

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ
СПРАВ
Кафедра кібербезпеки та DATA-технологій, факультет №6**

РОБОЧА ПРОГРАМА

навчальної дисципліни «Кібербезпека»
обов'язкових компонент освітньої програми
першого (бакалаврського) рівня вищої освіти

**Спеціальність: 125 «Кібербезпека та захист інформації»
(«Безпека інформаційних та комунікаційних систем»)**

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)

Розробники:

Професор кафедри, к.т.н., доцент; Струков В. М.;

Старший викладач, Цуранов М.В.;

Рецензенти:

- 1. Певнєв В.Я., д.т.н., доцент, професор кафедри комп'ютерних систем, мереж та кібербезпеки факультету радіоелектроніки, комп'ютерних систем та інфокомунікацій НАУ «ХАІ» ім. М.Є. Жуковського;*
- 2. Світличний В.А., к.т.н., доцент, доцент кафедри протидії кіберзлочинності факультету №4 ХНУВС.*

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 – 10 Загальна кількість годин – 300 Кількість тем - 12	12 Інформаційні технології; 125 Кібербезпека (Безпека інформаційних та комунікаційних систем) перший (бакалаврський) рівень вищої освіти	Навчальний курс – 3 Семестр – 6 Види контролю – залік
Розподіл навчальної дисципліни за видами занять:		
<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p style="text-align: center;">денна форма навчання VII семестр</p> <p>Лекції – $\frac{72}{\text{(години)}}$;</p> <p>Семінарські заняття – $\frac{\quad}{\text{(години)}}$;</p> <p>Практичні заняття – $\frac{30}{\text{(години)}}$;</p> <p>Лабораторні заняття – $\frac{48}{\text{(години)}}$;</p> <p>Самостійна робота – $\frac{150}{\text{(години)}}$;</p> </div> <div style="width: 45%;"> <p style="text-align: center;">заочна форма навчання VII семестр</p> <p>Лекції – $\frac{6}{\text{(години)}}$;</p> <p>Семінарські заняття – $\frac{\quad}{\text{(години)}}$;</p> <p>Практичні заняття – $\frac{6}{\text{(години)}}$;</p> <p>Лабораторні заняття – $\frac{10}{\text{(години)}}$;</p> <p>Самостійна робота – $\frac{278}{\text{(години)}}$;</p> </div> </div>		

2. Мета та завдання навчальної дисципліни

Метою викладання навчальної дисципліни "Кібербезпека" є діяльності на основі застосування системи теоретичних знань і практичних навичок з виявлення способів порушення інформаційної безпеки при роботі комп'ютерних систем обробки інформації; вирішення задач захисту програм та даних програмно-апаратними засобами; застосування системного підходу до забезпечення інформаційної безпеки, включаючи комплекс організаційних заходів.

Завдання застосовувати знання до вирішення задач інформаційної безпеки; обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації; аналізувати вхідні данні та обирати методи оцінки якості систем та моделей, а також:

– придбати знання про сучасних технологій захисту інформації в локальних і глобальних мережах.

Міждисциплінарні зв'язки : науковий фундамент дисципліни пов'язаний з такими дисциплінами як «Інформаційні технології», «Архітектура та структурно-логічні основи ЕОМ», «Алгоритмізація та програмування», «Прикладна криптологія», «Системне програмування», «Операційні системи та комп'ютерні мережі», «Теорія інформації та кодування» та ін.

Очікувані результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен

знати:

- загальні аспекти проблематики в галузі інформаційної безпеки (сучасний стан задач та проблем, загрози та види руйнівних програм та атаки на інформаційні та комунікаційні системи, вимоги до їх захищеності).
- встановлену політику інформаційної та/або кібербезпеки.
- методи забезпечування захисту інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки..
- характеристику методів реалізації основних функцій системи захисту інформації.
- принципи відновлювання штатного функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.

вміти:

- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-комунікаційних системах
- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної та/або кібербезпеки.
- вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки
- забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах
- вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-комунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
- виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
- впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

Форма підсумкового контролю - залік.

