Назва курсу	**«Кібербезпека інформаційних і комп'ютерних систем»**
Викладач (-і)	Яцків Василь Васильович
Профайл викладача (-ів)	http://www.tneu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext.56501
E-mail:	**v.yatskiv(@)tneu.edu.ua**
Сторінка курсу в moodle	https://moodle.tneu.edu.ua
Консультації	Очні консультації: понеділок: 14-00, ауд. 6501. Онлайн- консультації: у viberгрупі курсукожного дня з 14 - 00 до 18-00.

1. Анотація до курсу. Даний курс знайомить із принципами та прийомами пов'язаними із забезпеченням безпеки спеціалізованих комп'ютерних систем та Інтернет- речей. Швидке зростання кількості підключених пристроїв IoT дозволяє оцифровувати світ, але також збільшує вплив загроз безпеці. Ви будете використовувати новітні технології для оцінки вразливості та оцінки ризиків, а потім досліджувати та рекомендувати стратегії зменшення ризику для поширених загроз безпеці в системах IoT. Світ потребує більш кваліфікованих фахівців з кібербезпеки. Додавання IoT безпеки до набору компетентностей відрізнятиме вас від інших кандидатів на роботу.

2. Пререквізити.

Раніше вивчені дисципліни необхідні для освоєння курсу: методологія та організація наукових досліджень, інформаційні технології, математичне моделювання та обчислювальні методи, кібербезпека інформаційних і комп'ютерних систем.

Постреквізити. Дисципліни, які будуть використовувати результати навчання даного курсу: підготовка дисертаційної роботи.

3. Мета та цілі курсу.

Метою курсу " Кібербезпека інформаційних і комп'ютерних систем" є отримання знань та умінь, які необхідні для розробки та дослідження безпеки спеціалізованих комп'ютерних систем.

Результати навчання:

В результаті вивчення дисципліни аспірант повинен:

1. Використовувати основні методи, моделі та алгоритми захисту даних в програмно-апаратних системах спеціалізованих комп'ютерних систем та системах Інтернет-речей. Надавати рекомендації щодо побудови та використання апаратних засобів, протоколів при проектуванні системи Інтернет-речей.
2. Вміти планувати та проводити експерименти, що мають відношення до проблем з галузі знань технологій кібербезпеки спеціалізованих комп'ютерних систем, використовуючи належне програмне забезпечення, та знати, як аналізувати і відображати результати досліджень.
3. Вміти працювати з фахівцями з різних галузей в рамках наукових проектів з технологій кібербезпеки спеціалізованих комп'ютерних систем.
4. Вміти використовувати сучасні математичні методи, інформаційні технології та/або технічні засоби для забезпечення кібербезпеки спеціалізованих комп'ютерних систем.

5. Вміти організовувати проектування, розробляти архітектуру, методи проектування та технології функціонування систем кібербезпеки спеціалізованих комп'ютерних систем.

4 Загальна інформація про дисципліну

Ступінь вищої освіти	**доктор філософії**
Спеціальність	**121 Інженерія програмного забезпечення**
Курс (рік навчання)	**1**
Семестр	**2**
Нормативна \ вибіркова	**вибіркова**
Загальна кількість год/ кредитів	**150/5**
Лекції, год.	**10**
Лабораторні, год	**6**
Самостійна робота, год.	**134**

5. Перелік тем

Тема 1. Виклики безпеки IoT. Незахищені пов'язані речі IoT. Анатомія атаки IoT. Дослідження атаки на IoT. Модель безпеки IoT. Вступ до IoT в галузі охорони здоров'я. Моніторинг охорони здоров'я та IoT. Ризики IoT. Уразливості IoT. IT та IoT у виробничому секторі.

Тема 2. Системи та архітектури IoT. Моделі IoT-систем. Моделі мереж. Моделі OSI і TCP / IP. Контрольна модель IoT. Захищеність у базовій моделі IoT. Стандартизована архітектура ETSI M2M. Протоколи та стандарти IoT. Тріада: цілісність, доступність, конфіденційність. Десять критичних вимог щодо безпеки IoT. Системні вимоги безпеки IoT. Вимоги безпеки IoT до комунікацій. Аналіз моделі загрози для системи IoT.

