МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

В.о. проректора з наукової роботи

_____ Микола ДИВАК

«_____» _____ 2023 р.

РОБОЧА ПРОГРАМА

з дисципліни

«Безпека комп'ютерних та кіберфізичних систем»

Ступінь вищої освіти (освітньо – кваліфікаційний рівень) – **доктор філософії**

Галузь знань – **12 Інформаційні технології**

Спеціальність – **123 Комп'ютерна інженерія**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	СРС (год.)	Разом (год.)	Зал. (сем.)
Денна	1	2	20	20	110	150	2

Тернопіль – ЗУНУ

2023

Робочу програму склав д.т.н., професор, завідувач кафедри кібербезпеки Яцків Василь Васильович

Затверджено на засіданні кафедри кібербезпеки, протокол № 2 від 12 жовтня 2023 р.

Завідувач кафедри кібербезпеки,
д.т.н., професор Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності «Комп'ютерна інженерія», протокол № 3 від 24.11 2023 р.

Голова ГЗС
д-р. техн. наук, проф. Олег БЕРЕЗЬКИЙ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Безпека комп'ютерних та кіберфізичних систем»

Опис дисципліни «Безпека комп'ютерних та кіберфізичних систем»

Дисципліна «Безпека комп'ютерних та кіберфізичних систем»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань: 12 - Інформаційні технології	Вибіркова
Кількість залікових модулів	Спеціальності – 123 "Комп'ютерна інженерія"	Рік підготовки: *Денна – 1* Семестр: *Денна – 2*
Кількість змістових модулів – 2	Ступінь вищої освіти – доктор філософії	Лекції: *Денна – 20* Практичні заняття: *Денна – 20*
Загальна кількість годин – 150		Самостійна робота: *Денна – 80*
Тижневих годин: з них аудиторних: 4		Вид підсумкового контролю – залік

2. Мета і завдання дисципліни «Безпека комп'ютерних систем та кіберфізичних систем»

2.1. Мета вивчення дисципліни.

Метою «Безпека комп'ютерних та кіберфізичних систем» є отримання знань та умінь, які необхідні для успішного виявлення вразливостей у комп'ютерних системах та мережах і усунення проблем безпеки шляхом розробки та впровадження заходів захисту.

2.2. Завдання вивчення дисципліни:

Завдання дисципліни **«Безпека комп'ютерних та кіберфізичних систем»** полягає в навчанні аспірантів:

- розробляти та презентувати обґрунтований план досліджень, планувати та проводити експерименти щодо розробки методів забезпечення кібербезпеки інформаційних і комп'ютерних систем, віртуальних систем та критичних інфраструктур;

- визначати, аналізувати та поєднувати інформацію з різних джерел та підготовлювати нову форму вторинної інформації, зокрема, щодо забезпечення загальних та спеціальних вимог до кібербезпеки;

- ініціювати та виконувати оригінальні дослідження в напрямку освоєння методів забезпечення кібербезпеки інформаційних і комп'ютерних систем у звичайних та надзвичайних ситуаціях та досягати наукових результатів, які створюють нові знання;

- управляти науковими проектами або писати пропозиції на фінансування наукових досліджень, зокрема наукових досліджень методів і систем запобігання, виявлення, обробки та усунення наслідків інцидентів кібербезпеки, а також методики попередження та розслідування кіберзлочинів;

- використовувати сучасні математичні методи, моделі, інформаційні технології та техніки для забезпечення кібернетичної та інформаційної безпеки інформаційних і комп'ютерних систем;

- визначати місію, прогнозувати та планувати цілі і задачі технологій кібербезпеки інформаційних і комп'ютерних систем.

2.3 Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

Здатність виконувати дослідження, досягати наукових результатів, які створюють нові знання у галузі кібербезпеки.

Розуміння принципів функціонування систем і засобів криптографічного та технічного захисту інформації.

Уміння відслідковувати тенденції й напрямки розвитку інформаційної та кібербезпеки.

2.4. Результати навчання

В результаті вивчення дисципліни аспірант повинен:

Знати сучасні методи проведення досліджень в галузі кібербезпеки.

Вміти розв'язувати задачі синтезу та аналізу об'єктів професійної діяльності кібербезпеки.

Вміти досліджувати проблеми кібербезпеки критичної інфраструктури.

Вміти синтезувати науково обгрунтовані рішення по захисту інформації в кіберсистемах та кіберфізичних системах.

3. Зміст дисципліни «Безпека комп'ютерних та кіберфізичних систем»

Змістовий модуль 1. Кіберпростір та кібербезпека

Тема 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення. Кіберпростір і кібербезпека - головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу.

Тема 2. Поширені атаки на комп'ютерні системи.

Шкідливе ПЗ. Типи шкідливого ПЗ. Віруси. Трояни. Класифікація троянів. Типи мережевих атак. Віруси вимагачі.

