| | |
|---|---|
| **Назва курсу** | **«Безпека та конфіденційність Інтернет-речей»** |
| **Викладач (-і)** | Яцків Наталія Георгіївна |
| **Профайл викладача (-ів)** | https://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/ |
| **Контактний тел.** | +380352-475050 ext. 56501 |
| **E-mail:** | n.yatskiv(@)wunu.edu.ua |
| **Сторінка курсу в moodle** | https://moodle.wunu.edu.ua |
| **Консультації** | Очні консультації: вівторок: 14-00, ауд. 6501.Онлайн-консультації (zoom): вівторок з 15 -00 до 16-00. |

**1. Анотація до курсу.**

Даний курс розширює кругозір аспірантів в області передових підходів та методів захисту пристроїв Інтернету речей шляхом проведення досліджень, розробки відповідних заходів та їх впровадження.

**2. Пререквізити.**

Раніше вивчені дисципліни необхідні для освоєння курсу: базовий обсяг знань з апаратного комп'ютерного, мережного та програмного забезпечення, систематичних та ґрунтовних знань із суміжних курсів «Методологія та організація наукових досліджень», «Методи оптимізаці», «Математичне моделювання та обчислювальні методи» а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

**Постреквізити.** Матеріал даної дисципліни може бути використаний при написанні дисертаційної роботи.

**3. Мета та цілі курсу.**

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

**Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:**

СК-1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі кібербезпеки.

СК-6. Уміння відслідковувати тенденції й напрямки розвитку інформаційної та кібербезпеки, а також суміжних і прикладних областей.

**Результати навчання:**

В результаті вивчення дисципліни аспірант повинен:

ПРН-2. Знати сучасні методи проведення досліджень в галузі кібербезпеки.

ПРН-7. Вміти досліджувати проблеми кібербезпеки критичної інфраструктури.

ПРН-8. Вміти синтезувати науково обґрунтовані рішення по захисту інформації в комп’ютерних та кіберфізичних системах.

**4 Загальна інформація про дисципліну**

| | |
|---|---|
| **Ступінь вищої освіти** | **доктор філософії** |
| **Спеціальність** | **125 Кібербезпека** |
| **Курс (рік навчання)** | **перший** |
| **Семестр** | **2** |
| **Рік викладання** | **2023/2024** |
| **Формат курсу** | **Очний (offline)** |
| **Нормативна \ вибіркова** | **обов'язкова** |
| **Загальна кількість год/ кредитів** | **120/4** |
| **Лекції, год.** | **20** |
| **Лабораторні, год** | **20** |
| **Самостійна робота, год.** | **80** |

**5. Перелік тем**

1. Виклики безпеки IoT.
2. Системи та архітектури IoT.
3. Поверхня атаки на пристрої IoT.
4. Безпека фізичних пристроїв.
5. Поверхня атаки на комунікації IoT.
6. Атаки на рівні застосування IoT.
7. Оцінка вразливостей в системі IoT.
8. Оцінка ризику IoT.
9. Інновації в безпеці Інтернету речей.
10. Безпека Інтернету речей з використанням блокчейну.

**Рекомендовані джерела**

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. Raimundo, R. J., & Rosário, A. T. (2022). Cybersecurity in the internet of things in industrial management. Applied Sciences, *12*(3), 1598.

3. Курс мережевої академії Cisco, 2020 р: https://www.netacad.com/courses/cybersecurity/iot-security

4. 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.

5. Hanssen G., Stålhane T, Myklebust T. Safe Scrum – Agile Development of Safety-Critical Software. Springler, 2018.

6. NISTIR 8200, Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT). –National Institute of Standards and Technologies, 2018.

7. Inayat, U., Zia, M. F., Mahmood, S., Khalid, H. M., & Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects. Electronics, *11*(9), 1502.

8. Kandasamy, K., Srinivas, S., Achuthan, K., Rangan, V. P.. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*, 1-18.

9. Nunes P., Medeiros I., Fonseca J. at all. Benchmarking Static Analysis Tools for Web Security. IEEE Transactions on Reliability (2018), 67(3): 1159-1175

10. 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.

**Політика оцінювання**

● Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання екзамену відбувається із дозволу проректора з наукової роботи за наявності поважних причин (наприклад, лікарняний).

● Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%.

●Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

**Оцінювання**

Оцінка за курс визначається наступним чином:

| Види оцінювання | % від остаточної оцінки |
|---|---|
| Екзамен | 100 |

Шкала оцінювання аспірантів:

| 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 |