Силабус курсу

Реагування на комп’ютерні інциденти

Ступінь вищої освіти – бакалавр

Рік навчання: 4

Семестр: 7

Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Ігор Ігнатєв
Контактна інформація	iiv@wunu.edu.ua

Даний курс познайомить вас з теоретичними та практичними аспектами реагування на комп’ютерні інциденти. Впровадження технології обіцяє численні переваги - ось чому дані технології є великий інтерес, що охопив різні сфери, від академічної спільноти до промисловості. Метою вивчення дисципліни є засвоєння необхідних знань щодо технологій проектування та технологій захисту інформації. Програма дисципліни передбачає навчання у формі лекцій та практичних занять.

У курсі будуть розглянуті всі важливі теми, що стосуються технології, розглядаються картини загроз, моніторинг мережевої безпеки, аналіз журналу подій.

Метою курсу «Реагування на комп’ютерні інциденти» отримання знань та навичок, необхідних для успішного виконання завдань аналітика, який працює в центрі моніторингу та управління безпекою

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Тема 1. Вступ. Картини загроз, мотиви зловмисника, фінансові махінації, Методи атаки, анатомія атаки.	Картини загроз, мотиви зловмисника, фінансові махінації, Методи атаки, анатомія атаки.	Поточне опитування
2/1	Тема 2. Готовність до інцидентів. Підготовка процесу. Підготовка персоналу. Підготовка технології. .	Готовність до інцидентів. Підготовка процесу. Підготовка персоналу. Підготовка технології. .	Поточне опитування

2/1	Тема 3. Реагування на кіберінциденти. Нестандартні підключення. Незвичайні порти, процеси, служби, файли. Захист облікових записів.	Реагування на кіберінциденти. Нестандартні підключення. Незвичайні порти, процеси, служби, файли. Захист облікових записів. .	Поточне опитування
2/1	Тема 4. Інструменти віддаленого сортування. Windows Management Instrumentation. Привильні підходи. Доступ з допомогою PowerShell. Фреймворки.	Windows Management Instrumentation. Привильні підходи. Доступ з допомогою PowerShell. Фреймворки.	Поточне опитування
2/1	Тема 5.Створення дампу пам’яті . Порядок збору даних. Підготовка носія. Процес збору даних. Агенти для віддаленого збору даних. Аналіз пам’яті віддаленої системи	Порядок збору даних. Підготовка носія. Процес збору даних. Агенти для віддаленого збору даних. Аналіз пам’яті віддаленої системи	Поточне опитування
2/1	Тема 6. Створення образа диска. Захист цілісності доказів. Використання апаратного блокування даних. Використання завантажувального дистрибутива Linux. Створення образа віртуальної машини.	Захист цілісності доказів. Використання апаратного блокування даних. Використання завантажувального дистрибутива Linux. Створення образа віртуальної машини.	Поточне опитування, тестування
2/1	Тема 7. Аналіз статичних режимів. Постановка задачі. Метод простої ітерації. Метод Зейделя. Метод Ньютона. Кусково - лінійний метод Ньютона.	Архітектура мереж. Аналіз текстового журнала	Поточне опитування
2/1	Тема 8. Методи рішення системи лінійних алгебраїчних рівнянь. Метод Гауса. Метод LU-розкладання. Рішення систем лінійних рівнянь з розрідженими матрицями.	Журнал подій. Доступ до об’єкта. Аудит змін конфігурацій системи. Аудит процесів.	Поточне опитування
2/1	Тема 9. Аналіз чутливості. Постановка задачі. Аналіз чутливості методом прирощення. Аналіз чутливості прямим методом. Багатоваріантний аналіз.	Важливість базових показників. Джерела даних пам’яті. Плагіни. Служби. Вивчення мережевої активності.	Поточне опитування

2/1	Тема 10. Виготовлення графічної і текстової документації за допомогою САПР.	Аналітичні сервіси. Статистичний аналіз. Динамічний аналіз. Реверс-інжиніринг.	Поточне опитування
2/1	Тема 11. Статистичний аналіз. Постановка задачі. Аналіз методом найгіршого випадку. Аналіз методом Монте-Карло.	Аналіз тимчасових папок. Аналіз реєстра. Активність браузера. Тіньові копії. Автоматичне сортування	Поточне опитування
2/1	Тема 12. Параметрична оптимізація.Вибір цільової функції. Методи пошуку екстремуму. Методи одномірного пошуку екстремуму. Лінійне програмування.	Атаки pass-the-ticket и overpass-the-hash Планувальник завдань. SSH - тунелі	Поточне опитування

Рекомендовані джерела інформації

1. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. – Харків : ПРОМАРТ, 2019. – 452 с.
2. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. – 412 с.
3. Drescher, D. *Blockchain basics* (Vol. 276). Berkeley, CA: Apress. 2017. http://www.softouch.on.ca/kb/data/Blockchain%20Basics.pdf
4. V.Yatskiv, N.Yatskiv, O. Bandrivskyi. “Proof of Video Integrity Based on Blockchain”, in *Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on*, 2019, pp. 431-434.
5. A. Panarello, N.Tapas, G.Merlino, F.Longo, A.Puliafito “Blockchain and IoT integration: A systematic survey”. ***Sensors****, vol.***18(8),** *2575,* pp.1-37, 2018.
6. M. Salimitari, M. Chatterjee. “An Overview of Blockchain and Consensus Protocols for IoT Networks”. arXiv preprint arXiv:1809.05613, 2018.
7. B. Yu, J.Wright, S.Nepal, L.Zhu, J.Liu, R.Ranjan. “IoT Chain: Establishing trust in the internet of things ecosystem using blockchain”. *IEEE Cloud Computing*, vol.5(4), pp.12-23, 2018.
8. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security Internet of Things: 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.
9. 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.
10. Chen, F., Tang, Y., Cheng, X., Xie, D., Wang, T., & Zhao, C. (2021). Blockchain-based efficient device authentication protocol for medical cyber-physical systems. *Security and Communication Networks*, Volume 2021, *2021*, Article ID 5580939, 13 p. https://doi.org/10.1155/2021/5580939

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

11. Оцінювання

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:

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 (1-10 теми)	Середнє арифметичне оцінок, отриманих за виконання та захист лабораторних робіт 1-6	Середнє арифметичне з оцінок, отриманих за виконання та презентацію 1 завдання тренінгу	Середнє арифметичне оцінок, отриманих за виконання 1 завдання самостійної роботи (реферат, есе, тощо) та їх презентацію.

12. Шкала оцінювання:

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