МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____Ігор ЯКИМЕНКО
«___» _____ 2023 р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____Віктор ОСТРОВЕРХОВ
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА
з дисципліни
«РЕАГУВАННЯ НА КОМП'ЮТЕРНІ ІНЦИДЕНТИ»

ступінь вищої освіти – **бакалавр**
галузь знань – **12 Інформаційні технології**
спеціальність – **125 Кібербезпека**
освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. (год.)	ІРС (год.)	Тренінг КПІЗ (год.)	СРС (год.)	Разом (год.)	Зал. (сем.)
Денна	4	7	26	12	2	12	98	150	7

Тернопіль - 2023

Робочу програму склав викладач кафедри кібербезпеки, Ігнатєв Ігор Васильович.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 28.08.2023 р.

Завідувач кафедри кібербезпеки — Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол №1 від 30.08.2023 р.

Голова групи забезпечення спеціальності — Василь ЯЦКІВ

Гарант ОП — Ігор ЯКИМЕНКО

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. **Опис дисципліни “ Реагування на комп’ютерні інциденти””**

Дисципліна “ Реагування на комп’ютерні інциденти””	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань 12 - Інформаційні технології	Статус дисципліни – вибіркова Мова навчання - українська
Кількість залікових модулів – 4	Спеціальність - 125 Кібербезпека	Рік підготовки: 4 Семестр: 7
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: 26 год. Лабораторні заняття: 12 год.
Загальна кількість годин – 150		Самостійна робота: 98 год., тренінг – 12 год. Індивідуальна робота: 2 год.
Тижневих годин – 14, з них аудиторних – 3		Вид підсумкового контролю – залік

2. Мета і завдання дисципліни “ Реагування на комп’ютерні інциденти”

2.1. Мета вивчення дисципліни.

Метою дисципліни є - отримання знань та навичок, необхідних для успішного виконання завдань аналітика, який працює в центрі моніторингу та управління безпекою.

2.2. Завдання вивчення дисципліни:

Основне завдання дисципліни дати студентам теоретичну та практичну підготовку, зокрема: аналізувати роботу мережевих протоколів і служб; класифікувати різні типи мережевих атак; використовувати засоби мережевого моніторингу для визначення атак на мережеві протоколи і служби; застосовувати різні способи запобігання несанкціонованому доступу до комп'ютерних мереж, хостів і даними; виявляти попередження безпеки мережі; аналізувати дані про вторгнення в мережу для перевірки потенційних загроз; застосовувати моделі реагування для усунення інцидентів безпеки.

2.3. В результаті вивчення дисципліни студент повинен знати:

− принципи та переваги децентралізації;

- методи, алгоритми та програмні засоби забезпечення цілісності та конфіденційності даних в технології блокчейн;
- готовність до інцидентів. Підготовка процесу. Підготовка персоналу.;
- аналіз чутливості. Постановка задачі. Аналіз чутливості методом приросщення. аналіз чутливості прямим методом. Багатоваріантний аналіз;
- принцип функціонування блокчейн;
- алгоритми доказу виконаної роботи;
- статистичний аналіз. Постановка задачі. Аналіз методом найгіршого випадку. Аналіз методом Монте-Карло.;
- принципи роботи криптовалюти біткоін;
- параметрична оптимізація.Вибір цільової функції. Методи пошуку екстремуму. Методи одномірного пошуку екстремуму. Лінійне програмування. .

2.4. В результаті вивчення дисципліни студент повинен уміти:

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

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

- 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.

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

3. Зміст дисципліни " Реагування на комп'ютерні інциденти""

Змістовий модуль 1. Теоретичні основи САПР комп'ютеризованих систем управління та автоматики

Тема 1. Вступ. Картини загроз, мотиви зловмисника, фінансові махінації, Методи атаки, анатомія атаки.

Література: 1-7

Тема 2. Готовність до інцидентів. Підготовка процесу. Підготовка персоналу. Підготовка технології. .

Література: 1-14, 16, 18.

Тема 3. Реагування на кіберінциденти. Нестандартні підключення. Незвичайні порти, процеси, служби, файли. Захист облікових записів. .

Література: 9-15,

Тема 4. Інструменти віддаленого сортування. Windows Management Instrumentation. Привильні підходи. Доступ з допомогою PowerShell. Фреймворки.

Література: 4, 6, 8, 10, 12.

Тема 5.Створення дампу пам'яті . Порядок збору даних. Підготовка носія. Процес збору даних. Агенти для віддаленого збору даних. Аналіз пам'яті віддаленої системи

Література: 15-19.

Тема 6. Створення образа диска. Захист цілісності доказів. Використання апаратного блокування даних. Використання завантажувального дистрибутива Linux. Створення образа віртуальної машини.

Література: 15-19.

Тема 7. Моніторинг мережевої безпеки. Архітектура мереж. Аналіз текстового журнала

Література: 15-99.

