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

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«30» 08 2024 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«30» 08 2024 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. роботи (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік / екзамен (семестр)
Денна	4	7	26	12	2	12	98	150	Залік (7)

30.08.2024 р.

Тернопіль
2024

Робочу програму склав викладач кафедри кібербезпеки Ігор ІГНАТЄВ.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол №1 від 30 серпня 2024 р.

Голова групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант ОП _____ Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ “Реагування на комп’ютерні інциденти”

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

Дисципліна «Соціальна інженерія»	Галузь знань, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів – 5	Галузь знань 12 «Інформаційні технології»	Статус дисципліни - вибіркова Мова навчання - українська
Кількість залікових модулів – 3	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 – 10, 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. Основне завдання дисципліни дати студентам теоретичну підготовку з уміння реагувати на комп’ютерні інциденти та формування навиків дослідження причин, що призвело до конкретної дії або ситуації.

2.3. У результаті вивчення навчальної дисципліни студент повинен:

знати:

- Основні принципи захисту інформаційних систем.
- Види загроз та вразливостей у комп'ютерних системах.
- Моделі та методи захисту даних.
- Визначення та типологія комп'ютерних інцидентів.
- Різні види атак (наприклад, DDoS, фішинг, малваре) і методи їх виконання.
- Етапи реагування на комп'ютерний інцидент: підготовка, виявлення, стримування, ліквідація, відновлення.
- Принципи побудови ефективного плану реагування на інциденти.
- Роль та обов'язки команди з реагування на інциденти (Incident Response Team, IRT).
- Використання систем виявлення вторгнень (IDS/IPS).
- Інструменти для аналізу мережевого трафіку.

вміти:

- Виявляти різні типи інцидентів, такі як вторгнення, вірусні атаки, фішинг та інші кіберзагрози.

- Використовувати інструменти для моніторингу та аналізу мережевого трафіку, журналів подій та інших джерел даних.
- Оперативно приймати рішення щодо стримування, ліквідації та відновлення систем після інциденту.
- Виконувати необхідні дії для мінімізації шкоди, завданої інцидентом, та відновлення нормальної роботи системи.
- Вести точний журнал подій під час інциденту.
- Проводити аналіз причин і наслідків інциденту для розробки подальших захисних заходів.
- Готувати детальні звіти про інцидент для керівництва та правоохоронних органів.
- Використовувати програмне забезпечення для виявлення та аналізу загроз (IDS/IPS, антивіруси, фаєрволи тощо).
- Застосовувати методи збору та аналізу цифрових доказів.
- Створювати і впроваджувати плани реагування на інциденти, включаючи стратегії комунікації та розподіл відповідальності.
- Планувати тренування та навчання для персоналу щодо дій під час інцидентів.
- Ефективно взаємодіяти з командою з реагування на інциденти (IRT) та іншими зацікавленими сторонами.
- Забезпечувати співпрацю з правоохоронними органами у разі необхідності.
- Проводити постінцидентний аналіз для виявлення слабких місць у системах безпеки.

2.4. Передумови для вивчення дисципліни

Перелік дисциплін, які мають бути вивчені раніше: програмування на мові Python; Кібернетична безпека; Операційні системи; Алгоритми та структури даних; Архітектура комп'ютерів та систем.

Перелік раніше здобутих результатів навчання: використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності; діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. Розробляти моделі загроз та порушника; застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах.

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: 1-14, 32-42

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

Література: 1-14, 16, 18, 22, 35.

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

Література: 9-17, 22-37.

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

Література: 4, 6, 8, 10, 12, 30, 37.

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: 15-29.

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

віртуальної машини.

Література: 15-20, 31, 35, 40.

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

Література: 15-29, 35-40.

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: 15-22, .

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

Література: 15-26,.

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

Література: 13, 26, ,.

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

Література: 33-26.

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

Література: 15-26.

4. Структура залікового кредиту

	Кількість годин					
	Лекції	Лабор.	Самост. робота	Інд. робота	Тренінг,	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	6	Поточне опитування
Тема 2. Готовність до інцидентів. Підготовка процесу. Підготовка персоналу. Підготовка технології. .	2	2	10			
Тема 3. Реагування на кіберінциденти. Нестандартні підключення. Незвичайні порти, процеси, служби, файли. Захист облікових записів.	2		10			
Тема 4. Інструменти віддаленого сортування. Windows Management Instrumentation. Привильні підходи. Доступ з допомогою PowerShell. Фреймворки.	2	2	7			
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			
Тема 6. Створення образа диска. Захист цілісності доказів. Використання апаратного блокування даних. Використання завантажувального дистрибутива Linux. Створення образа віртуальної машини.	4		8			
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			
Тема 8. Методи рішення системи лінійних	2	2	8			

