МІНІСТЕРСТВООСВІТИІНАУКИУКРАЇНИ
НАЦІОНАЛЬНИЙАЕРОКОСМІЧНИЙУНІВЕРСИТЕТ
ІМ. М. Є. ЖУКОВСЬКОГО
«ХАРКІВСЬКИЙАВІАЦІЙНИЙІНСТИТУТ»

Кафедра ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХТЕХНОЛОГІЙ
ІМ. О. О. ЗЕЛЕНСЬКОГО № 504

"ЗАТВЕРДЖУЮ"

Гарант освітньої програми

(підпис) Олександр ТОЦЬКИЙ (ім'я та прізвище)

31 серпня 2023 р.

РОБОЧА ПРОГРАМА *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кібербезпека інфокомунікаційних систем
(назва навчальної дисципліни)

Галузь знань: 17 Електроніка, автоматизація та електронні комунікації
(шифр і найменування галузі знань)

Спеціальність: 172 Електронні комунікації та радіотехніка
(код і найменування спеціальності)

Освітня програма: Інформаційні мережі зв'язку
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: другий (магістерський)

Харків 2023 рік

Розробник: РУБЕЛЬ Андрій, старший викладач, доктор філософії
(прізвище та ім'я, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму розглянуто на засіданні кафедри інформаційно-комунікаційних технологій ім. О.О. Зеленського №504
(назва кафедри)

Протокол № 1 від «31» серпня 2023 р.

Завідувач кафедри д.т.н., професор Володимир ЛУКІН
(науковий ступінь і вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

<table>
<tr><td>Найменування показника</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="14">Галузь знань
17 Електроніка, автоматизація та електронні комунікації
(шифр і найменування)

Спеціальність
172 Електронні комунікації та радіотехніка
(код і найменування)

Освітня програма
Інформаційні мережі зв’язку
(найменування)

Рівень вищої освіти:
другий (магістерський)</td><td>Обов’язкова</td></tr>
<tr><td>Кількість модулів – 1</td><td>Навчальний рік</td></tr>
<tr><td>Кількість змістовних модулів – 2</td><td>2023/2024</td></tr>
<tr><td>Індивідуальне завдання – не передбачене навчальним планом</td><td>Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 48*/ 150</td><td>2-й</td></tr>
<tr><td>Лекції*</td></tr>
<tr><td rowspan="7">Кількість тижневих годин для денної форми навчання: аудиторних – 3 самостійної роботи здобувача – 6,38</td><td>24 години</td></tr>
<tr><td>Практичні*</td></tr>
<tr><td>24 години</td></tr>
<tr><td>Лабораторні*</td></tr>
<tr><td>-</td></tr>
<tr><td>Самостійна робота</td></tr>
<tr><td>102 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: **48/ 102**.

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

2. Мета та завдання навчальної дисципліни

Мета вивчення: набуття студентами знань, вмінь і навичок, використання їх у своїй практичній роботі, пов'язаній з виявленням порушень кібербезпеки і реагуванням на події безпеки, керуванням системами безпеки, роботою аналітика безпеки молодшого рівня, який працює в центрі моніторингу та управління безпекою (SOC).

Завдання: вивчення основних методів оцінки, виявлення та реагування на загрози безпеки мереж і кінцевих пристроїв, а також опанування сучасних інструментів моніторингу і реагування на події безпеки.

Компетентності, які набуваються:
загальні:
- навички використання інформаційних і комунікаційних технологій;
- здатність досліджувати проблеми з використанням системного аналізу, синтезу, комп'ютерного моделювання та методів оптимізації;
- здатність аналізувати, верифікувати, оцінювати повноту інформації в ході професійної діяльності, за необхідності доповнювати й синтезувати відсутню інформацію й працювати в умовах невизначеності;
- знання іншої мови(мов);

фахові:
- здатність застосовувати відповідні математичні, наукові і технічні методи, а також комп'ютерне програмне забезпечення для вирішення завдань в сфері розподілу і обробки інформації;
- здатність визначати ефективність рішень в сфері розподілу і обробки інформації з використання аналітичних методів і методів моделювання;
- здатність продемонструвати знання і розуміння математичних принципів і методів, необхідних для підтримки спеціалізацій з телекомунікацій.

