІ.	Конспект лекцій, література [1-13]
		Види документів на програмні засоби, що використовуються при створенні КСЗІ.	Конспект лекцій, література [1-13]
	Тема № 7. Введення комплексних систем захисту інформації в дію та оцінка захищеності інформації в ІТС.		
		Розпорядчі документи, що регламентують діяльність із забезпечення захисту інформації в ІТС.	Конспект лекцій, література [1-13]
		Будівельно – монтажні та пусконалагоджувальні роботи.	Конспект лекцій, література [1-13]
		Програми та методики випробувань комплексу технічного захисту інформації.	Конспект лекцій, література [1-13]
	Тема № 8. Експертиза комплексних систем захисту інформації.		
		Суб’єкти та об’єкти експертизи.	Конспект лекцій, література [1-13]
		Різновиди методів проведення експертиз.	Конспект лекцій, література [1-13]
	Тема № 9. Впровадження та супровід КСЗІ.		
		Основні положення організаційного забезпечення функціонування КСЗІ.	Конспект лекцій, література [1-13]
		Основні положення управління засобами захисту інформації	Конспект лекцій, література [1-13]

5. Індивідуальні завдання

5.1. Теми курсових робіт

1. Розробка системи захисту інформації для агентства з продажу нерухомості.
2. Розробка системи захисту інформації для кредитного відділу комерційного банку.
3. Розробка системи захисту інформації для бухгалтерії вищого навчального закладу.
4. Розробка системи захисту інформації для академії безперервної освіти.
5. Розробка системи захисту інформації для відділу виборчого комітету міської ради.
6. Розробка системи захисту інформації для інтернет-магазину продажу електротоварів.
7. Розробка системи захисту інформації для відділу кадрів комерційного банку.
8. Розробка системи захисту інформації для відділення фірми інтернет-провайдера.
9. Розробка системи захисту інформації для відділення комерційного банку.
10. Розробка системи захисту інформації для приватної конструкторської фірми.
11. Розробка системи захисту інформації для сховища даних супермаркету
12. Розробка системи захисту інформації для клінічної лабораторії.
13. Розробка системи захисту інформації для бібліотечного репозиторію кафедри.

6. Методи навчання

Вивчення курсу дозволить здобувачам вищої освіти оволодіти необхідними теоретичними знаннями щодо побудови та принципів функціонування комплексних систем захисту інформації. В навчальному плані для вивчення дисципліни передбачені такі організаційні форми занять як лекції, практичні та лабораторні заняття.

На лекційних заняттях викладаються теоретичні засади тем, що вивчаються, а також приклади їх використання для розв’язання конкретних навчальних задач.

На практичних заняттях під керівництвом викладача слухачі відпрацьовують прийоми виконання типових задач. Практичні заняття проводяться в комп’ютерному класі. Практичні заняття проводяться у здвоєному форматі, що дозволяє більш ефективно використовувати комп’ютерну техніку.

Перед практичним заняттям слухач повинен вивчити певний теоретичний матеріал і (можливо) виконати практичне завдання у відповідності до методичних вказівок до практичних занять з дисципліни. Після закінчення практичного заняття слухач отримує домашнє завдання для закріплення практичних навичок розв’язання задач.

Основним видом інформаційно-методичного забезпечення дисципліни є:

- конспект лекцій;
- методичні вказівки до практичних занять;
- навчальні посібники з дисципліни.

Перелічені складові елементи інформаційно-методичного забезпечення існують як у друкованому вигляді, так і в електронній формі у вигляді роздаткових матеріалів, відповідного розділу сайту кафедри кібербезпеки та інформаційних систем, а також у вигляді електронного навчального комплексу з дисципліни у системі ДО ХНУВС.

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

1. Що таке інформація? Види інформації.
2. Поняття доступу до інформації. Інформація з обмеженим доступом.
3. Що таке інформаційна взаємодія? Суб'єкти та об'єкти інформаційної взаємодії.
4. Які властивості інформації існують? Навести приклади.
5. Що таке загроза? Види загроз.
6. Що таке захист інформації?
7. Що таке технічний захист інформації?
8. Хто є суб'єктами відносин, пов'язаних із захистом інформації в системах?
9. Що таке комунікабельність носіїв інформації? Навести приклади комунікабельних та некомунікабельних носіїв.
10. Що таке режимна адекватність носіїв інформації? Навести приклади.
11. Які основні складові нормативно-правової бази України Ви знаєте?
12. Які основні аспекти технічного захисту інформації в Україні регулюються державою?
13. Що таке об'єкт критичної інфраструктури? Навести приклади.
14. Що таке критична інфраструктура?
15. Що таке об'єкт критичної інформаційної інфраструктури? Навести приклади.
16. Що таке критичні бізнес/операційні процеси об'єкта критичної інфраструктури?
17. Що таке Інформаційна система?
18. Які види інформаційних систем існують?
19. Назвіть загальні вимоги до кіберзахисту об'єкта критичної інфраструктури.
20. Що забезпечується організаційними та технічними заходами з кіберзахисту?
21. У чому полягає загальна політика інформаційної безпеки?
22. Що забезпечується управлінням доступом користувачів та адміністраторів до об'єктів критичної інфраструктури?
23. У чому полягає ідентифікація та автентифікація користувачів та адміністраторів об'єкта критичної інфраструктури?
24. Для чого використовують реєстрацію подій компонентами об'єкта критичної інфраструктури, чи потрібен їх періодичний аудит?