Тема 3. Поверхня атаки на пристрої IoT. Компоненти апаратного забезпечення пристроїв IoT. Огляд вразливості апаратного забезпечення OWASP. Типи процесорів IoT. Пам'ять. Фізичні порти. Компоненти апаратних пристроїв IoT. Компоненти програмного забезпечення пристроїв IoT. Вбудовані системи. Операційні системи IoT. Компоненти програмного забезпечення пристрою IoT. Фізичні вразливості обмежених пристроїв. Безпека фізичних пристроїв. Вразливості обладнання.

Тема 4. Атаки на системи зв'язку IoT. Вразливості рівня комунікаційного рівня IoT. Функції комунікаційного шару IoT. Вразливості шару зв'язку OWASP. Комунікаційні канали. Функції комунікаційного рівня IoT. Сценарії зв'язку IoT. Огляд протоколу бездротового зв'язку. Bluetooth та Wi-Fi. Огляд IEEE 802.15.4. Ролі пристрою IEEE 802.15.4. Топології IEEE 802.15.4. Безпека IEEE 802.15.4. Mesh-протоколи, які використовує 802.15.4. Бездротові протоколи. Вразливості шару зв'язку IoT. Захист протоколів зв'язку IoT. Ізоляція IoT трафіку.

Тема 5. Поверхня атаки на застосування IoT. Поверхня атаки шару програми IoT. Вразливості програми OWASP. Локальні програми. Мобільні додатки. Вразливості веб-та хмарних додатків OWASP. Вразливості пароля. Вразливості веб-інтерфейсу. Моделювання загрози на рівні програми. Протоколи обміну повідомленнями IoT. Протокол MQTT.

Тема 6. Оцінка вразливості та оцінка ризику в системах IoT. Процес оцінки вразливості. Види оцінки вразливості. Тестування на проникнення. Інструменти вразливості пароля. Інструменти вразливості веб-додатків. Послуги з оцінки вразливості. Джерела

інформації про вразливість. Оцінка ризику IoT. Загальна система оцінювання вразливості. Групи метрик CVSS. Базова метрична група CVSS. Процес CVSS. Стратегії управління ризиками. Рекомендуємо пом'якшення наслідків. Реакція на ризик. IoT та Blockchain. Поточні довірчі системи. Система довіри блокчейн. Особливості блокчейна. Цифровий підпис. Децентралізована книга. Досягнення консенсусу. Блокчейн, застосований до IoT Security.

6. 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. 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.

3. Hanssen G., Stålhane T, Myklebust T. SafeScrum® – Agile Development of Safety-Critical Software. Springler, 2018.

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

5. NIST SP 1500-201, Framework for Cyber-Physical Systems. National Institute of Standards and Technologies, 2017.

6. Martins B., Laranjeiro N., Vieira M. INTENSE: INteroperability TEstiNg as a Service // Proceedings of 2017 IEEE International Conference on Web Services (ICWS 2017).

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

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.

7. Система оцінювання та вимоги.

Підсумковий бал (за 100-бальною шкалою) з дисципліни **"Кібербезпека спеціалізованих комп'ютерних систем"** визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту.

Будь-яке завдання, за яке студент отримав оцінку, яка його не задовольняє, може бути повторно перездано протягом наступних двох тижнів.

Незадовільну оцінку за заліковий модуль студент може перездати до здачі наступного модуля.

Шкала оцінювання:

За шкалою ТНЕУ	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

8. Навчальні ресурси

№	Найменування	Номер теми
1.	Мультимедійний проектор	1 - 6

2.	Комп’ютерна лабораторія. Доступ до Інтернету.	1 - 6

9. Політики курсу.

Академічна доброчесність.**Дотримання академічної доброчесності аспірантами передбачає**:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

- дотримання норм законодавства про авторське право і суміжні права;

- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);

- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування: Відвідування занять є обов’язковим. За об’єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.