На вивчення навчальної дисципліни відводиться 150 годин/5 кредитів ECTS.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.	
Загальні компетентності (ЗК)	ЗК 1	Здатність застосовувати знання у практичних ситуаціях.
	ЗК 5	Здатність до пошуку, оброблення та аналізу інформації.
Спеціальні (фахові, предметні) компетентності (СК)	ФК 2	Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	ФК 3	Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
Програмні результати навчання	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 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 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 інформаційнотелекомунікаційних систем
ПРН 11.	виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах
ПРН 12	розробляти моделі загроз та порушника
ПРН 13	аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних
ПРН 14.	вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень
ПРН 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 інформаційнотелекомунікаційних (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 для 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 22	вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\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 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 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 для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
ПРН 32	вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
ПРН 42	впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
ПРН 43	застосовувати національні та міжнародні регулюючі акти в 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 рині класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-

	орієнтованому контролю доступу до інформаційних активів;
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 53.	вирішувати задачі аналізу програмного коду на наявність можливих загроз
ПРН 57.	проводити кримінальний аналіз при вирішенні завдань поліцейської діяльності

1. Програма навчальної дисципліни.

Тема № 1. Методи та моделі захисту інформації.

Загрози безпеки для ІТС. Застосування сервісів безпеки до рівнів безпеки ІТС. Визначення суб'єктів та об'єктів в моделях ЗІ. Мандатні моделі ЗІ. суб'єктно-об'єктні моделі ЗІ. Монітори безпеки. МБО. МБС. ІПС. Ядро безпеки.

Тема № 2. Захист інформації в обчислювальних мережах.

Загрози обчислювальним мережам. Методи захисту мереж. Механізми забезпечення безпеки. Огляд сучасних тенденцій резервного зберігання даних. Огляд систем резервного копіювання.

Тема № 3. Побудова захищених локальних мереж.

ІР-протокол та його версії. Веб-браузер та його місце у правопорушеннях. Способи виявлення прихованої ІР-адреси. Принципи побудови захищених локальних мереж. Фізичне розділення мережі.. VPN мережі. Захищенні оптичні локальні мережі.

Тема № 4. Побудова систем відеоспостереження.

Структура та основні елементи. Основні параметри камер відеоспостереження. Пристрої обробки відеосигналів. Аналогові системи. Цифрові системи. Комбіновані системи. Пересилання пакетів. Шлюзи. Принципи побудови захищеної мережі відео нагляду.

Тема № 5. Антивірусний захист.

Загальна характеристика та класифікація комп'ютерних вірусів. Фізична структура комп'ютерного вірусу. Зараження програми. Файловий транзитний вірус. Бутовий вірус. Stealth-вірус. Поліморфні віруси. Макровіруси. Мережеві віруси. Характеристика засобів нейтралізації комп'ютерних вірусів. Антивіруси. Детектори. Фаги. Вакцини. Щеплення. Ревізори. Монітори. Методів захисту від комп'ютерних вірусів. Архівування. Вхідний контроль. Профілактика. Ревізія. Карантин. Сегментація. Фільтрація. Вакцинація. Автоконтроль цілісності. Терапія. Інтегрований програмний комплекс. Каталог детекторів. Програма-пастка вірусів. Програма для вакцинації. База даних про віруси і їх характеристиках. Резидентні засоби захисту. Технології виявлення шкідливого

коду. Модель системи захисту від шкідливих програм. Технічний компонент. Аналітичний компонент.

Тема № 6. Принципи створення шкідливого програмного забезпечення.

Загальна характеристика шкідливого програмного забезпечення (malware) та комп'ютерних загроз. Класичні комп'ютерні віруси. Мережеві хробаки. Троянські програми (TrojWare). Руткіти (Rootkit).

Тема № 7. Методи фільтрації спаму.

Характеристика спаму та осіб що його відправляють. Засоби боротьби зі спамом. фільтр Байєса.

Тема № 8. Брандмауери.

Програмні та апаратні брандмауери, принципи реалізації. Принципи реалізації та використання брандмауерів в ОС Windows. Принципи реалізації та використання брандмауерів в ОС Linux, MacOS.