алгебраїчних рівнянь. Метод Гауса. Метод LU-розкладання. Рішення систем лінійних рівнянь з розрідженими матрицями.						
Тема 9. Аналіз чутливості. Постановка задачі. Аналіз чутливості методом приросщення. Аналіз чутливості прямим методом. Багатоваріантний аналіз.	2	4	8	1	6	Поточне опитування
Тема 10. Виготовлення графічної і текстової документації за допомогою САПР.	2		8			
Тема 11. Статистичний аналіз. Постановка задачі. Аналіз методом найгіршого випадку. Аналіз методом Монте-Карло.	2		6			
Тема 12. Параметрична оптимізація.Вибір цільової функції. Методи пошуку екстремуму. Методи одномірного пошуку екстремуму. Лінійне програмування.	2		6			
Разом	**26**	**12**	**98**	**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: 1-22.

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: 1-22.

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: 1-22.

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: 1-22.

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: 1-22.

6. Самостійна робота

Для самостійної роботи кожному студенту пропонується виконання вибраного наскрізного завдання. Орієнтовна тематика наскрізних завдань:

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.

7. Організація та проведення тренінгу з дисципліни.

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.
2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.
3. Практична частина реалізується шляхом виконання одного завдання тренінгу.
4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносяться на тренінг.

Тематика тренінгу: «Практичні аспекти реагування на комп'ютерні інциденти: від виявлення до відновлення».

Мета тренінгу: Формування практичних навичок у студентів щодо ефективного реагування на комп'ютерні інциденти, включаючи виявлення загроз, ліквідацію наслідків та відновлення систем. Тренінг має допомогти учасникам зрозуміти весь процес реагування на інциденти та здобути необхідний досвід роботи з реальними інструментами кібербезпеки.

Завдання тренінгу: Ознайомити студентів з процесом реагування на комп'ютерні інциденти. Навчити учасників використовувати сучасні інструменти для виявлення, аналізу та реагування на інциденти. Відпрацювати командну взаємодію під час реагування на інциденти. Розвинути навички документування інцидентів та підготовки звітів.

Оцінити ефективність запропонованих заходів щодо ліквідації інцидентів та відновлення систем. Орієнтовна тематика завдань тренінгу:

1. Виявлення інциденту: Аналіз журналів подій, моніторинг мережевого трафіку для ідентифікації підозрілої активності.
2. Класифікація та пріоритезація інцидентів: Визначення типу та рівня критичності інциденту, визначення першочергових дій.
3. Ліквідація наслідків інциденту: Відключення уражених систем від мережі, ізоляція шкідливого ПЗ, відновлення даних з резервних копій.
4. Документування процесу реагування: Створення детального звіту про інцидент, включаючи зібрані дані, виконані дії та результати.
5. Постінцидентний аналіз: Виявлення причин інциденту, аналіз вразливостей, підготовка рекомендацій для запобігання повторенню інциденту.
6. Відновлення та оцінка ефективності: Перевірка функціонування відновлених систем, оцінка ефективності прийнятих заходів та їх оптимізація.

Цей тренінг спрямований на те, щоб студенти змогли отримати практичний досвід, необхідний для успішного реагування на комп'ютерні інциденти у реальних умовах.

8. Методи навчання.

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

9. Засоби оцінювання та методи демонстрування результатів навчання

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

- поточне опитування;
- підсумковий модульний контроль за кожним змістовним модулем;
- оцінювання виконання лабораторних робіт;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи;
- підсумковий письмовий екзамен.

10. 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:

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Соціальна інженерія» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота
Середнє арифметичне з оцінок, отриманих за теоретичне опитування на заняттях (1-12 теми)	Середнє арифметичне оцінок, отриманих за виконання та захист лабораторних робіт 1-5	Середнє арифметичне з оцінок, отриманих за виконання та презентацію одного завдання тренінгу	Оцінка за виконання і представлення вибраного наскрізного завдання

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)

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. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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*,

9. 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.

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

11. Russell Scott. Computer Networking: This Book Includes: Computer Networking for Beginners and Beginners Guide (All in One) - (December 28, 2019), 359 pages.

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

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

14. 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.

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

16.Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.
17.Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
18.William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction - March 7, 2019, 504 pages.
19.Paul Troncone, Carl Albing Ph. D. Cybersecurity Ops with bash: Attack, Defend, and Analyze from the Command Line - April 20, 2019, 306 pages.
20.Tye Darwin. Linux for hackers: learn cybersecurity principles with shell,python,bash programming using kali linux tools. A complete guide for beginners (hackers essentials) - december 4, 2020, 292 pages.
21.Mike McGrath. Bash in easy steps - February 25, 2019, 192 pages.
22.Ahmed Alkabary, Abhishek Prakash. Learn Bash Quickly: A Friendly Guide with Exercises to Easily Get Started with Bash Scripting - September 17, 2020, 85 pages.