

Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми


(підпис)

О.О. Ілляшенко
(ініціали та прізвище)

« 31 » серпня 2024 р.

**РОБОЧА ПРОГРАМА ВИБІРКОВОЇ
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Комплексні системи захисту інформації: проектування, впровадження, супровід
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

Харків 2024 рік

Розробник: Брежнєв Є.В. професор кафедри 503, д.т.н., проф.
(прізвище та ініціали, посада, науковий ступінь та вчене звання)



(підпис)

Робочу програму розглянуто на засіданні кафедри _____
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 30 » 08 2024 р.

Завідувач кафедри д.т.н., професор _____ В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, рівень вищої освіти	Характеристика навчальної дисципліни денна форма навчання
Кількість кредитів – 4.5	Галузь знань 12 "Інформаційні технології" (шифр та найменування) Спеціальність 125 "Кібербезпека" (код та найменування) Освітня програма <u>Безпека інформаційних і комунікаційних систем</u> (найменування) Рівень вищої освіти: перший (бакалаврський)	Обов'язкова
Кількість модулів – 2		Навчальний рік 2022/2023
Кількість змістових модулів – 2		Семестр: 8-й
Індивідуальне завдання: не має		
Загальна кількість годин – 48/135		
Кількість тижневих годин для денної форми навчання: аудиторних – 4 самостійної роботи студента – 3		Лекції ¹⁾ 24 год.
		Практичні не має год.
		Лабораторні ¹⁾ 24 год.
		Самостійна робота 87 год.
		Індивідуальні завдання: не має
		Вид контролю: модульний контроль, іспит

Співвідношення кількості годин аудиторних занять до самостійної роботи становить:

Для денної форми навчання – 48/135.

¹⁾ Аудиторне навантаження може бути зменшене або збільшене на одну годину в залежності від розкладу занять.

2. Мета та завдання навчальної дисципліни

Мета діяльності: є формування у студентів теоретичних знань та практичних навичок у галузі проектування, впровадження та експлуатації комплексних систем захисту інформації; застосування системного підходу до забезпечення інформаційної безпеки, включаючи комплекс організаційних заходів.

Завдання (ОК 28): застосовувати знання до вирішення задач інформаційної безпеки; обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації; аналізувати вхідні дані та обирати методи оцінки якості.

Компетентності, які набуваються. Дисципліна має допомогти сформувати у студентів такі компетентності.

Загальні компетентності

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання. В результаті вивчення дисципліни студенти мають досягти такі програмні результати навчання:

ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

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 для ефективного рішення 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 часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

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 12 Розробляти моделі загроз та порушника.

ПРН 13 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН 17 Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН 19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 21 Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

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 отримання несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

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 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 і/або кібербезпеки.

Пререквізити

Дисципліна базується на: ОК15 «Курс на вибір 1 Захист інформації в інформаційно-комунікаційних системах», ОК23 «Прикладна криптологія», ОК24 «Надійність та функціональна безпека інформаційно-управляючих систем», ОК25 «Системи технічного захисту інформації». Дисципліна є базовою для: ВБ1.7 «Комплексні системи захисту інформації: проектування, впровадження, супровід», ВБ1.15 «Комплексні системи захисту інформації: проектування, впровадження, супровід (КП)», ОК36 «Дипломний робота (проект) бакалавра».

Кореквізити - відсутні

3. Програма навчальної дисципліни

Модуль 1

Змістовний модуль 1. Захист інформації інформаційно-телекомунікаційних мережах.

ТЕМА 1. Захист інформації в обчислювальних мережах

Загрози обчислювальним мережам. Методи захисту мереж. Механізми забезпечення безпеки.

ТЕМА 2. Засоби резервного копіювання інформації в мережах

Огляд сучасних тенденцій резервного зберігання даних. Огляд систем резервного копіювання.

ТЕМА 3. Місце IP-адреси в системі захисту конфіденційної інформації.

IP-протокол та його версії. Веб-браузер та його місце у правопорушеннях. Способи виявлення прихованої IP-адреси.

ТЕМА 4. Побудова захищених локальних мереж.

Принципи побудови захищених локальних мереж. Фізичне розділення мережі.. VPN мережі. Захищені оптичні локальні мережі.

ТЕМА 5. Системи відеоспостереження

Структура та основні елементи. Основні параметри камер відеоспостереження. Пристрої обробки відеосигналів.

ТЕМА 6. Побудова систем відеоспостереження.

Аналогові системи. Цифрові системи. Комбіновані системи. Пересилання пакетів. Шлюзи. Принципи побудови захищеної мережі відео нагляду.

Модульний контроль.

Модуль 2

Змістовний модуль 2. Методи та засоби протидії зловмисникам в комп'ютерних мережах.

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. Використання мереж стільникового зв'язку для скоєння правопорушень

Характеристика стільникового зв'язку. Стандарти стільникового зв'язку. Методи захисту мереж стільникового зв'язку.

ТЕМА 10. Характеристика хакерів.

Визначення та походження терміну хакер. Характеристика хакерських атак та їх види.

ТЕМА 11. Експлоїти та захист від них.

Характеристика експлоїтів. Способи використання експлоїтів. Способи захисту від експлоїтів.

ТЕМА 12. Методи і засоби сканування вузлів мережі.

