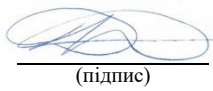
Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

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

ЗАТВЕРДЖУЮ

Голова НМК



(підпис) Д.М. Крицький (ініціали та прізвище)

« 31 » серпня 2023 р.

РОБОЧА ПРОГРАМА ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Безпека індустріальних систем та Інтернету речей
(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)

Освітні програми:
(найменування освітньої програми)

Форма навчання: денна

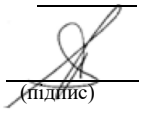
Рівень вищої освіти: другий (магістерський)

Харків 2023 рік

Розробник: Бабешко Євген Васильович, доцент, к.т.н., доцент 
(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 » серпня 2023 року

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 rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, спеціалізація, рівень вищої освіти</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td></tr>
<tr><td>Кількість кредитів – 5</td><td rowspan="6">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»</td><td>Вибіркова</td></tr>
<tr><td>Модулів – 2</td><td rowspan="2">Навчальний рік
2023/2024</td></tr>
<tr><td>Змістовних модулів – 2</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: немає</td><td rowspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин – денна – 861)/150</td><td>1-й</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи здобувача – 5.4</td><td rowspan="10">Рівень вищої освіти:
другий (магістерський)</td><td>Лекції1)</td></tr>
<tr><td>32 години</td></tr>
<tr><td>Практичні1)</td></tr>
<tr><td>0 годин</td></tr>
<tr><td>Лабораторні1)</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>Іспит</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної роботи становить *64/86*.

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

2. Мета та завдання навчальної дисципліни

Мета: надання знань і навичок зі створення, використання та аналізу індустріальних систем та Інтернету речей з урахуванням вимог до безпеки.

Завдання:

- придбання знань з базового аналізу функційної безпеки та кібербезпеки індустріальних систем та індустріальних IoT систем;
- отримання знань з використання баз уразливостей, розрахунку рівня критичності уразливості;
- отримання знань з використання баз атак (сценаріїв атак) на індустріальні системи та індустріальні IoT системи;
- отримання практичних знань з використання інструментальних засобів для аналізу трафіку, експлуатації уразливостей;
- придбання знань з встановлення, налаштування та використання систем виявленнь вторгнень та систем запобігання вторгненням.

Компетентності, які набуваються: Здатність виявляти, ставити та вирішувати проблеми інженерного та дослідницького характеру в галузі безпеки індустріальних систем та індустріального Інтернету речей

Очікувані результати навчання. В результаті вивчення дисципліни здобувачі мають вміти застосовувати підходи, сервіси та інструментальні засоби для розв'язання складних задач аналізу та забезпечення безпеки індустріальних систем та індустріального Інтернету речей.

Пререквізити: дисципліна є вибірковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки галузей 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».

Кореквізіти: Відсутні.

3. Зміст навчальної дисципліни

Модуль 1
Змістовний модуль 1

Тема 1. Вступ
Інформація про мету та обсяг дисципліни. Принципи оцінювання. Рекомендована література та веб-ресурси.

Тема 2. Функційна безпека та кібербезпека
Термінологія. Шари забезпечення безпеки. Нормативні документи з безпеки для індустрії. Ключові концепції документу IEC 61508. Ключові концепції документу IEC 62443. Оцінювання безпеки: методи та інструментальні засоби.

Тема 3. Засоби аналізу кібербезпеки індустріальних систем
Shodan. Приклади пошукових запитів. MITRE ATT&CK для індустріальних систем. Тактики, техніки, процедури. CIARA. Імітація атак. Генерація звітів. CSET. Опитувальники на базі нормативних документів.

Тема 4. Ідентифікація та аналіз уразливостей компонентів індустріальних систем
Бази даних уразливостей. CVE, NVD, Exploit DB. Common Vulnerability Scoring System. Ідентифікація типових компонентів індустріальних систем. Аналіз безпеки ідентифікованих компонентів.

Модуль 2
Змістовний модуль 2

Тема 5. Безпека комунікацій індустріальних систем
Аналіз трафіку індустріальних систем та індустріальних IoT систем. Аналіз пакетів. Аналіз індустріального протоколу обміну. Фільтрація трафіку.

Тема 6. Використання Wireshark для аналізу безпеки індустріальної системи
Використання Wireshark для аналізу трафіку віртуальної індустріальної системи. Практичний приклад.

Тема 7. Аналіз безпеки індустріальної системи: Metasploit
Використання Metasploit для експлуатації уразливостей, наявних у віртуальній індустріальній системі. Практичний приклад.

Тема 8. Системи виявлення та запобігання вторгнень
Системи виявлення вторгнень / атак (Intrusion Detection System, IDS). Системи запобігання вторгнень / атак (Intrusion Prevention System, IPS). Мережеві та вузлові IDS/IPS. Signature Based IDS/IPS та Anomaly Based IDS/IPS. Хибно позитивні та хибно негативні дії. Налаштування та використання Snort.