Тема 3. Типи атак на комп'ютерні системи.

Розвідка. Атаки доступу. Типи атак доступу. Атаки методом соціальної інженерії. DDoS- атаки.

Тема 4. Атаки на службові протоколи.

Вразливості ARP. Підробка записів хешу ARP. Атаки DNS. Тунелювання DNS. DHCP. Протоколи HTTP і HTTPS. Бази даних з веб-доступом.

Тема 5. Захист кінцевих пристроїв.

Захист від вторгнення на рівні хоста. Безпека додатків. Оцінка вразливостей кінцевих пристроїв. Загальна система оцінки вразливостей. Безпечне управління пристроями. Системи управління інформаційною безпекою.

Тема 6. Безпека хмарних технологій.

Принцип хмари. Безпека хмарних систем. Методи шифрування в хмарних сервісах.

Змістовий модуль 2. Моніторинг безпеки

Тема 7. **Моніторинг безпеки засоби моніторингу.**

Моніторинг загальних протоколів. Технології забезпечення безпеки. Файли журналів. Журнали кінцевих пристроїв. Мережеві журнали. Засоби моніторингу мережевої активності. Аналізатори мережевих протоколів. NetFlow. Системи SIEM.

Тема 8. **Аналіз даних вторгнень.**

Оцінка попереджень. Робота з даними безпеки мережі. Дослідження мережевих даних. Цифрова технічна експертиза. Порядок збору доказів.

Тема 9. **Реагування на інциденти.**

Моделі реагування на інциденти. Ланцюг кібервбивства. Ромбовидна модель вторгнення. Схема VERIS.

Тема 10. **Обробка інцидентів.**

Типи груп CSIRT. CERT. Життєвий цикл реагування на інциденти NIST. Виявлення і аналіз. Дії після інцидентів. Збір і зберігання даних про інциденти.

4. Структура залікового кредиту з дисципліни «Безпека комп'ютерних та кіберфізичних систем»

	Кількість годин	
	Лекції	Практичні заняття
Змістовий модуль 1 **Типи комп'ютерних атак**		
Тема 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення.	2	2
Тема 2. Поширені атаки на комп'ютерні системи.	2	2
Тема 3. Типи атак на комп'ютерні системи.	2	2
Тема 4. Атаки на службові протоколи	2	2
Тема 5. Захист кінцевих пристроїв	2	2
Тема 6. Безпека хмарних технологій	2	2
Змістовий модуль 2. Моніторинг безпеки		
Тема 7. Моніторинг мережі і засоби моніторингу	2	2
Тема 8. Аналіз даних вторгнень		2
Тема 9. Реагування на інциденти	2	2
Тема 10. Обробка інцидентів	2	2
Разом	20	20

5. Тематика практичних (семінарських або лабораторних) занять

Практичне заняття №1

Тема: Дослідження трафіку HTTP і HTTPS за допомогою програми Wireshark

Мета: навчитися аналізувати і перехоплювати трафік HTTP і HTTPS за допомогою програми Wireshark.

Питання для обговорення:

1. Перехоплення і перегляд HTTP-трафіку
2. Перехоплення і перегляд HTTPS-трафіку

Література: 1, 2.

Практичне заняття №2

Тема: Дослідження трафіку DNS

Мета: навчитися використовувати програму Wireshark в системі Windows для фільтрації пакетів DNS і перегляду інформації як про пакети запитів, так і відповідей DNS.

Питання для обговорення:

1. Перехоплення трафіку DNS
2. Вивчення трафіку DNS-запиту
3. Вивчення трафіку DNS-відповіді

Література: 1, 2.

Практичне заняття №3

Тема: Шифрування і розшифрування даних з допомогою OpenSSL

Мета: Вивчення алгоритмів шифрування і розшифрування даних з допомогою OpenSSL.

Питання для обговорення:

1. Шифрування повідомлень за допомогою OpenSS
2. Розшифрування повідомлень за допомогою OpenSS

Література: 1, 2.

Практичне заняття №4

Тема: Вивчення сеансів зв'язку за протоколами Telnet і SSH за допомогою програми Wireshark

Мета: вивчення протоколів зв'язку Telnet і SSH.

Питання для обговорення:

1. Вивчення сеансу Telnet за допомогою програми Wireshark.
2. Вивчення сеансу SSH за допомогою програми Wireshark.

Література: 1, 2.

Практичне заняття №5

Тема: Налаштування середовища з кількома ВМ

Мета: Навчитися налаштовувати середовища з кількома ВМ

Питання для обговорення:

Налаштування віртуальної мережі шляхом підключення одої до одної декількох віртуальних машин в Virtualbox

Література: 1, 2

Практичне заняття №6

Тема: Правила Snort і правила брандмауера

Мета: Навчитися створювати правила Snort і правила брандмауера

Питання для обговорення:

1. Підготовка віртуального середовища.
2. Брандмауер і журнали IDS.
3. Завершення і очищення процесу Mininet.