Тема № 9. Характеристика хакерів.

Визначення та походження терміну хакер. Характеристика хакерських атак та їх види. Характеристика експлоїтів. Способи використання експлоїтів. Способи захисту від експлоїтів.

Тема № 10. Методи і засоби сканування вузлів мережі.

Концепція протоколів стека TCP/IP. Виявлення відкритих мережних портів. Ідентифікація запущених TCP- и UDP-служб. Методи визначення операційної системи.

Тема № 11. Методи захисту ПЗ.

Необхідність захисту ПЗ. Загрози безпеці ПЗ. Використання захисту ПЗ. Види захисту ПЗ від злому й неконтрольованого розповсюдження. Аналіз систем захисту ПЗ.

Тема № 12. Генерація та використання Blockchain.

Огляд алгоритмів консенсусу у Блокчейні. Підтвердження виконання роботи та Підтвердження частки. Завдання візантійських генералів. Децентралізовані дані. Децентралізовані цінності. Децентралізована ідентичність. Децентралізовані обчислення.

4. Структура навчальної дисципліни
4.1. 1. Розподіл часу навчальної дисципліни за темами
(денна форма навчання)

Номер та найменування теми	Кількість годин відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр 6							
Тема № 1. Методи та моделі захисту інформації.	29	8		2	4	15	
Тема № 2. Захист інформації в обчислювальних мережах.	22	6		2	4	10	
Тема № 3. Побудова захищених локальних мереж.	22	6		2	4	10	
Тема № 4. Побудова систем відеоспостереження.	20	6		4		10	
Тема № 5. Антивірусний захист.	31	6		2	8	15	
Тема № 6. Принципи створення шкідливого програмного забезпечення.	26	6		2	8	10	
Тема № 7. Методи фільтрації спаму.	18	2		2	4	10	
Тема № 8. Брандмауери.	22	6		6		10	
Тема № 9. Характеристика хакерів.	23	2		2	4	15	
Тема № 10. Методи і засоби сканування вузлів мережі.	29	8		2	4	15	
Тема № 11. Методи захисту ПЗ.	29	8		2	4	15	
Тема № 12. Генерація та використання Blockchain.	29	8		2	4	15	
Всього за семестр № 2:	300	72		30	48	150	залік

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

Номер та найменування теми	Кількість годин відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр 6							
Тема № 1. Методи та моделі захисту інформації.	14	2		2		20	
Тема № 2. Захист інформації в обчислювальних мережах.	14					30	
Тема № 3. Побудова захищених локальних мереж.	14					30	
Тема № 4. Побудова систем відеоспостереження.	16					20	
Тема № 5. Антивірусний захист.	22	2			4	20	
Тема № 6. Принципи створення шкідливого програмного забезпечення.	25				2	30	
Тема № 7. Методи фільтрації спаму.	20					20	
Тема № 8. Брандмауери.	25					20	
Тема № 9. Характеристика хакерів.				2		20	
Тема № 10. Методи і засоби сканування вузлів мережі.					4	20	
Тема № 11. Методи захисту ПЗ.						20	
Тема № 12. Генерація та використання Blockchain.		2		2		28	
Всього за семестр № 2:	150	72		6	10	278	залік

4.1.3. Питання, що виносяться на самостійне опрацювання.