4. Структура навчальної дисципліни

Назви змістовних модулів і тем	Кількість годин				
	Денна форма				
	Усього	У тому числі			
		л	п	лаб.	с. р.
1	2	3	4	5	6
Модуль 1					
Змістовний модуль 1					
1. Вступ	1	1			
2. Функційна безпека та кібербезпека	12	4			8
3. Засоби аналізу кібербезпеки індустріальних систем	16	4		4	8
4. Ідентифікація та аналіз уразливостей компонентів індустріальних систем	18	4		4	10
Модульний контроль	1	1			
Разом за змістовним модулем 1	48	14		8	26
Модуль 2					
Змістовний модуль 2					
5. Безпека комунікацій індустріальних систем	25	4		6	15
6. Використання Wireshark для аналізу безпеки індустріальної системи	25	4		6	15
7. Аналіз безпеки індустріальної системи з використанням Metasploit	25	4		6	15
8. Системи виявлення та запобігання вторгнень	26	5		6	15

Модульний контроль	1	1			
Разом за змістовним модулем 2	102	18		24	60
Усього годин за дисципліною	**150**	**32**		**32**	**86**

5. Теми семінарських занять

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

6. Теми практичних занять

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

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Знайомство з платформою індустріального Інтернету речей	2
2	Використання Shodan для пошуку індустріальних пристроїв за заданими критеріями	4
3	Ідентифікація типових складових платформи індустріального Інтернету речей	4
4	Розрахунок критичності виявлених уразливостей (метрики CVSS)	4
5	Використання Wireshark для захоплення та аналізу трафіку індустріальної системи	6
6	Використання Metasploit для експлуатації наявних уразливостей	6
7	Використання Snort у режимах IDS та IPS	6
	Разом	**32**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Відпрацювання матеріалів лекційних занять за темою 2	8
2	Відпрацювання матеріалів лекційних занять за темою 3	8
3	Відпрацювання матеріалів лекційних занять за темою 4	10
4	Відпрацювання матеріалів лекційних занять за темою 5	15
5	Відпрацювання матеріалів лекційних занять за темою 6	15
6	Відпрацювання матеріалів лекційних занять за темою 7	15
7	Відпрацювання матеріалів лекційних занять за темою 8	15
	Разом	**86**

9. Індивідуальні завдання

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

10. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.14, 15).

11. Методи контролю

Проведення поточного контролю, електронного тестування, підсумковий контроль у вигляді іспиту.

12. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Лабораторні заняття	0...10	3	0…30
Тести	0...5	1	0...5
Модульний контроль	0..10	1	0..10
Змістовний модуль 2			
Лабораторні заняття	0…10	4	0…40
Тести	0…5	1	0…5
Модульний контроль	0..10	1	0..10
Усього за семестр			**0…100**

Білет для іспиту складається з двох теоретичних питань (25 балів за кожне питання), практичного завдання (25 балів) та тесту (25 балів).

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

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань лабораторних занять. Знати основи оцінювання функційної безпеки та кібербезпеки. Уміти розраховувати критичність уразливостей.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань лабораторних занять. Знати ключові принципи індустріального Інтернету речей та типові архітектури. Уміти виявляти типові компоненти індустріальних систем та проводити аналіз їх безпеки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Уміти налаштовувати захоплення та аналіз трафіку. Вміти налаштовувати та використовувати системи виявлення та запобігання атак / вторгнень.

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

Навчально-методичний комплекс дисципліни розміщений у системі дистанційного навчання «Ментор».

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=7901

14. Рекомендована література

Базова

1. Cybersecurity of Industrial Systems. Wiley, 2019. [Ел. ресурс]. URL: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119644538

Допоміжна

1. Ілляшенко О., Бабешко Є., Харченко В. Кібербезпека індустріальних систем. [Ел. ресурс]. URL: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-cybersecurity+++.pdf
2. Бабешко Є., Ілляшенко О., Харченко В. Функційна безпека індустріальних систем. [Ел. ресурс]. URL: https://tk185.appau.org.ua/whitepapers/aCampus-whitepaper-IEC-61508+++.pdf

15. Інформаційні ресурси

1. MITRE ATT&CK [Ел. ресурс]. URL: https://attack.mitre.org/
2. Search Engine for Internet of Everything [Ел. ресурс]. URL: https://shodan.io
3. CSET (Cyber Security Evaluation Tool) [Ел. ресурс]. URL: https://github.com/cisagov/cset/releases
4. Common Vulnerabilities and Exposures [Ел. ресурс]. URL: https://cve.org
5. National Vulnerability Database [Ел. ресурс]. URL: https://nvd.nist.gov
6. Exploit Database [Ел. ресурс]. URL: https://exploit-db.com
7. Metasploit Framework [Ел. ресурс]. URL: https://github.com/rapid7/metasploit-framework
8. Snort [Ел. ресурс]. URL: https://snort.org/