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

Модульний контроль.

4. Структура навчальної дисципліни

Назва змістовного модуля і тем	Кількість годин				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1. Захист інформації в інформаційно-телекомунікаційних мережах.					
Тема 1. Захист інформації в обчислювальних мережах.	16	2		4	10
Тема 2. Засоби резервного копіювання інформації в мережах.	16	2		4	10
Тема 3. Місце IP-адреси в системі захисту конфіденційної інформації.	12	2			10
Тема 4. Побудова захищених локальних мереж.	16	2		4	10
Тема 5. Системи відео спостереження.	2	2			
Тема 6. Побудова систем відеоспостереження.	2	2			
Разом за змістовним модулем 1	64	12		12	40
Усього годин за модуль 1	64	12		12	40
Модуль 2					
Змістовний модуль 2. Методи та засоби протидії зловмисникам в комп'ютерних мережах.					
Тема 7. Методи фільтрації спаму.	6	2		4	
Тема 8. Брандмауери .	6	2		4	
Тема 9. Використання мереж стільникового зв'язку для скоєння правопорушень.	12	2			10
Тема 10. Характеристика хакерів.	12	2			10
Тема 11. Експлоїти та захист від них.	12	2		4	10
Тема 12. Методи і засоби сканування вузлів мережі.	19	2			17
Разом за змістовним модулем 2	71	12		12	47
Усього годин за модуль 2	71	12		12	87
Усього годин за дисципліною	135	24		24	87

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
...	<i>Не передбачено</i>	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Розробка методу порівняльної оцінки захищеності систем електронного документообігу	4
2	Основи використання VPN.	4
3	Програмна реалізація резервного копіювання даних	4
4	Вивчення програмних утиліт контролю доступу до інформаційних ресурсів	6
5	Отримання практичних навичок з аудиту безпеки КМ.	6
	Разом	24

7. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	2	3
	<i>Не передбачено</i>	

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Принципи побудови систем захисту інформації на базі стеку протоколів TCP/IP	17
2	Засоби хмарного копіювання даних	10
3	Використання захищених оптичних мереж	10
4	Класифікація мережевих атак та способи захисту від найбільш розповсюджених вразливостей	10
5	Хакерські атаки та методи захисту від них	20
6	Принципи використання соціальної інженерії	20
	Разом	87

9. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин

10. Методи навчання

Проведення аудиторних лекцій, лабораторних занять, консультацій, а також самостійна робота студентів за матеріалами, опублікованими кафедрою.

11. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

12. Розподіл балів, які отримують студенти

12. Критерії оцінювання та розподіл балів, які отримують студенти

12.1. Розподіл балів, які отримують студенти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0...1	7	0...7
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	3	0...18
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 10 балів), другий блок – п'ять тестових питань по 1 балу, третій блок – п'ять визначень по 2 бали.	0...25	1	0...25
Змістовий модуль 2			
Робота на лабораторних заняттях. Відмічається активність при виконанні завдань.	0...1	7	0...7
Виконання і захист лабораторних робіт. Своєчасність та виконання всіх завдань лабораторної роботи оцінюється у максимальну оцінку 6 балів.	0...6	3	0...18
Модульний контроль складається з трьох блоків: перший блок – розгорнута відповідь на одне питання (максимум 10 балів), другий блок – п'ять тестових питань по 1 балу, третій блок – п'ять визначень по 2 бали.	0...25	1	0...25
Усього за семестр			0...100

Білет для іспиту складається з одного теоретичного та одного практичного запитань, максимальна кількість за кожне із запитань, складає 50 балів.

Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Критерії оцінювання роботи студента протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання. Захистити всі індивідуальні завдання та здати тестування.

Добре (75 – 89). Твердо знати мінімум знань, виконати всі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах.

Відмінно (90 – 100). Повно знати основний та додатковий матеріал. Знати всі теми. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

13. Методичне забезпечення

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс].
URL:

<https://mentor.khai.edu/course/view.php?id=1609>

на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

- робоча програма дисципліни;
- конспект лекцій (презентації), в тому числі в електронному вигляді, який за змістом повністю відповідає робочій програмі дисципліни;
- журнал успішності.
- Посилання на практики

14. Рекомендована література

Базова

1. Комплексні системи захисту інформації: навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.
2. Хорошко В. О. та ін Проектування комплексних систем захисту інформації - Л.: Львівська політехніка, 2020. - 320с

3. 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, 2019. – 144 с.

Допоміжна

1. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. пос. [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41_yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html
2. Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security Systems / Thomas L. Norman
3. Physical Security Systems Handbook: The Design and Implementation of Electronic Security systems / Michael Khairallah

15. Інформаційні ресурси

1. Вадим Гребенніков Комплексні системи захисту інформації. Проектування, впровадження, супровід [Електрон. ресурс]. - Режим доступу: https://www.academia.edu/40525032/Комплексні_системи_захисту_інформації_проектування_впровадження_супровід
2. Microsoft IT Academy Program [Електрон. ресурс]. - Режим доступу: <https://itacademy.microsoftlearning.com/>
3. Cisco Networking Academy [Електрон. ресурс]. - Режим доступу: <https://www.netacad.com/>, <http://www.cisco.com/web/learning/netacad/>