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

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

ЗАТВЕРДЖУЮ

Голова НМК
_____ Д. М. Крицький
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека розподілених систем
(назва навчальної дисципліни)

Галузь знань: 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»
(шифр і найменування галузі знань)

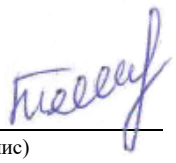
Спеціальність: _____
(код та найменування спеціальності)

Освітня програма: _____
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2023 рік

Розробник: Тецький А. Г., доцент, к.т.н. 
(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 2023 р.

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

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, спеціальність, освітня програма, рівень вищої освіти</td><td>Характеристика навчальної дисципліни
(денна форма навчання)</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="12">Галузь знань
10 «Природничі науки»,
11 «Математика та статистика»,
12 «Інформаційні технології»,
15 «Автоматизація та приладобудування»,
16 «Хімічна та біоінженерія»,
17 «Електроніка та телекомунікації»,
19 «Архітектура та будівництво»
(шифр та найменування)

Рівень вищої освіти:
другий (магістерський)</td><td>Вибіркова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістових модулів – 2</td><td>2023/2024</td></tr>
<tr><td>Індивідуальне завдання: немає</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин: 64/150</td><td>2-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи здобувача – 5</td><td>32 години</td></tr>
<tr><td>Практичні, семінарські[1)]</td></tr>
<tr><td>немає</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>86 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>модульний контроль, іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 64/86.

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

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є отримання навичок виявлення проблем кібербезпеки елементів розподілених інформаційних систем, ознайомлення з методами атак на такі компоненти та способами їх протидії.

Завдання: встановлення та налаштування платформи з вразливостями, оволодіння способами компрометації даних через незахищене з'єднання, отримання навичок застосування інструментальних засобів для експлуатації атак з модифікацією запиту до сервера баз даних, пошук можливостей проведення атак міжсайтового скриптингу, а також освоєння сценаріїв отримання вмісту бази даних з сервера, на який було завантажено виконувану оболонку для запуску довільних команд, отримання навичок сканування IP-мереж та аналіз проблем кібербезпеки елементів розподілених інформаційних систем на етапі проектування.

Після проходження курсу здобувачі мають **набути наступні компетенції:** здатність виявляти наукову сутність проблем у професійній сфері та знаходити адекватні шляхи щодо їх вирішення; навички використання інформаційних та комунікаційних технологій; здатність до самостійного освоєння нових методів дослідження та зміни своєї наукової й науково-виробничої профілю діяльності; здатність досліджувати проблеми з використанням системного аналізу, синтезу, комп'ютерного моделювання та методів оптимізації; здатність генерувати нові ідеї (креативність), виявляти, ставити та вирішувати проблеми, знаходити оптимальні шляхи щодо їх вирішення.

Очікувані результати навчання. Після успішного завершення дисципліни здобувачі мають вміти застосовувати підходи та засоби для виявлення та експлуатації проблем кібербезпеки розподілених інформаційних систем.

Пререквізити – дисципліна є вибірковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки галузі знань 12 «Інформаційні технології».

Кореквізити – Відсутні.

3. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1 «Проблеми кібербезпеки елементів сучасних розподілених інформаційних систем»

Тема 1. Підготовка тестового оточення. Встановлення майданчика з вразливостями

Встановлення на локальній машині платформи з вразливостями. Закріплення навичок роботи в Linux-подібних системах. Отримання навичок встановлення і налаштування веб-сервера для подальшого встановлення на нього вразливого елемента розподіленої інформаційної системи.

Тема 2. Аналіз трафіку комп'ютерних мереж, перехоплення трафіку

Отримання навичок роботи з аналізатором трафіку Wireshark і платформою Burpsuite, знайомство з атакою Man-in-the-Middle. Знайомство зі структурою мережевих пакетів. Отримання навичок роботи в сніффером на прикладі Wireshark і Burpsuite. Аналіз сценаріїв MitM-атак при роботі в Інтернет.