Очікувані (програмні) результати навчання:
- спроможність аналізувати складні інженерні задачі, процеси і системи відповідно до спеціалізації; обирати і застосовувати придатні типові аналітичні, розрахункові та експериментальні методи; уміння інтерпретувати результати таких досліджень;
- знання основних принципів реалізації інформаційних та телекомунікаційних мереж на різних етапах життєвого циклу.
- знання основних принципів організації і побудови інформаційно-комунікаційних систем, вміння враховувати особливості галузей їх застосування, визначати характеристики систем і окремих їх модулів;
- знання принципів керування інформаційними мережами, керування та методів оцінювання якості їх функціонування та надання послуг;
- знання принципів побудови сервісних платформ інформаційних мереж;
- знати та уміти застосовувати засоби сучасних інформаційних технологій для вирішення задач в сфері інформаційно-комунікаційних технологій;
- здатність ефективно застосовувати роботу з комп'ютером, його технічним та програмним забезпеченнями (носіями інформації, базами даних тощо).

Пререквізити – "Інтернет речей", "Хмарні інформаційні системи", "Розподілені сервісні системи".
Кореквізити – "Інтернет речей".

3. Зміст навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Основи моніторингу та управління безпекою

Тема 1. Кібербезпека і центр моніторингу та управління безпекою. Предмет вивчення і задачі дисципліни. Місце дисципліни в учбовому плані. Центри моніторингу та управління безпекою (SOC). основних ролі в центрі моніторингу та управління безпекою. Задачі аналітиків різних рівнів. Мережева безпека. Функцію центру моніторингу та управління безпекою.

Тема 2.Аспекти безпеки в операційних системах Windows та Linux. Основні поняття і компоненти ОС Windows. Принципи роботи ОС та інструменти, які використовуються для захисту кінцевих пристроїв з ОС Windows. Використання ОС Linuxв центрі моніторингу та управління безпекою. Базові операції Linux, а також завдання адміністрування і завдання, пов'язані з безпекою. Інструменти Linux для дослідження та моніторингу безпеки.

Тема 3. Мережеві протоколи і служби. Принципи роботи мережі і мережевих сервісів. Протоколи мережевої взаємодії. Нормальна поведінка мереж на прикладі протоколів з стека протоколів TCP / IP і пов'язаних служб, які дозволяють виконувати завдання в комп'ютерних мережах.

Тема 4. Мережева інфраструктура. Основи функціонування мережевої інфраструктури, в тому числі провідні та безпровідні мережі, мережева безпека і конструкції мереж. Принципи роботи мережевої інфраструктури. Типи міжмережевих екранів. Сервіси мережевої безпеки.

Тема 5. Принципи забезпечення безпеки мережі. Засоби і методи, які використовуються хакерами для проведення мережевих атак. Атаки на мережі: типи загроз і атак, які використовуються зловмисниками. Інструменти зловмисників. Типи шкідливого ПЗ. Інструменти для організації атак на мережі.

Тема 6. Мережеві атаки. Поглиблений аналіз. Інструменти аналітиків з кібербезпеки для виявлення атак. Віддзеркалення портів, аналізатори протоколів і системи SIEM. Вразливості існуючих протоколів. Моніторинг трафіку і способи його проведення. Вразливості мережевих протоколів і служб, включаючи IP, TCP, UDP, ARP, DNS, DHCP, HTTP і електронну пошту.

Модульний контроль

Змістовний модуль 2.Аналіз і реагування на інциденти безпеки

Тема 1. Захист мережі. Завдання захисту мережі. Методи захисту мереж, пристроїв і даних. Способи захисту мережевої безпеки, методи контролю доступу. Методи управління доступом. Система безпеки AAA. Служби аналітики загроз (Cisco Talos, FireEye).

