Силабус курсу

РЕАГУВАННЯ НА КОМП'ЮТЕРНІ ІНЦИДЕНТИ

Освітньо-професійна програма «Комп’ютерна інженерія»
Ступінь вищої освіти – бакалавр
Спеціальність: 123 «Комп’ютерна інженерія»
Рік навчання: 4**, Семестр:** 7
Кількість кредитів: 5**, Мова викладання:** українська та вірменська

Керівник курсу

ПІП Арутюнян Гамлет Арутюнович
Контактна інформація erfiltanx@yahoo.com

Опис дисципліни

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.

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

Тема	Результати навчання	Завдання
Вступ. Картини загроз, мотиви зловмисника, фінансові махінації, Методи атаки, анатомія атаки.	Знати класифікацію кібер-загроз	Питання
Готовність до інцидентів. Підготовка процесу. Підготовка персоналу і технології.	Знати класифікацію кіберінцидентів.	Питання лабораторна робота
Реагування на кіберінциденти. Нестандартні підключення. Незвичайні порти, процеси, служби, файли. Захист облікових записів	Знати класифікацію кіберінцидентів і засоби аналізу.	Питання лабораторна робота
Інструменти віддаленого сортування. Windows Management Instrumentation. Доступ з допомогою PowerShell.	Вміти користуватися Windows Management Instrumentation та PowerShell	Питання

Створення дампу пам’яті. Порядок збору даних. Підготовка носія. Агенти для віддаленого збору даних. Аналіз пам’яті віддаленої системи	Вміти користуватися засобами для віддаленого збору даних	Питання, лабораторна робота
Створення образа диска. Захист цілісності доказів. Використання апаратного блокування даних. Використання завантажувального дистрибутива Linux. Створення образа віртуальної машини	Вивчення середовища програми VirtualBox.	Питання, лабораторна робота
Моніторинг мережевої безпеки. Архітектура мереж. Аналіз текстового журнала	Вміти виконувати моніторинг мережевої безпеки	Питання
Аналіз журналу подій. Журнал подій. Доступ до об’єкта. Аудит змін конфігурацій системи. Аудит процесів	Вміти застосовувати засоби журналювання подій	Питання
Аналіз пам’яті. Важливість базових показників. Джерела даних пам’яті. Плагіни. Служби. Вивчення мережевої активності.	Вміти застосовувати засоби вивчення мережевої активності.	Питання, лабораторна робота
Аналіз шкідливих програм. Аналітичні сервіси. Статистичний аналіз. Динамічний аналіз. Реверс-інжиніринг.	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації	Питання, лабораторна робота
Вивільнення інформації з образу жорсткого диска. Аналіз тимчасових папок. Аналіз реєстра. Активність браузера. Тіньові копії. Автоматичне сортування	Вміти аналізувати активність прикладних процесів	Питання, лабораторна робота
Аналіз поширення по мережі. Атаки pass-the-ticket и overpass-the-hash Планувальник завдань. SSH - тунелі.	Знати основні види мережевих атак та засоби протидії	Питання

У процесі вивчення даної дисципліни використовуються наступні способи оцінювання та методи демонстрування результатів навчання: поточне опитування, тестування; презентації результатів виконаних завдань; оцінювання результатів самостійної роботи студентів; інші види індивідуальних і групових завдань; залік.

Політика щодо академічної доброчесності: списування під час здачі заліків та екзаменів заборонено (в т.ч. із використанням мобільних девайсів).

Літературні джерела

1. Yatskiv V., Yatskiv N., Bandrivskyi O.. “Proof of Video Integrity Based on Blockchain”, in Proc. Advanced Computer Information Technologies (ACIT), 2019 IEEE 9th International Conference on, 2019, pp. 431-434.

2. Panarello A., Tapas N., Merlino G., Longo F., Puliafito A. “Blockchain and IoT integration: A systematic survey”. Sensors, vol.18(8), 2575, pp.1-37, 2018.

3. Salimitari M., Chatterjee M. “An Overview of Blockchain and Consensus Protocols for IoT Networks”. arXiv preprint arXiv:1809.05613, 2018.

4. Yu B., Wright J., Nepal S., Zhu L., Liu J., Ranjan R. “IoT Chain: Establishing trust in the internet of things ecosystem using blockchain”. IEEE Cloud Computing, vol.5(4), pp.12-23, 2018.

5. 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.

6. 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.

7. 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.

Шкала оцінювання

За шкалою університету 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)