25. Що таке забезпечення мережевого захисту компонентів та інформаційних ресурсів об’єкта критичної інфраструктури?
26. Що таке забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об’єкта критичної інфраструктури?
27. Що визначається умовами використання програмного та апаратного забезпечення об’єкта критичної інфраструктури?
28. Які вимоги до умов розміщення компонентів об’єкта критичної інфраструктури існують?
29. Які варіанти захисту інформації можливі?
30. Які основні етапи технічного захисту інформації існують?
31. У чому полягає визначення й аналіз загроз?
32. Яким чином можуть здійснюватися загрози?
33. Що таке ситуаційна карта об’єкта критичної інфраструктури?
34. Що таке окрема модель загроз?
35. З яких основних етапів складається процес обстеження об’єкта критичної інфраструктури?
36. Які основні складові окремої моделі загроз Ви знаєте?
37. Що таке технічне завдання на розробку системи захисту інформації? Які основні розділи технічного завдання?
38. Які документи містить план технічного захисту інформації?
39. Які заходи захисту інформації з обмеженим доступом може містити план технічного захисту інформації?
40. Що виконується у процесі розроблення і реалізації організаційних заходів?
41. Що забезпечується під час реалізації первинних технічних заходів?
42. Яким чином здійснюється блокування каналів витоку інформації?
43. Яким чином здійснюється блокування несанкційованого доступу до інформації або її носіїв?
44. Що виконується у процесі реалізації основних технічних заходів захисту?
45. Для чого використовують програмні засоби захисту інформації?
46. Що таке спеціальні інженерно-технічні споруди, засоби та системи? Навести приклади.
47. Які основні вимоги до заходів захисту інформації існують?
48. Що таке рівень захисту інформації?
49. Які рівні захисту інформації існують?
50. Що є об’єктом атестації технічного захисту інформації?
51. Що виконується у ході атестації?
52. У чому полягає реалізація технічного плану захисту інформації?
53. У чому полягає контроль функціонування системи захисту інформації?
54. У чому полягає управління системою захисту інформації?

8. Розподіл балів, які отримують здобувачі вищої освіти з навчальної дисципліни

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних, лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти 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 національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи в окрему графу за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів вищої освіти в Університеті враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

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 в окрему графу.

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 в окрему графу.

Здобувач вищої освіти***, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний його відпрацювати.***

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 переводу до 100-бальної системи помножується на коефіцієнт **10**.

Загальна кількість балів (перед підсумковим контролем)	***=((***	***Результат навчальних занять за семестр***	***+***	***Результат самостійної роботи за семестр***	***) /***	***2)***	****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 реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках курсантів (студентів, слухачів), залікових книжках. ***Присутність курсантів (студентів, слухачів) на проведенні підсумкового контролю (заліку, 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, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі (екзамені, заліку), 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 курсантів (студентів, слухачів), становить – **50.**

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

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

Здобувач вищої освіти, який під час складання підсумкового контролю отримав оцінку «незадовільно», складає підсумковий контроль (екзамен, залік) повторно. Повторне складання підсумкового контролю (екзамену, заліку) допускається не більше двох разів з кожної навчальної дисципліни, у тому числі один раз – викладачеві, а другий – комісії, що створюється навчально-науковими інститутами (факультетами). Незадовільні оцінки виставляються тільки в відомостях обліку успішності. Студентам, які отримали не більше як дві незадовільні оцінки (нижче ніж 60 балів) з навчальної дисципліни, можуть бути встановлені різні строки ліквідації академічної заборгованості, але не пізніше як за день до фактичного початку навчальних занять у наступному семестрі. Студенти, які не ліквідували академічну заборгованість у встановлений термін, відраховуються з Університету. Особи, які одержали більше двох незадовільних оцінок (нижче ніж 60 балів) за підсумковими результатами вивчення навчальних дисциплін з урахуванням підсумкового контролю, відраховуються з Університету.