Перелік питань до тем навчальної дисципліни		Література:
Тема № 1. Методи та моделі захисту інформації.		1-6-основна
	Модель порушника. Види політики безпеки. Використання політик безпеки.	
	Ізольоване програмне середовища	
Тема № 2. Захист інформації в обчислювальних мережах.		1-6-основна, 1-допоміжна
	Оцінка ризиків витоку інформації в мережах.	
	Організаційні методи захисту корпоративних мереж.	
Тема № 3. Побудова захищених локальних мереж.		1-6-основна, 1-4- допоміжна
	Оптичні локальні мережі.	
	SIEM системи. Принципи аналізу трафіку на наявність конфіденційної інформації.	
Тема № 4. Побудова систем відеоспостереження.		1-6-основна
	Побудова аналогових систем відеоспостереження. Необхідність аналогових систем.	
	Функціонал ПЗ для відеоспостереження.	
Тема № 5. Антивірусний захист.		1-6-основна, Інформаційні ресурси
	Про активні антивіруси. Принципи побудови HIPS антивірусів. Системи виявлення вторгнень.	
Тема № 6. Принципи створення шкідливого програмного забезпечення.		1-6-основна, інформаційні ресурси
	Принципи створення корисного навантаження в Metasploit. Нешкідливі віруси. Піратське ПЗ як засіб розповсюдження вірусів.	
Тема № 7. Методи фільтрації спаму.		1-5-основна 1-4- допоміжна, інформаційні ресурси
	Налаштування спам фільтрів для користувача. Адміністрування спам фільтрів	
Тема № 8. Брандмауери.		3-5-основна, інформаційні ресурси
	Навчання брандмауерів. Правила OAWSP для брандмауерів.	
Тема № 9. Характеристика хакерів.		3-5-основна, інформаційні ресурси
	Білі та чорні хакери. Інструменти для виконання тесту на проникнення. Хмарні технології для хакерів.	
Тема № 10. Методи і засоби сканування вузлів мережі.		3-5-основна, інформаційні ресурси
	Використання мережевих утиліт для сканування.	

	Тема № 11. Методи захисту ПЗ.	3-5-основна, інформаційні ресурси
	Принцип легальне гірше ніж піратське. Сучасні принципи онлайн захисту ПЗ.	
	Тема № 12. Генерація та використання Blockchain.	3-5-основна інформаційні ресурси
	Алгоритми консенсусу. Використання децентралізованих мереж на практиці. Криптові біржі.	

5. Індивідуальні завдання

5.1. Теми рефератів

1. Порівняльний аналіз безкоштовних сервісів VPN в глобальній мережі.
2. Технології TOR мережі.
3. Технології часникової маршрутизації.
4. Технології I2P мережі.
5. Принципи побудови Mash мереж.
6. Порівняльний аналіз безкоштовних персональних міжмережних екранів.
7. Порівняльний аналіз ОС тестування на вразливість до атак.
8. Використання технології Blockchain в Україні.
9. Використання технології Blockchain. Світова практика.

5.2. Теми курсових робіт

1. Аналіз та практична оцінка сервісів і програмних засобів збору інформації про веб-сайти.
2. Аналіз та практична оцінка програмних засобів збору інформації, що використовують пошуковий сервіс Google.
3. Аналіз та практична оцінка сервісів і програмних засобів збору інформації із сервісу Whois.
4. Аналіз та практична оцінка сервісів і програмних засобів збору інформації із серверів DNS.
5. Аналіз та практична оцінка сервісів і програмних засобів збору інформації про логічну і фізичну структуру віддаленої мережі.
6. Аналіз та практична оцінка сервісів і програмних засобів комплексного збору інформації в глобальній мережі.
7. Збір інформації про вузли та мережні пристрої за допомогою Shodan.
8. Аналіз та практична оцінка сервісів і програмних засобів побудови та аналізу зв'язків між частинами отриманої інформації.
9. Аналіз та практична оцінка сервісів і програмних засобів збору інформації за заголовками електронної пошти.
10. Аналіз та практична оцінка сервісів і програмних засобів OSINT.

