ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ

Тип дисципліни	Вибіркова
Рівень вищої освіти	Перший (бакалаврський)
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 знати: основні джерела вторгнень в комп'ютерні системи та мережі, основні методи та технології протидії вторгнень; основні методи та засоби налаштування захищених операційних систем; основні вразливості операційних систем; класифікацію систем виявлення атак;
вміти: підбирати, налагоджувати та використовувати сучасні технології для виявлення вторгнень у комп'ютерні системи та мережі, оцінювати імовірність вторгнення та вживати заходи для протидії.

Зміст навчальної дисципліни. Введення в задачі і технології виявлення вразливостей інформаційних систем (ІС). Класифікація технологій тестування вразливостей ІС. Ручне та автоматичне тестування вразливостей. Канали доступу, цілі тестування вразливостей, критерії вибору технологій. Організація тестування вразливостей на замовлення. П'ять фаз тестування вразливостей на проникнення. Модулі процедур тестування. Тестування на виявлення вразливостей – практичний аспект. Реалізація тестування на виявлення вразливостей. Аналіз результатів тестування. Технології сканування. Сканування портів. Сканери вразливостей як інструмент інформаціної безпеки. Сканування вразливостей як процес інформаціної безпеки. Тестування вразливостей зовнішньої і внутрішньої інфраструктури. Тестування хмарого простору, технологій віртуалізації, бездротового захисту. Збір інформації та написання звітів як супутні складові в задачах виявлення вразливостей.

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, самостійна робота (опрацювання лекційного матеріалу, підготовка до лабораторних робіт, індивідуальні завдання).

Форми оцінювання результатів навчання: усне опитування; письмове опитування (контрольна робота); захист лабораторних робіт.

Вид семестрового контролю: залік.

Навчальні ресурси:
1. Sinha Sanjib Beginning Ethical Hacking with Kali Linux: Computational Techniques for Resolving Security Issues. / Sanjib Sinha . Howrah, West Bengal, India : Apress Media LLC, 2018. 426 p.
2. Методи та засоби технічного аудиту інформаційної безпеки комп'ютерних систем та мереж. Практикум/ О. І. Алєнін, А. В. Габінет, О. П. Роковий, С. Г. Стіренко, О. О. Ілляшенко, А. А. Стрєлкіна: под ред. В.С. Харченко – Министерство освіти та науки України, Національний аэрокосмічний університет ім. М .Є. Жуковського «ХАІ». 2017. 136 с.
3. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khnu.km.ua
4. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php

Викладач: канд. техн. наук, доцент Тітова В.Ю.