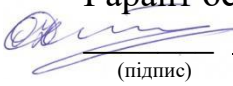
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми

О.О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Операційні системи
(назва навчальної дисципліни)

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

Спеціальність: 125 «Кібербезпека»
(код та найменування спеціальності)

Освітня програма: Безпекаінформаційних і комунікаційних систем
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: перший (бакалаврський)

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 – 4,5</td><td rowspan="14">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальність
125 «Кібербезпека»
(код та найменування)

Освітня програма
Безпекаінформаційних і комунікаційних систем
(найменування)

Рівень вищої освіти:
перший (бакалаврський)</td><td>Обов’язкова</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: 48/135</td><td>4-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="6">Кількість тижневих годин для денної форми навчання:
аудиторних – 3
самостійної роботи здобувача –5,5</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>16 годин</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>87 годин</td></tr>
<tr><td>Вид контролю</td></tr>
<tr><td>іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить: для денної форми навчання – 48/87.

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

2. Мета та завдання навчальної дисципліни

Мета вивчення: ознайомитись з основними загрозами і вразливостями операційних систем, а також прикладного програмного забезпечення. Оволодіти навичками роботи з інструментальними засобами для пошуку вразливостей прикладного програмного забезпечення.

Завдання:

знайомство з інструментами тестування безпеки KaliLinux; робота з базами даних вразливостей на прикладі застарілого програмного забезпечення; огляд загроз і вразливостей операційних систем різного типу; знайомство з методами атак на віддалені сервери; пошук вразливостейвебзастосунків; робота з фреймворком тестування безпеки Metasploit; знайомство з методами соціальної інженерії та захисту від них.

Компетентності, які набуваються:

– 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.

– КФ 4. Здатність забезпечувати неперервність бізнесу згідно 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 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики 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 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

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

– 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 25 Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

– ПРН 49 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

Пререквізити – ОК7«Архітектура комп'ютерів»,ОК12 «Операційні системи».

Кореквізити – ОК18 «Web-технології», ОК21 «Програмування систем IoT».

3. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1 «Огляд сучасних проблем безпеки програмного забезпечення»

Тема 1.Знайомство з VirtualBox. Встановлення операційної системи KaliLinux

Базовий та розширений функціонал засобу віртуалізації VirtualBox. Доповнення гостьової операційної системи. Зміна параметрів жорсткого диска. Закріплення навичок роботи в Linux-подібних системах.

Тема 2. Перелік загальних слабких місць програмного забезпечення. Загальні вразливості та загрози. Бази даних вразливостей

Бази CWEта CVE.Класифікація загальних слабких місць програмного забезпечення. Загальна система оцінки вразливостей.Життєвий цикл вразливості. Пошук інформації за відомим ідентифікатором вразливості.

Тема 3. Вразливості операційних систем. Огляд специфіки

Принципи створення захищених систем. Основні підсистеми комплексу засобів захисту операційної системи. Модель загроз операційної системи. Комплекс засобів захисту операційних систем.

Тема4. Мережеві атаки. Особливості атак та їх наслідки

Сценарії здійснення атак та інструменти атак. Атака «людина посередині». Сканування вузлів мережі. Бездротові мережі. Засоби забезпечення безпечної передачі даних у мережі.

Модульний контроль

ЗМІСТОВИЙ МОДУЛЬ 2 «Автоматизовані засоби пошуку проблем безпеки та вплив персоналу на захищеність кіберсистем»

Тема 5. Сканери вразливостейвебзастосунків. Поширені проблеми безпеки вебзастосунків

Розробки проекту Open Web Application Security Project. Особливості систем керування вмістом як об’єкта дослідження проблем кібербезпеки. Виявлення атак і ліквідація наслідків. Кращі світові практики оцінювання і забезпечення кібербезпекивебзастосунків. Стандарт PCIDSS.

Тема 6. Виконання команд в операційній системі під час атаки.ФреймворкMetasploit

Можливості фреймворкуMetasploitпід час тестування проблем безпеки. Способи завантаження виконуваної оболонки в операційну систему сервера. Робота з виконуваною оболонкою.

Тема 7. Методи соціальної інженерії

Актуальні і перспективні техніки соціальної інженерії. Захист від методів соціальної інженерії.Роль штучного інтелекту при виконанні зловмисних дій.