11. Аналіз та практична оцінка сервісів і програмних засобів визначення типу і версії ОС вузла.
12. Аналіз та практична оцінка програмних засобів отримання інформації з NetBIOS.
13. Аналіз та практична оцінка програмних засобів отримання інформації з SMTP.
14. Аналіз та практична оцінка сервісів і програмних засобів пошуку вразливостей.
15. Аналіз та практична оцінка програмних засобів створення SSH-тунелю.
16. Аналіз та практична оцінка програмних засобів виявлення вторгнень.
17. Аналіз та практична оцінка програмних засобів міжмережного керування доступу.
18. Аналіз та практична оцінка програмних засобів Honeypot.
19. Аналіз та практична оцінка програмних засобів підбору гешів.
20. Аналіз та практична оцінка програмних засобів перехоплення і Порівняльний аналізу мережного трафіку.
21. Аналіз та практична оцінка програмних засобів реалізації MAC затоплення та ARP Spoofing.
22. Аналіз та практична оцінка програмних засобів атаки на DHCP сервер.
23. Аналіз та практична оцінка програмних засобів MITM атак.
24. Аналіз та практична оцінка програмних засобів вивчення та доступу до безпроводних мереж.
25. Аналіз та практична оцінка програмних засобів прискорення підбору паролів.
26. Аналіз та практична оцінка програмних засобів DoS атаки на безпроводні мережі.
27. Аналіз та практична оцінка програмних засобів створення шкідливого програмного забезпечення.
28. Аналіз та практична оцінка програмних засобів дослідження вразливостей веб-сервера.
29. Аналіз та практична оцінка програмних засобів експлуатації вразливостей операційної системи.
30. Аналіз та практична оцінка програмних засобів експлуатації вразливостей веб-сервера.
31. Аналіз та практична оцінка програмних засобів завантаження та виконання довільних файлів.
32. Аналіз та практична оцінка програмних засобів, що реалізують міжсайтову підробку запиту (Cross Site Request Forgery).

33. Аналіз та практична оцінка програмних засобів, що реалізують міжсайтовий скриптинг (Cross Site Scripting).
34. Аналіз та практична оцінка програмних засобів, що реалізують атаку "відмова в обслуговуванні".
35. Аналіз та практична оцінка програмних засобів, що реалізують SQL-ін'єкції.
36. Аналіз та практична оцінка програмних засобів соціальної інженерії.

6. Методи навчання

Навчання з дисципліни проходить у формі:

для денної форми навчання:

- лекцій (36 занять, 72 години);
- практичних занять (15 занять, 30 годин);
- лабораторних занять (12 занять, 48 годин);
- самостійної роботи (150 години);

для заочної форми навчання:

- лекцій (3 заняття, 6 годин);
- практичних занять (3 заняття, 6 годин);
- лабораторних занять (3 заняття, 10 годин);
- самостійної роботи (278 годин);

Аудиторні заняття проводяться у формі візуального представлення аналітично-графічного матеріалу дисципліни, на яких курсанти повинні виконувати відповідні розмови, обчислювальні та практичні дії.

Самостійна робота за кожною темою передбачає вивчення теоретичних питань лекційних занять, опрацювання завдань практичних і лабораторних занять.

Індивідуальна робота передбачає написання рефератів.

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

1. Наведіть класифікацію збоїв та порушення прав доступу до мережі.
2. Опишіть програмно-апаратні комплекси захисту системи архівування та дублювання інформації.
3. Опишіть можливі напрями витоку інформації у обчислювальних мережах.
4. Опишіть заходи захисту обчислювальних мереж.
5. Опишіть організаційно-технічні заходи захисту обчислювальних мереж.
6. Опишіть технічні засоби захисту обчислювальних мереж.
7. Охарактеризуйте основні компоненти Kerberos.
8. Коротко опишіть механізми безпеки в обчислювальних мережах.
9. Назвіть механізми захисту від зовнішніх загроз у обчислювальних мережах.
10. Назвіть вимоги до систем резервного копіювання.