Результат вивчення дисципліни визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\textit{Підсумкові бали навчальної дисципліни} = (\textit{Підсумкові бали за поточний семестр} + \textit{Підсумкові бали за попередній семестр}) : 2$$

Кафедрою визначено наступні критерії оцінювання результатів роботи здобувачів вищої освіти під час поточного контролю (роботу на семінарських, практичних, лабораторних й інших аудиторних заняттях, виконання самостійних навчальних та індивідуальних творчих завдань) та підсумкового контролю.

Робота під час навчальних занять	Самостійна та індивідуальна робота	Підсумковий контроль
Отримати не менше 4 позитивних оцінок (денна форма навчання)	Підготувати реферат, підготувати конспект за темами самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка**	
		Оцінка	**Пояснення**
97-100	Відмінно («зараховано»)	A	«**Відмінно"** – теоретичний зміст курсу засвоєний **цілком,** необхідні 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, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **більшості** з них оцінена числом балів, близьким до **максимального,** робота з двома-трьома незначними помилками.
80-84			
75-79		C	«**Добре"** – теоретичний зміст курсу засвоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** 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.
70 -74	Задовільно («зараховано»)	D	«**Задовільно"** – теоретичний зміст курсу засвоєний **частково**, але **прогалини не носять істотний** характер, потрібні практичні 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.
65-69			
60-64		E	«**Достатньо"** – теоретичний зміст курсу освоєний **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.
41-59	Незадовільно («не зараховано»)	FX	«**Умовно незадовільно"** – теоретичний зміст курсу засвоєний **частково**, потрібні практичні навички роботи **несформовані, більшість** передбачених програмою навчання, навчальних завдань **не виконано**, 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 **неосвоєний**, 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, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Інформаційна безпека / Ю. Я. Бобал [та ін.]; за ред. Ю. Я. Бобала, І. В. Горбатого . – Львівська політехніка, 2019. – 580 с.
2. Schneier, Bruce. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition edition // Bruce Schneier. – 2017. – 784 p.
3. Matt Walker. CEH Certified Ethical Hacker All-in-One Exam Guide. McGraw-Hill, 2012.
4. ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications. / ITU-T Recommendation X.805, 10/2003. URL: https://www.itu.int/rec/T-REC-X.805-200310-I/en (дата звернення: 20.09.2016).
5. Конспект лекцій.

Допоміжна

1. Грищук, Р. Основи кібербезпеки / Р. Грищук, Ю. Даник. – Житомир : ЖНАЕУ, 2016. – 636 с.
2. Основи захисту інформації: навч. посіб. / Ю. Даник, С. Вдовенко, В. Шестаков, О. Писарчук, Р. Грищук, М. Куликівський, В. Ходаківський. – Жито-мир: ЖВІ ДУТ, 2015. – 220 с.
3. Бурячок, В. Політика інформаційної безпеки. / В. Бурячок, Р. Грищук, В. Хорошко. – ПВП «Задруга», 2014. – 222 с.
4. Корченко, А. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія / А. Корченко, О. Архипов, Ю. Дрейс. – К: наук.-вид. центр НА СБУ України, 2014. – 332 с.
5. Остапов, С.Е. Технології захисту інформації / С.Е. Остапов, С.П. Євсеєв, О. Г. Король. – Родовід, 2014. – 428 с.
6. Забезпечення інформаційної безпеки держави / І. Іванченко [та ін.]; за ред. проф. В. Хорошка. – К: ПВП «Задруга», 2013. – 170 с.
7. Юдін, О. Інформаційна безпека. Нормативно-правове забезпечення / О. Юдін. – К.: НАУ, 2011. – 640 с.
8. Голубєв, В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк; за заг. ред. Р. А. Калюжного. – Запоріжжя: Просвіта, 2001. – 252 с.

Інформаційні ресурси в Інтернеті

1. Про інформацію: Закон України від 25 квітня 2019 року N 2704-VIII. URL: http://www.ukrstat.gov.ua/Zakon/ukr/lawinform.html (дата звернення: 01.09.2020)
2. Про державну таємницю: Закон України від 15.08.2020 № 3855-XII URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 01.09.2020)
3. Про доступ до публічної інформації: Закон України від 15.08.2020, № 3856-XII URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 01.09.2020)
4. Про захист персональних даних: Закон України від 20.03.2020, № 2297-VI URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.09.2020)
5. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 03.07.2020, № 3475-IV URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 01.09.2020)
6. Про основні засади забезпечення кібербезпеки України: Закон України від 03.07.2020, № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.09.2020)
7. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. –Чинний з 1997-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.
8. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. –Чинний з 1997-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.
9. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Терміни та визначення. –Чинний з 1998-01-01. – К.: Держспоживстандарт України, 1997. – 11 с.