Змістовний модуль 2. Реагування на комп'ютерні інциденти

Тема 8. Аналіз журналу подій. Журнал подій. Доступ до об'єкта. Аудит змін конфігурацій системи. Аудит процесів.

Література: 15-29, .

Тема 9. Аналіз пам'яті. Важливість базових показників. Джерела даних пам'яті. Плагіни. Служби. Вивчення мережевої активності.

Література: 15-29,.

Тема 10. Аналіз шкідливих програм. Аналітичні сервіси. Статистичний аналіз. Динамічний аналіз. Реверс-інжиніринг.

Література: 13, 29, ,.

Тема 11. Вивільнення інформації з образу жорсткого диска. Аналіз тимчасових папок. Аналіз реєстра. Активність браузера. Тіньові копії. Автоматичне сортування

Література: 33-29.

Тема 12. Аналіз поширення по мережі. Атаки pass-the-ticket и overpass-the-hash Планувальник завдань. SSH - тунелі

Література: 15-29.

4. Структура залікового кредиту

		Кількість годин

	Лекції	Лабор.	Самост. робота	Інд. робота	Тренінг, КПІЗ	Контр. заходи
Змістовий модуль 1. Теоретичні основи САПР комп'ютеризованих систем управління та автоматики						
Тема 1. Вступ. Картини загроз, мотиви зловмисника, фінансові махінації, Методи атаки, анатомія атаки.	2		10		1	Поточне опитування
Тема 2. Готовність до інцидентів. Підготовка процесу. Підготовка персоналу. Підготовка технології. .	2	2	10		1	Поточне опитування
Тема 3. Реагування на кіберінциденти. Нестандартні підключення. Незвичайні порти, процеси, служби, файли. Захист облікових записів.	2		10		1	Поточне опитування
Тема 4. Інструменти віддаленого сортування. Windows Management Instrumentation. Привильні підходи. Доступ з допомогою PowerShell. Фреймворки.	2	2	10		1	Поточне опитування
Тема 5.Створення дампу пам'яті . Порядок збору даних. Підготовка носія. Процес збору даних. Агенти для віддаленого збору даних. Аналіз пам'яті віддаленої системи	2	2	9		1	Поточне опитування
Тема 6. Створення образа диска. Захист цілісності доказів. Використання апаратного блокування даних. Використання завантажувального дистрибутива Linux. Створення образа віртуальної машини.	2		8	1	1	Поточне опитування
Змістовий модуль 2. Методи синтезу та аналізу комп'ютеризованих систем управління в САПР						
Тема 7. Аналіз статичних режимів. Постановка задачі. Метод простої ітерації. Метод Зейделя. Метод Ньютона. Кусково - лінійний метод Ньютона.	2		8		1	Поточне опитування
Тема 8. Методи рішення системи лінійних алгебраїчних рівнянь. Метод Гауса. Метод LU-розкладання. Рішення систем лінійних рівнянь з розрідженими матрицями.	2	2	8		1	Поточне опитування
Тема 9. Аналіз чутливості. Постановка задачі. Аналіз чутливості методом прирощення. Аналіз чутливості прямим методом. Багатоваріантний аналіз.	2	2	8	1	1	Поточне опитування
Тема 10. Виготовлення графічної і текстової документації за допомогою САПР.	2	2	8	1	1	Поточне опитування
Тема 11. Статистичний аналіз. Постановка задачі. Аналіз методом найгіршого випадку. Аналіз методом Монте-Карло.	2		4	1	1	Поточне опитування
Тема 12. Параметрична оптимізація.Вибір цільової функції. Методи пошуку екстремуму. Методи одномірного пошуку екстремуму.	2		4	1	1	Поточне опитування

Лінійне програмування.						
Разом	**26**	**12**	**97-12**	**2**	**12**	**Іспит**

5. Тематика лабораторних робіт.

Лабораторна робота №1

Тема: Встановлення VirtualBox з операційною системою Ubuntu на Windows 10.

Мета: Вивчення середовища програми VirtualBox. Робота з елементами програми.

Питання для обговорення:

1. Завантаження та встановлення VirtualBox на Windows 10.
2. Типи позначень та функціонал об'єктів.
3. Вимоги до системи.

Література: 1-19.

Лабораторна робота №2

Тема: Відслідквування файлів в UBUNTU

Мета: Визначення прав доступу до файлів

Питання для обговорення:

1.Основні елементи системи.

2.Основні команди.

3.Вимоги до системи.

Література: 1-19.

Лабораторна робота №3

Тема: Засоби аналізу трафіку

Мета: Аналіз трафіку у системі Linux

Питання для обговорення:

1. Основні елементи системи.
2. Основні команди.
3. Трафік системи.

Література: 1-19.

Лабораторна №4

Тема: Налаштування та розповсюдження TIP

Мета: Встановлення та налаштування компонентів

Питання для обговорення:

1. Основні елементи системи.
2. Основні команди.
3. Перегляд структур даних.

Література: 1-19.