- 11.Опишіть категорію PBVA систем.
- 12.Опишіть основні відмінності систем резервного копіювання.
- 13.Опишіть базові та розширені функції систем резервного копіювання.
- 14.Коротко опишіть переваги та недоліки систем резервного копіювання присутніх на українському ринку.
- 15.Охарактеризуйте протокол IP. Опишіть основні відмінності четвертої та шостої версії протоколу IP.
- 16.Дайте визначення класової та безкласової адресації.
- 17.Назвіть основні відмінності статичної динамічної IP-адреси. Дайте визначення терміну веб-браузер.
- 18.Дайте визначення терміну cookies, як cookies допомагають розкрити IP-адресу хакера? Як скрипти допомагають визначити IP-адресу комп'ютера?
- 19.Опишіть мову програмування Java, чому ця мова дозволяє дізнатися IP-адресу.
- 20.Опишіть основне призначення технології ActiveX, чому ця технологія допомагає визначити адресу атакуючого комп'ютера?
- 21.Які існують засоби захисту від визначення IP-адреси?
- 22.Дайте визначення терміну експлоїт. Назвіть дві основні вразливості, які використовують для атак хакерів, опишіть їх основні переваги.
- 23.Зобразіть структуру локальної мережі з фізичним поділом КС та ІС. Коротко охарактеризуйте основні засади фізичного розподілу мережі.
24. Опишіть принцип роботи АРМ «СЕТЬ» схематично зобразіть її роботу.
- 25.Опишіть основні переваги використання мережевих компонентів СКС АМР.
- 26.Перерахуйте основні заходи, які необхідно застосовувати для захисту локальної мережі ПЕМІН.
- 27.Схематично зобразіть схему безпечної оптичної мережі. Що включає базовий модуль ТК ОКИ?
- 28.Опишіть принцип роботи захищеної локальної оптичної мережі.
- 29.Зобразіть типову структуру системи IP-відеоспостереження, назвіть основні завдання, які вона вирішує.
- 30.Дайте визначення аналогової системи відеоспостереження, намалюйте таку систему.
- 31.Опишіть основні параметри камер відеоспостереження, назвіть основні відмінності внутрішніх та зовнішніх камер.
- 32.Які пристрої обробки відео ви знаєте? Назвіть основні характеристики.
- 33.Опишіть основні варіанти побудови систем відеоспостереження.
- 34.Опишіть основні завдання, які виникають під час проектування мереж відеоспостереження.
- 35.Опишіть основні технології захисту даних у мережах відеоспостереження.
- 36.Дайте визначення терміну спам. Опишіть превентивні способи боротьби зі спамом.
- 37.Яким чином адреси електронної пошти можуть потрапити до списку спам розсилки? Опишіть основні засоби боротьби зі спамом.

- 38.Опишіть принцип роботи фільтра Байєса. Напишіть основну формулу роботи фільтра Байєса. Назвіть переваги та недоліки фільтра Байєса.
- 39.Назвіть основні відмінності розподілених чорних списків від сірих списків. Назвіть переваги та недоліки використання сірих списків.
- 40.Охарактеризуйте хакера як фахівця, назвіть основні відмінності хакера від крекера.
- 41.Опишіть атаку хакерів у широкому і вузькому сенсі. Порівняйте хакерську атаку із крекерською атакою.
- 42.Опишіть атаки типу: Mailbombing, сніффінг пакетів та переповнення буфера.
- 43.Опишіть атаки типу: Man-in-the-Middle, ін'єкція та соціальна інженерія.
- 44.Наведіть класифікацію експлоїтів.
- 45.Опишіть види експлоїтів. Для чого потрібні експлоїти?
- 46.Як користуватись експлоїтом? Як написати експлоїт?
- 47.Назвіть основні засоби захисту від експлоїтів.
- 48.Навіщо призначений механізм трансляції адрес? Які існують види трансляції адрес і чим вони відрізняються? Як механізм трансляції адрес захищає внутрішній вміст мережі?
- 49.Що таке брандмауер-система та які функції та завдання вона виконує? Що таке загальна довірча точка та які переваги її використання?
- 50.Назвіть стандартні служби безпеки брандмауер-систем. Які заходи захисту вживаються кожною з цих служб, і які фактори впливають на їхню безпеку та надійність?
- 51.Які основні концепції були розроблені під час проектування брандмауерів? Що вони означають?
- 52.Перерахуйте основні елементи брандмауерів. За виконання яких функцій відповідальний кожен з них?
- 53.З яких програмних секцій складається брандмауер? За виконання яких функцій відповідальна кожна із секцій?
- 54.Поясніть призначення пакетних фільтрів. Яку інформацію фільтрують пакетні фільтри та які механізми при цьому використовуються? Чим вони відрізняються від механізмів, які застосовуються в маршрутизаторах?
- 55.Які завдання можна розв'язувати за допомогою шлюзів прикладного рівня? Чим механізми фільтрації на прикладному рівні відрізняються від механізмів на мережному рівні?
- 56.Чи є ефективним (з метою підвищення рівня захищеності системи) комбінування пакетних фільтрів та шлюзів прикладного рівня та чому? Назвіть кілька різновидів такого поєднання.
- 57.Перерахуйте різновиди атак на брандмауер-системи. Які з них є найпоширенішими, а які менш поширеними? Як ці атаки можуть знижувати рівень захисту системи?
- 58.Перерахуйте види атак на брандмауер-системи. Чи всі з них однаково успішно припиняються брандмауерами?
- 59.Які дії користувачів та розробників системи можуть призвести до зниження рівня захищеності брандмауер-системи?

