Анотація до навчальної дисципліни

БЕЗПЕКА ІНТЕРНЕТУ РЕЧЕЙ

Метою викладання дисципліни «Безпека Інтернету речей» є навчити студентів навичкам етичних хакерів виконувати вразливість та оцінку ризиків, а також досліджувати та рекомендувати стратегії зменшення ризику для поширених загроз безпеці в системах IoT

Завданням дисципліни є розвиток основоположних навичок для розробки рішень з IoT з інтегрованими засобами безпеки, підготовка спеціалістів здатних оцінити ризики безпеки для рішень IoT, змоделювати вплив загроз, оцінити вразливість систем та запропонувати рішення для нейтралізації або пом'якшення наслідків атак на IoT системи. За рахунок практичної лабораторної діяльності стимулювати студентів до застосування творчого підходу до вирішення проблем та швидкого прототипування в міждисциплінарній галузі електроніки, мереж, безпеки, аналітики даних та бізнесу.

Вивчення курсу передбачає теоретичну підготовку і практичне вивчення матеріалу з використанням персональних комп'ютерів, активного мережного обладнання фірми Cisco, мікроконтролерів Arduino, мікрокомп'ютерів Raspberry Pi та утиліт, які використовуються зловмисниками наприклад, Kali Linux, для виявлення та демонстрації вразливостей в системах IoT. Як складова процесу можелювання загроз, будуть розроблені заходи їх нейтралізації.

Курс завершиться командною навчальної грою, в якій студентам для подолання місій знадобляться отримані під час вивчення дисципліни знання та навички.

При розробці курсу використовувалися матеріали мережної академії Cisco, а саме курсів лінійки IoT Fundamentals: "Connecting Things", "IoT Security".

За умови успішного вивчення курсу студенти додатково отримають сертифікати про успішне завершення курсів Академії Cisco "IoT Security".

В результаті вивчення навчальної дисципліни студент повинен
знати:

- як IoT можна використовувати для рішень у галузі охорони здоров'я, енергетики, розумного міста та виробництва;
- важливість розробки IoT-рішень, які мають інтегрований захист пристроїв, програмного забезпечення та даних;
- ризики безпеки IoT в індустрії;
- ввикористання схеми моделювання загроз та управління ризиками, щоб рекомендувати заходи щодо зменшення загрози;
- • вплив нових технологій на безпеку IoT.

вміти:

- збирати схеми та програмувати поведінку Arduino з різноманітними сенсорами та виконавчими механізмами;
- розробляти програми на на Python для Raspberry Pi, які забезпечують функціонал IoT;
- застосовувати мультидисциплінарні навички підключення речей, безпеки IoT та аналітики для виявлення та вирішення реальної проблеми;
- використовувати стандартні моделі для пояснення вимог безпеки в системах IoT;
- виконувати моделювання загроз для оцінки вразливості фізичних пристроїв безпеки в системах IoT;
- •ввиконувати моделювання загроз для оцінки вразливості безпеки зв'язку в системах IoT;
- •ввиконувати моделювання загроз для оцінки вразливості безпеки додатків у системах IoT;

Структура навчальної дисципліни "Безпека Інтернету речей"

Тема 1. IoT – як виклик безпеці інформаційних систем та мереж.

Тема 2. IoT системи та архітектури.

Тема 3. Сенсори та актуатори, їх взаємодія з мікроконтролером. Програмування рішень на основі мікроконтролера.

Тема 4. Програмування Raspberry Pi.

Тема 5. Туманні обчислення та хмарні обчислення в IoT.

Тема 6. Наскрізний процес проектування та прототипування IoT рішення.

Тема 7. Ризики безпеки IoT в промисловості.

Тема 8. Поверхня атак на IoT Device Layer.

Тема 9. Поверхня атак на IoT Communication Layer.

Тема 10. Поверхня атак на IoT Application Layer.

Тема 11. Вразливості та оцінка ризиків в IoT системах.

Тема 12. IoT Security навчальна гра