ЗАСОБИ ВИЯВЛЕННЯ ТА АНАЛІЗУ КОМП'ЮТЕРНИХ ВІРУСІВ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Перший (бакалаврський)
Мова викладання	Українська
Семестр	8
Кількість встановлених кредитів ЄКТС	8
Форми навчання, для яких викладається дисципліна	Очна (денна)

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: вміло застосовувати технології та засоби для виявлення та аналізу комп'ютерних вірусів; виконувати реверс-інжиніринг програмного забезпечення; використовувати навички програмування, технології розроблення алгоритмів і комп'ютерних програм на низькорівневій мові Assembler в середовищі masm64; проводити аналіз програмного забезпечення на предмет наявності комп'ютерних вірусів.

Зміст навчальної дисципліни. Основні положення, що лежать в основі засобів виявлення та налізу шкідливого програмного забезпечення. Структура виконуваного файлу PE EXE, основні структури та поля. Реверс-інжиніринг, основні концепції програмування. Основи мови програмування Assembler, програмування для платформи x64 в середовищі masm64. Алгоритми ін'єкції коду в структуру виконуваного файлу: додавання коду в кінець існуючої секції з та без використання API функцій, створення нової секції.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для ***першого*** (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням методів візуалізації, проблемного й інтерактивного навчання, мотиваційних прийомів**,** інформаційно-комунікаційних технологій); лабораторні заняття (з використанням методів комп'ютерного моделювання, методів проєктної діяльності, тренінгових вправ, аналізу проблемних і наукових ситуацій, пояснення, дискусія тощо); самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, поточного та підсумкового контролю) з використанням інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

Форми оцінювання результатів навчання: оцінювання контрольної роботи та лабораторних робіт; тестування.

Вид семестрового контролю: залік

Навчальні ресурси:

1. Botwright R. Malware Analysis: Digital Forensics, Cybersecurity, And Incident Response. – Pastor Publishing Ltd, 2023. – 302 p.
2. Adams M. C. K. Computer Virus and Malware Bible: A Comprehensive and Simplified A-Z Guide for Beginners and Seniors. – Independently Published, 2024. – 224 p.
3. Khawaja G. Practical Web Penetration Testing: Secure web applications using Burp Suite, Nmap, Metasploit, and more. – Packt Publishing, 2020. – 294 p
4. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua.
5. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладач: канд. техн. наук, доцент Нічепорук А.О.