60. Що таке концепція універсального брандмауера? Які вимоги висуваються до партнерів з комунікації всередині та поза організацією?
61. Коротко напишіть концепцію протоколів TCP/IP.
62. Опишіть port scanning та його основні типи.
63. Коротко напишіть утиліти UNIX для ідентифікації запущених служб.
64. Опишіть утиліти сканування портів для Windows.
65. Опишіть механізми захисту від сканування портів.
66. Які процедури необхідно виконати визначення версії ОС.
67. Які загрози виникають під час підключення корпоративної мережі до відкритої мережі? Як VPN допомагає мінімізувати загрози?
68. Опишіть принципи створення VPN тунелю, які пристрої VPN існують?
69. Які варіанти побудови віртуальних захищених каналів?
70. Опишіть засоби безпеки VPN.
71. Наведіть коротку класифікацію мереж VPN. Які варіанти архітектури мереж VPN ви знаєте?
72. Опишіть типові етапи Penetration Testing.
73. Опишіть списки категорій Чезовика та Белловіна.
74. Наведіть приклад матричної класифікації Лендвейра.
75. Опишіть класифікацію атак Ховарда.
76. Наведіть приклад побудови онтології мережеских атак.
77. Опишіть процес роботи мережеских сканерів безпеки.
78. Чому соціальна інженерія ефективна? Які заходи протидії соціальній інженерії ви знаєте?
79. Опишіть основні техніки та категорії соціальної інженерії.
80. Перерахуйте основні особливості розподілених АС.
81. Опишіть основні складові АС, як впливають на безпеку АС?
82. Опишіть основні загрози ІБ.
83. Дайте визначення терміну модель загроз, коротко опишіть основні ненавмисні штучні загрози.
84. Опишіть основні навмисні штучні небезпеки.
85. Розкрийте суть терміну неформальної моделі порушника, чим порушник відрізняється від зловмисника?
86. Які параметри визначаються розробки моделі порушника?
87. Наведіть зразкову класифікацію порушників у АС.
88. Опишіть три компоненти, пов'язані з порушенням безпеки. Дайте визначення термінам: «політика безпеки» та «доступ».
89. Опишіть перші три аксіоми комп'ютерної безпеки.
90. Дайте визначення терміну "користувач", опишіть четверту аксіому комп'ютерної безпеки.
91. Дайте визначення об'єкта джерела для новоствореного суб'єкта.
92. Опишіть механізм створення нового суб'єкта у моделях комп'ютерної безпеки.
93. Дайте визначення термінам «потік інформації» та «об'єкт, що асоціюється».

94. Дайте визначення термінам «доступ суб'єкта до об'єкта» та «правила розмежування доступу суб'єктів».
95. Опишіть поняття тотожності для суб'єктів та об'єктів комп'ютерної безпеки.
96. Що таке МО? Які види МО ви знаєте?
97. Опишіть комп'ютерну безпеку АДЕПТ-50.
98. Опишіть модель комп'ютерної безпеки п'ятивимірний простір безпеки Хартстона.
99. Опишіть модель комп'ютерної безпеки Белла-ЛаПадула.
100. Опишіть комп'ютерну безпеку low-water-mark (LWM).
101. Опишіть модель комп'ютерної безпеки MMS.
102. Опишіть модель комп'ютерної безпеки Лендвера.
103. Дайте визначення впливовим та незалежним суб'єктам.
104. Дайте визначення термінам МБС та МПС.
105. Дайте визначення термінам ІПС та ізольовану множину суб'єктів.
106. Опишіть процес створення суб'єкта з контролем незмінності об'єкта.
107. Сформулюйте базову теорему ІПС.
108. Зобразіть модель функціонування ядра безпеки.