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 безпеки програмного забезпечення.					
Тема 1.Знайомство з VirtualBox. Встановлення операційної системи KaliLinux.	16	4		2	10
Тема 2. Перелік загальних слабких місць програмного забезпечення. Загальні вразливості та загрози. Бази даних вразливостей.	16	4		2	10
Тема 3. Вразливості операційних систем. Огляд специфіки.	18	4		2	12
Тема 4. Мережеві атаки. Особливості атак та їх наслідки.	18	4		2	12
Модульнийконтроль	1			1	
Разом за змістовим модулем 1	**69**	**16**		**9**	**44**
Змістовий модуль 2.Автоматизовані засоби пошуку проблем безпеки та вплив персоналу на захищеність кіберсистем.					
Тема 5. Сканери вразливостейвебзастосунків. Поширені проблеми безпеки вебзастосунків.	22	6		2	14
Тема 6. Виконання команд в операційній системі під час атаки. ФреймворкMetasploit.	22	6		2	14
Тема 7. Методи соціальної інженерії.	21	4		2	15
Модульний контроль	1			1	
Разом за змістовим модулем 2	66	16		7	43

Усього годин	**135**	**32**		**16**	**87**

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	Встановлення операційної системи KaliLinux.	2
2	Пошук застарілого програмного забезпечення.	2
3	Вразливості операційних систем.	2
4	Мережеві атаки.	2
5	Сканери вразливостейвебзастосунків.	2
6	Робота з Metasploit.	2
7	Пошук інформації з відкритих джерел.	2
	Разом	**14**

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Знайомство з VirtualBox. Встановлення операційної системи KaliLinux.	10
2	Перелік загальних слабких місць програмного забезпечення. Загальні вразливості та загрози. Бази даних вразливостей.	10
3	Вразливості операційних систем. Огляд специфіки.	12
4	Мережеві атаки. Особливості атак та їх наслідки.	12
5	Сканери вразливостейвебзастосунків. Поширені проблеми безпеки вебзастосунків	14
6	Виконання команд в операційній системі під час атаки. ФреймворкMetasploit	14
7	Методи соціальної інженерії	15

	Разом	**87**

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. Знати основні загрози безпеки операційних систем. Знати назви стандартів / спільнот, що описують вимоги до кібербезпекивебзастосунків 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 на проникнення. 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). 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. ТецькийА. Г. Теоретичне введення до лабораторних робіт.
2. ТецькийА. Г. Методичні вказівки щодо виконання лабораторних робот.

Електронний ресурс https://mentor.khai.edu/course/view.php?id=3726, 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 | OpenSourceFoundationforApplicationSecurity[Ел. ресурс]. URL: https://owasp.org/

2. RicMessier. PenetrationTestingBasics: A Quick-Start GuidetoBreakingintoSystems / Apress, 2016. – 115 p.
3. RonLepofsky. TheManager'sGuidetoWebApplicationSecurity: A ConciseGuidetotheWeakerSideoftheWeb / Apress, 2014. – 232 p.
4. PeterKim. TheHackerPlaybook 3: PracticalGuideToPenetrationTesting. – 2018. – 289 p.

Допоміжна

1. WilliamShotts. TheLinuxCommandLine, 2nd Edition: A CompleteIntroduction / NoStarchPress, 2019. – 504 p.
2. RaphaëlHertzog, JimO'Gorman, MatiAharoni. KaliLinuxRevealed - MasteringthePenetrationTestingDistribution / OffsecPress, 2017. – 344 p.
3. Засоби тестування на проникнення[Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=3726.
4. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.
5. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П.Основи кіберпростору, кібербезпеки та кіберзахисту/ Ліра-К, 2021. – 554 с.
6. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник / Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236 с.
7. АйзексонВолтер. Інноватори. Як група хакерів, геніїв та ґіків здійснила цифрову революцію / ВолтерАйзексон; пер. з англ. Дмитра Гломозди. К.: Наш формат, 2017. –488 с.

15. Інформаційні ресурси

1. KaliLinux | PenetrationTestingandEthicalHackingLinuxDistribution[Ел. ресурс]. URL: https://www.kali.org/
2. NationalVulnerabilityDatabase[Ел. ресурс]. URL: https://nvd.nist.gov/
3. Common Weakness Enumeration[Ел. ресурс]. URL: https://cwe.mitre.org/