Тема 3. SQL-ін'єкції. Принципи, пошук і експлуатація атак з модифікацією запитів до сервера баз даних

Атаки з порушенням логіки запитів до бази даних. Робота з інструментальним засобом для пошуку і експлуатації ін'єкцій. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти sqlmap для експлуатації SQL-ін'єкцій. Порівняльний аналіз методів ін'єкцій при різної складності експлуатації вразливостей в Damn Vulnerable Web Application.

Тема 4. Робота з міжсайтовим скриптингом. Особливості атак та їх наслідки

Сценарії здійснення атак та інструменти атак. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти xsser для пошуку вразливостей. Можливості XSS-атак. Розроблення заходів щодо захисту веб-застосунка від XSS-атак.

Модульний контроль

ЗМІСТОВИЙ МОДУЛЬ 2 «Аналіз проблем кібербезпеки інформаційних інфраструктур та системного програмного забезпечення»

Тема 5. Завантаження виконуваної оболонки в Metasploit. Виконання довільних команд в атакованій системі

Отримання навичок роботи в фреймворку на прикладі модуля управління виконуваною оболонкою. Отримання навичок використання модулів фреймворка Metasploit. Отримання навичок управління атакованим сервером. Можливі наслідки експлуатації виконуваної оболонки. Розроблення заходів

щодо захисту сервера від завантаження шкідливого програмного забезпечення.

Тема 6. Сканування IP-мереж. Бази даних вразливостей

Знайомство з призначенням і функціоналом утиліти nmap в ОС Kali Linux, знайомство з основними відкритими базами даних вразливостей. Отримання навичок використання утиліти nmap. Отримання навичок пошуку інформації у відкритих базах вразливостей. Методи і засоби виявлення сканування. Розроблення заходів щодо захисту мережі від сканування.

Тема 7. Забезпечення кібербезпеки багатокомпонентної розподіленої системи

Аналіз можливих проблем безпеки інфраструктури на етапі проєктування. Список вимог, які повинні бути перевірені перед здачею проєкту замовнику. Методи і засоби захисту від поширених атак. Аналіз методів Web Application Firewall для виявлення потенційно небезпечного трафіку.

Модульний контроль

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовий модуль 1. Огляд сучасних проблем кібербезпеки веб-застосунків.					
Тема 1. Підготовка тестового оточення. Встановлення майданчика з вразливостями.	16	4		4	8
Тема 2. Аналіз трафіку комп'ютерних мереж, перехоплення трафіку.	16	4		4	8
Тема 3. SQL-ін'єкції. Принципи, пошук і експлуатація атак з модифікацією запитів до сервера баз даних.	20	4		4	12
Тема 4. Робота з міжсайтовим скриптингом. Особливості атак та їх наслідки.	20	4		4	12
Модульний контроль	1			1	
Разом за змістовим модулем 1	**73**	**16**		**17**	**40**
Змістовий модуль 2. Аналіз проблем кібербезпеки мереж та системного програмного забезпечення.					
Тема 5. Завантаження виконуваної оболонки в Metasploit. Виконання довільних команд в атакованій системі.	22	4		4	14
Тема 6. Сканування IP-мереж. Бази даних вразливостей.	24	6		4	14
Тема 7. Забезпечення кібербезпеки багатокомпонентної розподіленої системи.	30	6		6	18
Модульний контроль	1			1	
Разом за змістовим модулем 2	77	16		15	46
Усього годин	**150**	**32**		**32**	**86**

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено.*	
	Разом	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	*Не передбачено.*	
	Разом	

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Підготовка тестового оточення. Встановлення майданчика з вразливостями	4
2	Аналіз трафіку комп'ютерних мереж, перехоплення трафіку	4
3	SQL-ін'єкції. Принципи, пошук і експлуатація атак з модифікацією запитів до сервера баз даних	4
4	Робота з міжсайтовим скриптингом. Особливості атак та їх наслідки	4
5	Завантаження виконуваної оболонки в Metasploit. Виконання довільних команд в атакованій системі	4
6	Сканування IP-мереж. Бази даних вразливостей	4
7	Забезпечення кібербезпеки багатокомпонентної розподіленої системи	6
	Разом	**30**

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Знайомство з Penetration Testing Execution Standard.	8
2	Особливості роботи зі сніфферами.	8
3	Автоматизований пошук вразливостей за допомогою параметрів sqlmap.	12
4	Особливості експлуатації Stored та Reflected XSS вразливостей різними інструментальними засобами.	12
5	Можливості Metasploit під час пошуку проблем безпеки у	14

	застарілому програмному забезпеченні.	
6	Методи і засоби виявлення сканування.	14
7	Аналіз методів Web Application Firewall для виявлення потенційно небезпечного трафіку.	18
	Разом	**86**

9. Індивідуальні завдання

Індивідуальні завдання не передбачені.