Лабораторна №5

Тема: Контейнери у Linux

Мета: Встановлення конфігурацій Linux

Питання для обговорення:

1. Основні елементи системи.
2. Основні команди.
3. Робота з SSH
4. Література: 1-19.

6. Комплексне практичне індивідуальне завдання

Варіанти КПІЗ з дисципліни «Інтернет - речей»

1. Підключення до Інтернету нових пристроїв.
2. Створення Web - інтерфейсу.
3. Керування пристроєм за допомогою мобільного телефону.
4. Підключення до хмарного сервісу.
5. Аналіз та обробка даних.

Студент може самостійно запропонувати та погодити з викладачем тему КПІЗ.

7. 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	Політики безпеки
16	Контроль вразливостей
17	Моніторинг безпеки
18	Протоколи HTTP, HTTPS, ICMP
19	Протоколи електронної пошти
20	Технології перетворення мережевих адрес (NAT) і перетворення адрес портів (PAT)
21	Реагування на інциденти і їх обробка
22	Структура правила Snort.
23	Робота в Sguil. Запити в Sguil.
24	Обробка подій в Sguil.
25	Реагування на інциденти і їх обробка
26	Життєвий цикл реагування на інциденти NIST.
27	Етапи виявлення та аналізу інцидентів.

8. Тренінг з дисципліни

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Рекомендується проведення тренінгу за наступною темою: Розробка та дослідження системи з використанням програмного забезпечення.

9. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, індивідуальні заняття; робота в Інтернет.

10. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

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

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни "**Реагування на комп'ютерні інциденти**" визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3
30%	40%	30%
1. Усне опитування на заняттях (6 тем по 4 бали) - max 24 бали. 2. Письмова робота - max 56 бали. 3. Практичне завдання (2 практичних завдань по 10 бали)- max 20 балли	1. Усне опитування на заняттях (6 тем по 4 бали) - max 24 бали. 2. Письмова робота - max 52 балів. 3. Практичне завдання (3 практичних завдань по 8 балив)- max 24 бали	1. Підготовка КПІЗ - max 40 балів. 2. Захист КПІЗ -max 40 балів. 3. Участь у тренінгах - max 20 балів

Шкала оцінювання:

За шкалою університету	**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)

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

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1-12
2.	Програмне забезпечення Packet Tracer	1-12
3.	Операційна система Linux	4-12

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Курс мережевої академії Cisco IoT Fundamentals: Connecting Things, 2020 р. Режим доступу: https://www.netacad.com/courses/iot/iot-fundamentals

2. Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 1. Основи і технології / За ред. В. С. Харченка. - Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. -547 с.

3. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security of IoT: Practicum / Kharchenko V.S. and Sklyar V.V. (Eds.) – Ministry of Education and Science of Ukraine, National Aerospace University "KhAI", Ternopil National Economic University, 2019. –

98 p.

4. 5.Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 2. Modelling and Development /V.S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 547 p.

5. Sarhan, Q. I. (2018). Internet of things: a survey of challenges and issues. International Journal of Internet of Things and Cyber-Assurance, 1(1), 40-75.

6. Puliafito, C., Mingozzi, E., Longo, F., Puliafito, A., & Rana, O. (2019). Fog computing for the internet of things: A Survey. ACM Transactions on Internet Technology (TOIT), 19(2), 1-41.

7. Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. Computer Networks, 153, 113-131.

8. Ravidas, S., Lekidis, A., Paci, F., & Zannone, N. (2019). Access control in Internet-of-Things: A survey. Journal of Network and Computer Applications, 144, 79-101.

9. Oliveira, L., Rodrigues, J. J., Kozlov, S. A., Rabêlo, R. A., & Albuquerque, V. H. C. D. (2019). MAC layer protocols for Internet of Things: A survey. Future Internet, 11(1), 16.

10. Ray, P. P., Dash, D., & De, D. (2019). Edge computing for Internet of Things: A survey, e-healthcare case study and future direction. Journal of Network and Computer Applications, 140,

11. Jason Callaway. COMPUTER NETWORKING: 2 BOOKS IN 1 – All You Need to Know to Become a Networking Engineer from Scratch (Wireless Technologies, Network System, IP subnetting, Cybersecurity, and much more) - (October 8, 2021), 181 pages.

12. Scott Jernigan, Mike Meyers. CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008) 8th Edition - (March 28, 2022), 976 pages.

13. Craig Berg. Cisco Networking Essentials: Complete Guide To Computer Networking For Beginners And Intermediates (Code tutorials) Paperback – June 15, 2020, 85 pages.

14. Larry L. Peterson, Bruce S. Davie. Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition- (March 29, 2021), 848 pages.

15. José Manuel Ortega. Mastering Python for Networking and Security: Leverage the scripts and libraries of Python version 3.7 and beyond to overcome networking and security issues, 2nd Edition - (January 4, 2021), 538 pages.

16. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.

17. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.

18. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата. – М.: Юрайт, 2019. - 349с

19. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction - March 7, 2019, 504 pages.