Силабус курсу
БЕЗПЕКА ІНТЕРНЕТ – РЕЧЕЙ

Ступінь вищої освіти – магістр
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Наталія Яцків
Контактна інформація	jng@wunu.edu.ua

Опис дисципліни

Анотація до курсу. З мільярдами пристроїв підключених до Інтернету, потенціал Інтернету речей (IoT) великий і постійно зростає. Однак із цим потенціалом постає не менш важлива проблема захисту цих пристроїв і мереж, до яких вони підключаються.

Кожен пристрій IoT є потенційною точкою входу для суб'єктів загроз. Поспішаючи отримати ринкові можливості IoT, компанії продають вразливі пристрої тисячами. З цими проблемами безпеки з'являються можливості для таких студентів, як ви, отримати навички, які підготують вас до кар'єри у сфері захисту Інтернету речей і критичної інфраструктури Інтернету речей.

Пристрої відкривання гаражних дверей з підключенням до Інтернету забезпечують зручність і спокій, оскільки власники будинків можуть контролювати двері гаража та перевіряти, чи відкриті чи закриті двері з будь-якого місця. Розумні розетки можна використовувати для керування електроприладами, навіть коли власник будинку десь у відпустці. Камери безпеки IoT безперервно контролюють будинки та підприємства. Однак суб'єкти загрози можуть контролювати двері гаража та дозволяти крадіжки з дому. Приладами можна керувати неналежним чином, що спричиняє пошкодження або знищення приладів чи будинку. Конфіденційність може бути порушена хакерами, які отримують доступ до камер відеоспостереження, щоб побачити наше приватне життя.

Настав час подумати про своє місце експерта з кібербезпеки в IoT. Цей курс допоможе вам почати подорож.

Метою курсу «Безпека Інтернет - речей» є - отримання знань та умінь, які необхідні для розробки та дослідження безпеки Інтернет речей.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Концепції гарантоздатності та безпеки для IoT	Пояснювати концепцію безпеки IoT	Поточне опитування
2/0	Моделі гарантоздатності та надійності IoT	Застосовувати заходи щодо надійності та безпеки IoT	Поточне опитування
2/1	Моделі безпеки для IoT	Здійснювати моделювання загроз та атак для систем IoT	Поточне опитування
2/1	Вимоги управління безпекою до IoT	Розробляти план управління безпекою та безпекою	Поточне опитування
2/1	Життєвий цикл безпеки та безпеки для IoT	Розуміти життєвий цикл безпеки для IoT	Поточне опитування

2/1	Огляд, аналіз та методи тестування IoT	Проводити тестування безпеки пристроїв IoT	Поточне опитування, тестування
2/1	Забезпечення Case основи	Застосовувати концепцію Case	Поточне опитування
2/1	Прийоми та заходи безпеки для IoT	Застосовувати заходи безпеки для IoT	Поточне опитування
2/2	Інформація про безпеку та інформування про енергетичну ефективність	Використовувати інструменти для розробки енерго ефективних систем	Поточне опитування
2/1	Основи технології blockchain та приклади застосування	Розуміти технологію блокчейн та її застосування	Поточне опитування
2/2	Алгоритми консенсусу в технології Blockchain	Використовувати алгоритми консенсусу при проектуванні децентралізованих систем	Поточне опитування
2/1	Технологія Blockchain для безпеки IoT	Застосовувати технологію блокчейн для безпеки IoT	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 1. Основи і технології / За ред. В. С. Харченка. - Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. -547 с.
2. Курс мережевої академії Cisco: Безпека Інтернет-речей. 2020 р: https://www.netacad.com/courses/cybersecurity/iot-security
3. Sklyar V.V., Yatskiv V.V., Yatskiv N.G. Dependability and Security of IoT: 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.
4. . Alajlan, R., Alhumam, N., & Frikha, M. (2023). Cybersecurity for blockchain-based IoT systems: a review. *Applied Sciences*, *13*(13), 7432. https://doi.org/10.3390/app13137432
5. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An Overview on Edge Computing Research. *IEEE Access* 2020, *8*, 85714–85728. [CrossRef]
6. Ajayi, O.J., Rafferty, J.; Santos, J., Garcia-Constantino, M., Cui, Z. BECA: A Blockchain-Based Edge Computing Architecture for Internet of Things Systems. *IoT*, 2021, *2*,610–632. https://doi.org/10.3390/ iot2040031
7. Kandhro, I. A., Alanazi, S. M., Ali, F., Kehar, A., Fatima, K., Uddin, M., & Karuppayah, S. (2023). Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures. *IEEE Access*, *11*, 9136-9148. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10023499
8. Sklyar V., Kharchenko V. Green Assurance Case: Applications for Internet of Things. Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control, vol 171. Springer, Cham, 2019.
9. Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. *Internet of Things*, *22*, 100759
1. 10. Taherdoost, H. (2023). Security and internet of things: benefits, challenges, and future perspectives. *Electronics*, *12*(8), 1901.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20 %	20 %	5 %	15 %	40 %
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 1-6.	Підсумкова письмова робота за темами №1-12.	Визначається як середнє арифметичне з оцінок за виконання трьох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання наскрізного завдання.	1. 15тестів по 4 бали - max 60 балів. 2.Практич-не завдання - max 40 балів

Шкала оцінювання:

ECTS	**Бали**	**Зміст**
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом