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

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

ЗАТВЕРДЖУЮ

Керівник (гарант) освітньої програми
_____ О. О. Ілляшенко
(підпис) (ініціали та прізвище)

« 31 » серпня 2024 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційно-комунікаційні системи
(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: 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 2024 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</td><td rowspan="11">Галузь знань
12 «Інформаційні технології»
(шифр та найменування)

Спеціальність
125 «Кібербезпека»
(код та найменування)

Освітня програма
Безпека інформаційних 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>2024/2025</td></tr>
<tr><td rowspan="2">Індивідуальне завдання: РГР</td><td>Семестр</td></tr>
<tr><td>5-й</td></tr>
<tr><td rowspan="2">Загальна кількість годин: 64/120</td><td>Лекції*</td></tr>
<tr><td>32 години</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи здобувача – 3,5</td><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>56 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 – 64/56.

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

2. Мета та завдання навчальної дисципліни

Мета вивчення: набуття знань про структуру та принципи функціонування інформаційно-комунікаційних систем, а також формування практичних навичок застосування інструментальних засобів для аналізу, тестування й забезпечення їх кібербезпеки.

Завдання:

знайомство з архітектурою ІКС та типами мережевої взаємодії, аналіз типових вразливостей протоколів та сервісів, отримання практичних навичок роботи з інструментами Kali Linux для тестування безпеки, впровадження базових засоби захисту від атак у тестовому середовищі.

Компетентності, які набуваються:

– (КЗ1) Здатність застосовувати знання у практичних ситуаціях;

– (КЗ2) Знання та розуміння предметної області та розуміння професії;

– (КЗ3) Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово;

– (КЗ4) Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

– (КЗ5) Здатність до пошуку, оброблення та аналізу інформації;

– (КФ2) Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

– (КФ3) Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;

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

– (ПРН1) Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

– (ПРН2) Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

– (ПРН3) Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

– (ПРН4) 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.

– (ПРН8) Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

– (ПРН10) Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

– (ПРН11) Виконувати аналіз зв’язків між інформаційними процесами на

віддалених обчислювальних системах.

– (ПРН13) Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

– (ПРН14) Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;

– (ПРН15) Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

– (ПРН17) 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.

– (ПРН22) Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

– (ПРН23) Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

– (ПРН24) Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

– (ПРН26) Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

– (ПРН27) Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

– (ПРН31) Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

– (ПРН38) Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

– (ПРН40) Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

– (ПРН47) Вирішувати задачі захисту інформації, що обробляється в

інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.

Пререквізити:

- ОК7 «Архітектура комп'ютерів»
- ОК8 «Системи технічного захисту інформації»

Кореквізити:

- ОК24 «Управління інформаційною безпекою»
- ОК25 «Захист інформації в інформаційно- комунікаційних системах (КП)»
- ОК26 «Надійність та функціональна безпека інформаційно-управляючих систем»
- ОК27 «Захист інформації в інформаційно -комунікаційних системах»
- ОК28 «Комплексні системи захисту інформації: проектування, впровадження, супровід»

3. Програма навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1 «Архітектура і протоколи ІКС»

Тема 1. Підготовка безпечного тестового середовища. Віртуалізація, топологія ІКС, ролі вузлів.

Поняття тестового середовища для аналізу безпеки. Основи віртуалізації, налаштування взаємодії між вузлами (Kali Linux, Metasploitable). Структура інформаційно-комунікаційних систем.

Тема 2. Перехоплення, візуалізація та аналіз мережевого трафіку як основа виявлення аномалій в ІКС.

Основи функціонування протоколів канального та транспортного рівнів. Перехоплення та декодування трафіку. Інструменти аналізу (Wireshark, Burpsuite). Виявлення ознак вторгнення, небезпечних протоколів та аномальної поведінки в мережевому трафіку.

Тема 3. Методи автентифікації та пошук слабких місць через перебір паролів. Захист від brute-force атак.

Типові помилки конфігурації служб автентифікації. Перебір облікових даних. Огляд вразливостей при використанні облікових записів за замовчуванням. Аналіз загроз, пов’язаних з недостатнім контролем доступу в ІКС.

Тема 4. Вразливості протоколу FTP та принципи безпечної передачі файлів у ІКС.

Огляд архітектури протоколу FTP та його недоліків у контексті кібербезпеки. Демонстрація анонімного доступу, витоку облікових даних через незашифровані з'єднання, типові експлойти. Основи переходу до безпечних альтернатив.

Модульний контроль

ЗМІСТОВИЙ МОДУЛЬ 2 «Системи захисту в ІКС»

Тема 5. Збирання та аналіз журналів подій для виявлення кіберінцидентів. Основи розслідування подій безпеки.

Важливість логування в ІКС. Типи журналів. Методи виявлення слідів атак: підозріла активність, помилки входу, сканування. Основи створення звітів про інциденти.

Тема 6. Протидія атакам перебору. Налаштування системи блокування підозрілих входів у ІКС.

Інструменти запобігання brute-force атакам. Принцип динамічного блокування IP-адрес. Практика побудови правил фільтрації. Вплив захисту від перебору на доступність систем та безпеку інформаційного середовища.

Тема 7. Захист ІКС від аномальної активності. Фільтрація та виявлення підозрілих запитів.

Методи виявлення шкідливої активності в реальному часі. Аналіз запитів до вебсервісів. Побудова правил блокування для iptables. Практика виявлення та нейтралізації простих атак типу DoS, сканування або HTTP-флуду.

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. Архітектура і протоколи ІКС.					
Тема 1. Підготовка безпечного тестового середовища. Віртуалізація, топологія ІКС, ролі вузлів.	14	4		4	6
Тема 2. Перехоплення, візуалізація та аналіз мережевого трафіку як основа виявлення аномалій в ІКС.	18	6		4	8
Тема 3. Методи автентифікації та пошук слабких місць через перебір паролів. Захист від brute-force атак.	20	6		6	8
Тема 4. Вразливості протоколу FTP та принципи безпечної передачі файлів у ІКС.	14	4		4	6
Модульний контроль	1			1	
Разом за змістовим модулем 1	**67**	**20**		**19**	**28**
Змістовий модуль 2. Системи захисту в ІКС.					
Тема 5. Збирання та аналіз журналів подій для виявлення кіберінцидентів. Основи розслідування подій безпеки.	14	4		4	6
Тема 6. Протидія атакам перебору. Налаштування системи блокування підозрілих входів у ІКС.	16	4		4	8
Тема 7. Захист ІКС від аномальної активності. Фільтрація та виявлення підозрілих запитів.	16	4		4	8
РГР	6				6
Модульний контроль	1			1	
Разом за змістовим модулем 2	53	12		13	28
Усього годин	**120**	**32**		**32**	**56**

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	Налаштування тестового оточення.	4
2	Перехоплення та аналіз мережевого трафіку .	4
3	Пошук даних за замовчуванням за допомогою перебору.	6
4	Протокол передачі файлів (FTP) і пов'язані вразливості.	4
5	Аналіз логів для виявлення інцидентів.	4
6	Впровадження системи захисту від перебору.	4
7	Впровадження системи захисту від підозрілих запитів.	4
	Разом	**30**

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Підготовка безпечного тестового середовища. Віртуалізація, топологія ІКС, ролі вузлів.	6
2	Перехоплення, візуалізація та аналіз мережевого трафіку як основа виявлення аномалій в ІКС.	8
3	Методи автентифікації та пошук слабких місць через перебір паролів. Захист від brute-force атак.	8
4	Вразливості протоколу FTP та принципи безпечної передачі файлів у ІКС.	6
5	Збирання та аналіз журналів подій для виявлення кіберінцидентів. Основи розслідування подій безпеки.	6
6	Протидія атакам перебору. Налаштування системи блокування підозрілих входів у ІКС.	8
7	Захист ІКС від аномальної активності. Фільтрація та виявлення підозрілих запитів.	8
8	РГР	6
	Разом	**56**

9. Індивідуальні завдання

РГР на тему «Розроблення плану тестування на проникнення компонентів інформаційно-комунікаційної системи».

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…20	1	0…20
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…20	1	0…20
РГР	0…10	1	0…10
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 кібербезпеки різних 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 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. 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=7365, 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. Терейковський І. А., Гнатюк С. О. Захист інформації в комп'ютерних системах : навч. посіб. / І. А. Терейковський, С. О. Гнатюк. – Київ : Університет «Україна», 2019. – 220 с.
3. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity / edited by Markus Christen, Bert Gordijn, Michele Loi. – Cham : Springer, 2020.
4. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. – 115 p.

Допоміжна

1. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction / No Starch Press, 2019. – 504 p.
2. Інформаційно-комунікаційні системи [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=7365.
3. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.
4. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту / Ліра-К, 2021. – 554 с.
5. 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.

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/
3. Common Weakness Enumeration [Ел. ресурс]. URL: https://cwe.mitre.org/