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 та лабораторних робіт; - якості виконання самостійної роботи.

Поточний контроль здійснюється під час проведення практичних занять та лабораторних робіт 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 переводу до 100бальної системи множиться на коефіцієнт 10.

Загальна

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

Підсумковий контроль.

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, залікових книжках. Присутність здобувачів на проведенні підсумкового контролю (іспиту) обов'язкова. Якщо здобувач не з'явився на підсумковий контроль (іспит), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

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

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

Загальна кількість

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

Здобувач вищої освіти, який під час складання підсумкового контролю (іспиту) 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. Кафедра визначає 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
90 – 100	Відмінно (“зараховано”)	A	„Відмінно” – теоретичний зміст курсу освоєний цілком , необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
80 – 89	Добре (“зараховано”)	B	„Дуже добре” – теоретичний зміст курсу освоєний цілком , необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані , якість виконання більшості з них оцінено числом балів, близьким до максимального , робота з двома-трьома незначними помилками.
75 – 79		C	„Добре” – теоретичний зміст курсу освоєний цілком , практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання, виконані , якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками , робота з декількома незначними помилками або з однією–двома значними помилками.
68 – 74	Задовільно (“зараховано”)	D	„Задовільно” – теоретичний зміст курсу освоєний неповністю , але прогалини не носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано , деякі з виконаних завдань містять помилки , робота з трьома значними помилками.
60 – 67		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 оцінено числом балів, близьким до мінімального , робота, що задовольняє мінімуму критеріїв оцінки.

35–59	Незадовільно („не зараховано”)	FX	„Умовно незадовільно” – теоретичний зміст курсу освоєний частково , необхідні практичні навички роботи не сформовані , більшість передбачених програм 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
1–34		F	„Безумовно незадовільно” – теоретичний зміст курсу не освоєно , необхідні практичні навички роботи не сформовані , всі виконані навчальні завдання містять грубі помилки , додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання навчальних завдань, робота, що потребує повної переробки

10. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна література

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
2. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері. Підручник/ [Цуранов М.В., Струков В.М., Пєвнєв В.Я.] Харків: ХНУВС, 2015. 256 с.
3. Кібербезпека для спеціальних агентів кіберполіції (лекції). OSCE. 2016.
4. Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
5. Matt Walker. CEN Certified Ethical Hacker All-in-One Exam Guide. McGraw-Hill, 2012.
6. 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: 16.01.2023).

Допоміжна література

1. ITU-T Rec. X.800. Security architecture for Open Systems Interconnection for CCITT applications. / Recommendation X.800, Geneva, 1991. URL: <http://www.itu.int/rec/T-REC-X.800-199103-I> (дата звернення: 16.01.2023).
2. ITU-T E.408. Telecommunication networks security requirements. / ITU-T Recommendation E.408, 05/2004. URL: <https://www.itu.int/rec/T-REC-E.408-200405-I/en> (дата звернення: 16.01.2023).
3. NIST Special Publication 800-33. Underlying Technical Models for Information Technology Security. / Gary Stoneburner. CODEN: NSPUE2, December 2001. URL: <http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf> (дата звернення: 16.01.2023).

Інформаційні ресурси в Інтернеті

1. <http://www.hackerhighschool.org/>
2. <https://securityonline.info/>
3. <https://kali.tools/>
4. <https://tools.kali.org/>
5. <https://hackersonlineclub.com/>
6. <https://hakin9.org/>
7. <https://gbhackers.com/>
8. <https://securityonline.info/>
9. <https://www.hackingarticles.in/>