10. Методи навчання

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

11. Методи контролю

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

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

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

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист лабораторних робіт	0...6	4	0…24
Модульний контроль	0…25	1	0…25
Змістовний модуль 2			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист лабораторних робіт	0...6	3	0…18
Модульний контроль	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 здобувач має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60 - 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи та домашні завдання. Знати основні загрози елементів розподілених інформаційних систем. Знати назви стандартів /

спільнот, що описують вимоги до кібербезпеки інформаційних систем та надають рекомендації з підвищення кібербезпеки досліджуваних систем. Знати назви основних інструментальних засобів, що використовуються під час тестування на проникнення.

Добре (75 - 89). Твердо знати мінімум знань, виконати усі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах. Вміти пояснювати природу походження вразливостей. Вміти складати план тестування елементів розподілених інформаційних систем відповідно до їх функціональності. Вміти обирати інструментальні засоби тестування на проникнення. Знаходити вразливості за допомогою інструментальних засобів тестування на проникнення.

Відмінно (90 - 100). Повно знати основний та додатковий матеріал. Знати усі теми. Орієнтуватися у підручниках та посібниках. Вміти аналізувати сирцевий код та прогнозувати можливі вразливості (статичний аналіз коду). Розуміти відмінності у межах окремих вразливостей (зокрема, SQL-ін’єкцій та XSS-атак). Вміти проводити всі етапи тестування на проникнення відповідно до Penetration Testing Execution Standard. Знати рекомендації зі створення безпечного програмного забезпечення відповідно до OWASP. 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

1. Тецький А. Г. Теоретичне введення до лабораторних робіт.
2. Тецький А. Г. Методичні вказівки щодо виконання лабораторних робот.

Електронний ресурс https://mentor.khai.edu/course/view.php?id=1979, на якому розміщено навчально-методичний комплекс дисципліни, який включає в себе:

- робоча програма дисципліни;
- конспект лекцій, в тому числі в електронному вигляді, які за змістом повністю відповідають робочій програмі дисципліни;

- методичні вказівки та рекомендації для виконання лабораторних робіт, а також рекомендації для самостійної підготовки;
- модульний контроль.

14. Рекомендована література

Базова

1. OWASP Foundation | Open Source Foundation for Application Security [Ел. ресурс]. URL: https://owasp.org/
2. Devansh Gandhi, Rutvij Jhaveri. Penetration Testing Frameworks for Web Applications and APIs: Vulnerability Assessment and Pen Testing Frameworks / LAP LAMBERT Academic Publishing, 2022. – 124 p.
3. Vickie Li. Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities / No Starch Press, 2021. – 416 p.
4. Jeremy Martin, Nitin Sharma, Frederico Ferreira, Shoriful Islam, Vishal Belbase, Ambadi MP, Yang Jue, Carlyle Collins, Daniel Traci. Bug Bounty Bootcamp: The Guide to Finding and Reporting Web Vulnerabilities / Information Warfare Center; 1st edition, 2021. – 177 p.

Допоміжна

1. Ryan Soper, Nestor N Torres, Ahmed Almoailu. Zed Attack Proxy Cookbook: Hacking tactics, techniques, and procedures for testing web applications and APIs / Packt Publishing; 1st edition, 2023. – 284 p.
2. Corey J. Ball. Hacking APIs: Breaking Web Application Programming Interfaces / No Starch Press, 2022. – 368 p.

15. Інформаційні ресурси

1. Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [Ел. ресурс]. URL: https://www.kali.org/
2. National Vulnerability Database [Ел. ресурс]. URL: https://nvd.nist.gov/