Література: 1, 2

Практичне заняття №7

Перетворення даних в універсальний формат

Мета: навчити студентів, як знаходити місце зберігання файлів журналів, а також як управляти ними і переглядати їх.

Питання для обговорення:

1. Нормалізація мітки часу в файлі журналу.
2. Нормалізація мітки часу в файлі журналу Apache
3. Підготовка файлу журналу в Security Onion

Практичне заняття №8

Тема: Зчитування виконуваного файлу з PCAP

Мета: Навчитися аналізувати трафік в раніше перехопленому файлі PCAP і витягувати виконуваний файл з файлу а також розуміння виконання мережевих транзакцій на рівні пакетів.

Питання для обговорення:

1. Підготовка віртуального середовища.
2. Аналіз попередньо записаних журналів і перехоплень трафіку.

Література: 1, 2.

Практичне заняття №9

Тема: Інтерпретація даних HTTP і DNS для ізоляції хакера

Мета: навчитися відслідковувати по журналам використання відомих вразливостей DNS і HTTP.

Питання для обговорення:

1. Підготовка віртуального середовища.
2. Вивчення атаки на основі впровадження шкідливого коду SQL.
3. Аналіз крадіжки даних.

Література: 1, 2.

Практичне заняття №10

Тема: Обробка інцидентів

Мета: навчитися обробляти інциденти кібербезпеки.

Питання для обговорення:

1. Зараження інтернет-хробаком і агентом розподіленої атаки типу «Відмова в обслуговуванні» (DDoS-атака).
2. Несанкціонований доступ до зарплатних відомостях.

Література: 1, 2.

6. Самостійна робота

№ п/п	Тематика
1	Елементи центру моніторингу та управління безпекою SOC
2	Технології в SOC
3	Корпоративний SOC і послуги з управління інформаційною безпекою
4	Безпека кінцевих пристроїв.
5	Захист від шкідливого ПЗ на рівні хоста.
6	Захист від шкідливого ПЗ на рівні мережі.
7	Рішення для захисту від складного шкідливого програмного забезпечення Cisco AMP.
8	Міжмережеві екрани на рівні хоста.
9	Виявлення аномалій мережі
10	Перевірка мережі на уразливості
11	Загальна система оцінки вразливостей (Common Vulnerability Scoring System, CVSS).
12	База вразливостей CVE.
13	Стандарт безпеки даних індустрії платіжних карт (PCI DSS).
14	Управління ризиками.
15	Контроль вразливостей
16	Моніторинг безпеки
17	Протоколи HTTP, HTTPS, ICMP
18	Протоколи електронної пошти
19	Технології перетворення мережевих адрес (NAT) і перетворення адрес портів (PAT)
20	Реагування на інциденти і їх обробка
21	Структура правила Snort.
22	Робота в Sguil. Запити в Sguil. Обробка подій в Sguil.
23	Реагування на інциденти і їх обробка
24	Життєвий цикл реагування на інциденти NIST.
25	Етапи виявлення та аналізу інцидентів.

7. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни **«Безпека комп'ютерних та кіберфізичних систем»** використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- стандартизовані тести;
- поточне опитування;
- залікове модульне тестування та опитування;
- наскрізні проекти;
- командні проекти;
- аналітичні звіти, реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- оцінювання результатів КПІЗ;
- презентації та виступи на наукових заходах;
- розрахункові роботи;
- завдання на лабораторному обладнанні, тренажерах, реальних об'єктах тощо;
- екзамен;
- інші види індивідуальних та групових завдань.

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

8. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 10
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 10

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка 2019. – 580.

2. Messier, R. CEH V10 Certified Ethical Hacker Study Guide. John Wiley & Sons. 2019. – 584 с.

3. Warsinske, J., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., & Vasquez, M. The Official (ISC) 2 Guide to the CISSP CBK Reference. John Wiley & Sons. 2019. – 928 с.

4. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), № 45, ст.403 зі змінами від 28.07.2022 року. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. – pp. 466-478.

6. Hamdani, Syed Wasif Abbas, et al. "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons." *ACM Computing Surveys (CSUR)* 54.3, 2021. – pp.1-36

7. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. – 341 p.

8. Grubb S. How Cybersecurity Really Works. 2021. – 219 p.

9. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.

10. Maurushat, Alana. *Ethical hacking*. University of Ottawa Press, 2019.

11. Cisar, P., & Pinter, R. Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences*, *9*(4), 2019, pp.129-149.

12. Teixeira, D. Metasploit Penetration Testing Cookbook - Third Edition. Packt Pub- lishing Ltd. 2018.

13. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.