РЕВЕРС ІНЖИНІРИНГ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Другий (магістерський)
Мова викладання	Українська
Кількість встановлених кредитів ЄКТС	8,0
Форми навчання, для яких викладається дисципліна	Денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен:
вміти застосовувати методи проведення зворотної розробки програмного забезпечення та апаратних пристроїв; досліджувати програмний код і дані; використовувати програмні засоби, які реалізують основні методи реверс інжинірингу; виявляти шкідливе програмне забезпечення, проводити аналіз шкідливих програм, розуміти технічні аспекти функціонування шкідливих програм; зменшувати негативні наслідки від впливу шкідливого програмного забезпечення; використовувати сучасні технології програмування; виконувати відтворення програмного коду програм, його динамічний і статичний аналіз, пошук і експлуатацію вразливостей, аналіз шкідливого програмного коду; проводити дослідження, обробляти та аналізувати отримані експериментальні дані.
володіти основними фундаментальними поняттями і методами реверс інжинірингу для їх використання в сучасних умовах; навичками збору і аналізу інформації; принципами побудови і алгоритмічними структурами сучасного програмного забезпечення; основним математичним апаратом та законами декомпіляції програмного забезпечення.

Зміст навчальної дисципліни. Основи реверс інжинірингу, низькорівневе програмування (асемблер), дизасеблерування, розпізнавання конструкцій мов високого програмування в асемблері, захищений режим процесора, внутрішній устрій операційної системи, WinApi функції, Native додатки, програмування служб; відтворення програмного коду програм, динамічний і статичний аналіз коду, shell коди, Metasploit, пошук і експлуатація вразливостей, аналіз шкідливого програмного коду.

Запланована навчальна діяльність: кількість аудиторних годин - не менше 1/3 від загальної кількості годин, які заплановані для вивчення дисципліни.

Форми (методи) навчання: лекції (з використанням методів проблемного навчання і візуалізації); лабораторні роботи (з використанням методів комп'ютерного моделювання, тренінгів, майстер-класів), самостійна робота (індивідуальні завдання), наочні методи, робота в групі, використання сучасних інформаційних технологій та прикладного програмного забезпечення.

Форми оцінювання результатів навчання: усне опитування, тестування, захист лабораторних робіт; письмове опитування (тестування).

Вид семестрового контролю: залік.

Навчальні ресурси:

1. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник / В. М. Джулій, Ю. П. Кльоц, І. В. Муляр, В. М. Чешун. – Хмельницький: ХмНУ, 2020. – 196 с.
2. Інформаційна безпека : навчальний посібник / Ю. Я. Бобало та інші ; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
3. Тарнавський, Ю. А. Технології захисту інформації: підручник / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.
4. Цифрова криміналістика: консп. лекцій / уклад. І. З. Якименко. - Тернопіль : ТНЕУ, 2019. - 109 с.
5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua.
6. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Викладач: канд. техн. наук, доцент Чешун В.М.