МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

Декан ФКІТ
Ігор ЯКИМЕНКО

«30» 09 2024 р.

ЗАТВЕРДЖУЮ

Проректор з науково-
педагогічної роботи
Віктор ОСТРОВЕРХОВ

«30» 09 2024 р.

ЗАТВЕРДЖУЮ:
Директор ННІНОТ
Святослав ПИТЕЛЬ

04 10 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Безпека Інтернет – речей»
ступінь вищої освіти – магістр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра спеціалізованих комп'ютерних систем

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (семін.) (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)
Денна	1	2	30	14	4	6	96	150	2
Заочна	1	2	8	4	-	-	138	150	3

Тернопіль – 2024

Робочу програму склала доцент кафедри спеціалізованих комп'ютерних систем, к.т.н., доцент Наталія ЯЦКІВ

Робоча програма затверджена на засіданні кафедри спеціалізованих комп'ютерних систем, протокол
№ 3 від 04. 10. 2024 р.

Завідувач кафедри
спеціалізованих комп'ютерних систем _____ Андрій СЕГІН

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол № 2 від 16. 10. 2024 р.

Голова групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Василь ЯЦКІВ

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Опис дисципліни “Безпека Інтернет - речей”

Дисципліна “Безпека Інтернет - речей”	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів ECTS – 5	Галузь знань – 12 Інформаційні технології	**Статус дисципліни** Вибіркова **Мова навчання** українська
Кількість залікових модулів – 4	Спеціальність – 125 Кібербезпека та захист інформації	Рік підготовки: *Денна – 1* *Заочна -1* Семестр: *Денна – 2* Заочна -2,3
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції (год.): *Денна – 30* *Заочна - 8* Практичні заняття (год.): *Денна – 14* *Заочна - 4*
Загальна кількість годин – 150		Самостійна робота (год.): *Денна – 96* *Тренінг 6 год.* *Заочна – 138* Індивідуальна робота (год.): *Денна – 4*
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Безпека Інтернет - речей»

2.1. Мета вивчення дисципліни.

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

2.2. Завдання вивчення дисципліни

Основне завдання дисципліни дати студентам теоретичну та практичну підготовку з безпеки Інтернет речей.

2.3 В результаті вивчення дисципліни студент повинен знати:

− моделі безпеки для IoT;
− життєвий цикл безпеки для IoT;
− вимоги управління безпекою до IoT;
− принцип технології blockchain;
− алгоритми консенсусу в технології Blockchain.

2.4 В результаті вивчення дисципліни студент повинен уміти:

− використовувати основні методи, моделі та алгоритми захисту даних в програмно-апаратних системах Інтернет-речей;
− надавати рекомендації щодо побудови та використання апаратних засобів, протоколів, каналів зв'язку при проектуванні системи Інтернет-речей.

3. Програма навчальної дисципліни: «Безпека Інтернет - речей»

Змістовий модуль 1. Концепції та моделі IoT

Тема 1. Концепції гарантоздатності та безпеки для IoT.
1. Таксономія вимог надійності та безпеки.
2. Гарантоздатність, надійність та безпека визначає таксономію.
3. Основи аналізу ризиків.
Література: 1, 2, 4.

Тема 2.Моделі гарантоздатності та надійності IoT.
1. Довідкові архітектури Індустріальних IoT.
2. Заходи щодо надійності та безпеки.
3. Режим відмов, аналіз ефектів та критичності (FMECA) систем IoT.
Література: 1, 2, 3.

Тема 3. Моделі безпеки для IoT.
1. Архітектури систем IoT з точки зору безпеки.
2. Заходи безпеки.
3. Моделювання загроз та атак для систем IoT.
Література: 1, 2, 5.

Тема 4. Вимоги управління безпекою до IoT.
1. План управління безпекою та безпекою.
2. Управління людськими ресурсами.
3. Управління конфігурацією.
4. Підбір та оцінка інструментів.
5. Управління документацією.
6. Оцінка безпеки та безпеки.
Література: 1, 2, 10.

Тема 5. Життєвий цикл безпеки та безпеки для IoT.
1. Загальний життєвий цикл.
2. Життєвий цикл безпеки та безпеки: дизайнерський обід зверху вниз.
3. Життєвий цикл безпеки та безпеки: інтеграція вгорі.
4. Відстеження вимог.
Література: 1, 2, 6.