Тема 2. Криптографія і інфраструктура загальних ключів. Криптографічні технології для забезпечення конфіденційності та безпеки даних. Криптографічні методах і вплив їх використання на моніторинг безпеки мережі. Забезпечення безпеки взаємодій в мережах. Використання хеш-функцій. Аутентифікацію поряд з перевіркою цілісності повідомлень за допомогою хеш-функцій (HMAC). Симетричне шифрування. Асиметричне шифрування. Протоколи безпеки. Робота інфраструктури відкритих ключів (PKI). Цифровий підпис. Цифрові сертифікати.

Тема 3. Захист і аналіз кінцевих пристроїв. Кінцеві пристрої. Вразливості кінцевих пристроїв і атаки на них. Визначення вразливостей кінцевих пристроїв. Система виявлення вторгнень на стороні хоста (HIDS). Функції брандмауера. Інструменти для виконання оцінки вразливостей кінцевих пристроїв. Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS). Інструменти для управління ризиками.

Тема 4. Моніторинг безпеки. Системи моніторингу безпеки мережі. Типи даних для виявлення, перевірки та стримування експлойтів. Технології забезпечення безпеки. Протокол моніторингу Syslog. Файли журналів. Списки контролю доступу. Шифрування трафіку. VPN.

Тема 5. Аналіз даних вторгнень. Системи аналізу даних вторгнень. Попередження про безпеку в мережі. Ескалація попереджень. Пакет аналізу даних попереджень SecurityOnion.

Аналіз даних про вторгнення. Засоби виявлення і аналізу вторгнень – Snort, Bro, OSSEC, ELSA, Sguil.Докази і цифрова технічна експертиза.

Тема 6. Реагування на інциденти і їх обробка. Моделі і процедури реагування та робота в разі виникнення інцидентів. Ланцюжок кібервбивства (Cyber-Kill Chain), ромбовидна модель, схема VERIS і рекомендації NIST за структурою груп реагування на вразливості, пов'язані з комп'ютерною безпекою (CSIRT). Процеси, що виконуються при виникненні інцидентів.

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. Основи моніторингу та управління безпекою					
Тема 1. Кібербезпека і центр моніторингу та управління безпекою	12	2	2	-	8
Тема 2.Аспекти безпеки в операційних системах Windows таLinux	12	2	2	-	8
Тема 3.Мережеві протоколи і служби	12	2	2	-	8
Тема 4. Мережева інфраструктура	12	2	2	-	8
Тема 5. Принципи забезпечення безпеки мережі	12	2	2	-	8
Тема 6. Мережеві атаки. Поглиблений аналіз	11	1	2	-	8
Модульний контроль	4	1	-	-	3
Разом за змістовним модулем 1	**75**	**12**	**12**	**-**	**51**
Змістовний модуль 2. Аналіз і реагування на інциденти безпеки					
Тема 1. Захист мережі	12	2	2	-	8
Тема 2. Криптографія і інфраструктура загальних ключів	12	2	2	-	8
Тема 3.Захист і аналіз кінцевих пристроїв	12	2	2	-	8
Тема 4.Моніторинг безпеки	12	2	2	-	8
Тема 5.Аналіз даних вторгнень	12	2	2	-	8
Тема 6.Реагування на інциденти і їх обробка	11	1	2	-	8
Модульний контроль	4	1	-	-	3
Разом за змістовним модулем 2	**75**	**12**	**12**	**-**	**51**
Усього годин	**150**	**24**	**24**	**-**	**102**
Модуль 2					
Індивідуальне завдання	-	-	-	-	-
Усього годин	**150**	**24**	**24**	**-**	**102**