Тема 6. Огляд, аналіз та методи тестування IoT.
1. Огляд документів.
2. Статичний аналіз коду.
3. Функціональне тестування.
4. Структурне тестування коду.
Література: 1, 4, 9.

Змістовий модуль 2. **Прийоми та заходи безпеки для IoT.**
Тема 7. Забезпечення Case основи.
1. Концепція та історія Case основи.
2. Стандарти щодо забезпечення Case.
Література: 1, 2, 9, 10.

Тема 8. Прийоми та заходи безпеки для IoT.
1. Позначення претензій, аргументів та доказів (CAE).
2. Оновлення та застосування записів про претензії, аргументи та докази (CAE)
3. Позначення про структурування цілей (GSN).
Література: 1, 2, 4.

Тема 9. Інформація про безпеку та інформування про енергетичну ефективність
1. Інструменти для розробки випадку впевненості.
2. Структура випадку впевненості для систем IoT.
Література: 1, 2, 7.

Тема 10. Основи технології blockchain та приклади застосування
1 Принцип технології blockchain
2 Структура блоку та дерево Меркле
3 Криптографія в блокчейні
Література: 1, 2, 10.

Тема 11. Алгоритми консенсусу в технології Blockchain
1 Алгоритм підтвердження роботи
2 Доведення алгоритмів консенсусу
3 Технологія Blockchain для безпеки IoT
Література: 1, 2, 5

Тема 12. Технологія Blockchain для безпеки IoT
1 Blockchain та IoT
2 Переваги інтеграції Blockchain з IoT
3 Основні проблеми Blockchain в IoT
4 Рішення безпеки IoT на основі Blockchain
Література: 1, 2, 8.

4.1 Структура залікового кредиту з дисципліни «Безпека Інтернет – речей» (денна форма навчання)

	Кількість годин					
	Лекції	Практичні заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Концепції та моделі IoT						
Тема 1. Концепції гарантоздатності та безпеки для IoT.	2		6	2	3	Поточне опитування
Тема 2. Моделі гарантоздатності та надійності IoT	2	-	8			
Тема 3. Моделі безпеки для IoT.	2	2	8			
Тема 4. Вимоги управління безпекою до IoT.	2	2	8			
Тема 5. Життєвий цикл безпеки та безпеки для IoT.	2	2	8			
Тема 6. Огляд, аналіз та методи тестування IoT.	2	2	8			
Змістовий модуль 2 Прийоми та заходи безпеки для IoT						
Тема 7. Забезпечення Case основи	4	2	8	2	3	Поточне опитування
Тема 8. Прийоми та заходи безпеки для IoT	4	2	8			
Тема 9. Інформація про безпеку та інформування про енергетичну ефективність	2	2	8			
Тема 10. Основи технології blockchain та приклади застосування	2	-	8			
Тема 11. Алгоритми консенсусу в технології Blockchain	4	-	10			
Тема 12. Технологія Blockchain для безпеки IoT	2	-	8			
Разом	**30**	**14**	**96**	**4**	**6**	

4.2 Структура залікового кредиту з дисципліни «Безпека Інтернет – речей» (заочна форма навчання)

	Кількість годин		
	Лекції	Практичні заняття	Самостійна робота
Змістовий модуль 1. Концепції та моделі IoT			
Тема 1. Концепції гарантоздатності та безпеки для IoT.	2	2	8
Тема 2. Моделі гарантоздатності та надійності IoT			10
Тема 3. Моделі безпеки для IoT.			12
Тема 4. Вимоги управління безпекою до IoT.	2		12
Тема 5. Життєвий цикл безпеки та безпеки для IoT.			12
Тема 6. Огляд, аналіз та методи тестування IoT.			12
Змістовий модуль 2 Прийоми та заходи безпеки для IoT			
Тема 7. Забезпечення Case основи	2	2	12
Тема 8. Прийоми та заходи безпеки для IoT			12
Тема 9. Інформація про безпеку та інформування про енергетичну ефективність			12
Тема 10. Основи технології blockchain та приклади застосування	2		12
Тема 11. Алгоритми консенсусу в технології Blockchain			12
Тема 12. Технологія Blockchain для безпеки IoT			12

Разом	**8**	**4**	**138**

5. Тематика практичних (семінарських або лабораторних) занять

Лабораторна робота №1

Тема: Оцінювання показників безпеки.