5. Теми семінарських занять

№ п/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	
2		
	Разом	

6. Теми практичних занять

№ п/п	Назва теми	Кількість годин
1	Моніторинг системних ресурсів в ОС Windows та GNU/Linux і налаштування повноважень	2
2	Аналіз кадрів Ethernet за допомогою Wireshark	2
3	Робота з Nmap	2
4	Аналіз перехоплених пакетів за допомогою Wireshark	2
5	Аналіз трафіку HTTP і HTTPS за допомогою Wireshark	2
6	Атака на базу даних MySQL	2
7	Вивчення файлів журналів сервера	2
8	Вивчення сеансів зв'язку за протоколами Telnet і SSH за допомогою Wireshark	2
9	Правила Snort і брандмауера	2
10	Інтерпретація даних HTTP і DNS для ізоляції хакера	2
11	Ізоляція зламаного хоста	2
12	Опрацювання інцидентів безпеки	2
	Разом	24

7. Теми лабораторних занять

№ п/п	Назва теми	Кількість годин
1	Не передбачено навчальним планом	
	Разом	

8. Самостійна робота

№ п/п	Назва теми	Кількість годин
1	Опрацювання матеріалу лекцій	30
2	Підготовка до практичних занять	60
3	Опрацювання матеріалів та результатів отриманих на практичних заняттях	12
	Разом	102

9. Індивідуальні завдання

Не передбачено навчальним планом.

10. Методи навчання

При викладанні курсу використовуються наступні навчальні методи:
– демонстрація;
– ілюстрація;
– розповідь;
– спостереження;
– дослідження;
– практичне заняття;
– виконання вправ.

11. Методи контролю

1) поточний контроль (оцінювання роботи студентів на практичних заняттях);
2) модульний контроль за змістовними модулями;
3) семестровий 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			
Виконання і захист практичних робіт	0...5	6	0...30
Модульний контроль	0…20	1	0…20
Змістовний модуль 2			
Виконання і захист практичних робіт	0...5	6	0...30
Модульний контроль	0…20	1	0…20
Усього за семестр			**0…100**

Білет для іспиту складається з тридцяти тестових теоретичних та практичних питань. Максимальна сума балів - 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Задовільно (60-74). Мати мінімум знань та умінь. Захистити всі практичні роботи та здати тестування. Вміти самостійно налаштовувати права доступу до файлів системи, робити перехват пакетів за допомогою Wireshark та вміти виявити попередження щодо безпеки системи за допомогою Sguil. Мати уявлення про роботу брандмауера. Вміти задокументувати події безпеки.
Добре (75 - 89). Твердо знать мінімум знань, виконати і захистити усі практичні завдання, здати тести та поза аудиторну самостійну роботу. Показати вміння виконувати завдання в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах. Вміти пояснювати принцип роботи брандмауера, системи виявлення вторгнень на стороні хоста (HIDS), вміти налаштувати правила Snort, виявляти події безпеки за допомогою Sguil, користуватися файлами журналів за допомогою ELSAв системі SecurityOnion.
Відмінно (90 - 100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх.

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. Інформаційна безпека. Терміни і визначення : довід. / В. Я. Пєвнєв, Т. В. Лавровська ; Міністерство освіти і науки України, Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", 2016. - 84 с . – електронне видання.

14. Рекомендована література

Базова

1. Bandler J. Cybercrime Investigations / J. Bandler, A. Merzon. – CRC Press, 2020. – 360 p.
2. Fischer R. Introduction to Security / R. Fischer, E. Halibozek, D. Walters. – Butterworth-Heinemann, 2018. – 586 p.

Допоміжна

1. WylieP. The Pentester BluePrint: Starting a Career as an Ethical Hacker / P. Wylie, K. Crawley. – Wiley, 2020. – 192 p.

15. Інформаційні ресурси

1. https://www.netacad.com/
2. https://www.ossec.net/
3. https://bammv.github.io/sguil/index.html
4. http://elsa.sourceforge.net/
5. https://securityonionsolutions.com/
6. https://www.snort.org/
7. https://talosintelligence.com/