Мета: вивчення та дослідження показників надійності систем IOT.

Питання для обговорення:

1. Самодіагностика
2. Показники надійності
3. Аналіз режиму відмов, аналіз ефекту та критичності

Література: 1, 2

Лабораторна робота №2

Тема: Аналіз сценаріїв атак на IoT системи

Мета: Вивчення та дослідження можливих сценаріїв атак IOT

Питання для обговорення:

1. Загрози системи IoT
2. Вбивчий ланцюг
3. Моделювання атак

Література: 1, 2.

Лабораторна робота №3

Тема: Розробка плану управління функціональною та інформаційною безпекою IoT систем.

Мета: Вивчення та дослідження структури та змісту плану управління надійністю та безпекою для системи IoT.

Питання для обговорення:

1. План управління безпекою та безпекою.
2. Управління людськими ресурсами.
3. Управління конфігурацією.
4. Підбір та оцінка інструментів.
5. Управління документацією.

Література: 1, 2.

Лабораторна робота №4

Тема:. **Розробка життєвого циклу функціональної та інформаційної безпеки IoT систем**

Мета: вивчення та дослідження структури життєвого циклу надійності та безпеки (SSLC).

Питання для обговорення:

1. Життєвий цикл надійності та безпеки
2. Відстеження вимог
3. Основні завдання відстеження вимог.

Література: 1, 2.

Лабораторна робота №5

Тема: Програмні засоби для розробки Case

Мета: Вивчення та дослідження структури та змісту Служби достовірності систем IoT.

Питання для обговорення:

1. Концепція забезпечення Case
2. Структурування цілей (GSN)
3. Програмний інструмент Astah GSN

Література: 1, 2

Лабораторна робота №6

Тема: Методи та засоби забезпечення функціональної та інформаційної безпеки IoT систем

Мета: Вивчення та дослідження технічних засобів та заходів безпеки для систем IoT.

Питання для обговорення:

1. Методи та заходи безпеки організації, що застосовуються для систем IoT
2. Технічні методи безпеки та заходи безпеки, що застосовуються для систем IoT
3. Спеціальні методи та заходи щодо запобігання кібератакам

Література: 1, 2.

6. Самостійна робота

Для самостійної роботи кожному студенту пропонується виконання наскрізного проєкту **«Виконання тесту на проникнення для Інтернет - речей»**, який складається із п'яти завдань**:**

1. Збір інформації та пошук цілей.
2. Пошук вразливостей.
3. Експлуатація та проведення атак.
4. Розширення зони впливу і ескалація привілеїв.
5. Написання звіту.

7. Організація та проведення тренінгу з дисципліни «Безпека Інтернет - речей»

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Налаштування інфраструктури MQTT для публікації/підписки	1. Налаштування топології. 2. Запустіть локальний сервер-посередник 3. Підпишіться на тему та опублікуйте повідомлення MQTT
2	Аналіз даних за допомогою Kali	1. Атака MITM за допомогою Kali на TCP 2. Перегляньте запис за допомогою Wireshark 3. Опублікуйте фальшиві дані
3	Додавання захисту TLS	1. Додайте рівень TLS для транспортування даних 2. Атака MITM за допомогою Kali 3. Перегляньте зашифровані дані за допомогою Wireshark

8. Методи навчання.

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; лабораторні роботи, індивідуальні заняття; самостійна робота студентів, робота в Інтернет.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «**Безпека Інтернет – речей**» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

– поточне опитування;

– підсумковий модульний контроль за кожним змістовним модулем;

– оцінювання виконання лабораторних робіт;

– оцінювання тренінгів;

– оцінювання результатів самостійної роботи.

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни "**Безпека Інтернет - речей**" визначається як середньозваженам величина, залежно від питомої ваги кожної складової залікового кредиту:

Для екзамену

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:

За шкалою ЗУНУ	**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)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 12
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 12
3.	Одноплатні комп'ютери Raspberry Pi	2 - 12

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

10. Taherdoost, H. (2023). Security and internet of things: benefits, challenges, and future perspectives. *Electronics*, *12*(8), 1901.