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

ЗАТВЕРДЖУЮ

Декан факультету комп'ютерних інформаційних технологій
Ігор ЯКИМЕНКО
«__» _____ 2025 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ
«__» _____ 2025 р.

ЗАТВЕРДЖУЮ:
Директор Навчально-наукового інституту новітніх освітніх технологій
Святослав ПИТЕЛЬ
_____ 2025 р.

РОБОЧА ПРОГРАМА

з дисципліни «Безпека Інтернет – речей»
ступінь вищої освіти – магістр
галузь знань – F Інформаційні технології
спеціальність – F5 Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кафедра спеціалізованих комп'ютерних систем

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	Інд. роб. (год.)	Тренінг (год.)	Самост. робота (год.)	Разом (год.)	Залік/ екзамен. (семестр)
Денна	1	2	32	14	5	6	93	150	Екзамен (2)
Заочна	1	2	8	4	-	-	138	150	Екзамен (2)

Тернопіль – 2025

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
№ 7 від 25.05.25 р.

Завідувач кафедри
спеціалізованих комп'ютерних систем _____ Андрій СЕГІН

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 – F Інформаційні технології	**Статус дисципліни** Вибіркова **Мова навчання** українська
Кількість залікових модулів – 4	Спеціальність – F5 Кібербезпека та захист інформації	Рік підготовки: *Денна – 1* *Заочна -1* Семестр: *Денна – 2* Заочна -2
Кількість змістових модулів – 2	Ступінь вищої освіти – магістр	Лекції (год.): *Денна – 32* *Заочна - 8* Лабораторні роботи (год.): *Денна – 14* *Заочна - 4*
Загальна кількість годин – 150		Самостійна робота (год.): *Денна – 93* *Тренінг 6 год.* *Заочна – 138* Індивідуальна робота (год.): *Денна – 5*
Тижневих годин – 10, з них аудиторних – 3		Вид підсумкового контролю – екзамен

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

2.1. Мета вивчення дисципліни.

Сформувати у здобувачів системне розуміння загроз і механізмів захисту екосистем Інтернету речей на всіх рівнях – від архітектури та протоколів до прошивки, хмарних платформ і OT/IIoT – та навчити застосовувати перевірені практики безпеки з урахуванням реальних інцидентів і сучасних трендів (AI/5G/Edge).

2.2. Завдання вивчення дисципліни:

- проаналізувати типові вразливості IoT-пристроїв і причини їх виникнення; навчитися оцінювати ризики;
- засвоїти криптографічні механізми для IoT (хеші/HMAC, підписи) та принципи коректної імплементації;
- вивчити автентифікацію/авторизацію та типові помилки, що ведуть до компрометації;
- забезпечити апаратну/фізичну безпеку, захист ключів, контроль цілісності, безпеку ланцюга постачання;
- забезпечити захист даних і приватність: шифрування в дорозі/на носіях, OSCORE, управління ключами;
- забезпечити безпеку хмарних/мобільних IoT-платформ та їхніх API;
- опанувати сучасні протоколи/моделі доступу (EAP, DTLS, EDHOC, RBAC/ABAC) та тренди (5G/MEC/AI).

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

– здатність розуміти роль CIA-моделі, активів і векторів атак у багатошарових системах;

– здатність ідентифікувати типові уразливості пристроїв і визначати пріоритети ризиків;

– здатність застосовувати хеші/HMAC/підписи й уникати помилок імплементації;

– здатність обирати адекватні схеми/фреймворки з урахуванням IoT-обмежень;

– здатність аналізувати відомі атаки/ботнети для підвищення стійкості систем;

– здатність застосовувати профільні стандарти й вимоги для промислових середовищ.

2.4 Результати навчання:

– пояснювати архітектуру IoT, модель CIA та типові загрози/вектори атак;

– аналізувати поширені уразливості IoT-пристроїв і визначати причини їхньої появи;

– описувати криптомеханізми, їхні сильні/слабкі сторони та вимоги до впровадження;

– впроваджувати та використовувати методи автентифікації/авторизації та виявляти типові помилки;

– досліджувати безпеку протоколів, моделі шифрування трафіку та типові уразливості.

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

Змістовий модуль 1. Загрози Інтернет - речей

Тема 1. Вступ до IoT і основи безпеки

IoT- архітектура. Сфери застосування IoT. Модель CIA у контексті IoT. Приклади атак та інцидентів IoT. Стандарти та фреймворки безпеки IoT

Тема 2. Уразливості та загрози IoT

Типові вразливості IoT-пристроїв. Реальні приклади атак на IoT. Стандарти та рекомендації з безпеки для IoT. Чому IoT-пристрої особливо вразливі.

Тема 3. Основи криптографії для IoT

Застосування хеш-функцій і HMAC. Цифрові підписи. Типові помилки реалізації. Принципи правильного впровадження.

Тема 4. Аутентифікація та авторизація

Основні методи аутентифікації IoT. Протоколи і фреймворки. Особливості аутентифікації в IoT. Типові помилки в аутентифікації/авторизації IoT. Приклади атак через неналежну аутентифікацію/авторизацію.

Тема 5. Безпечні протоколи IoT

Основні IoT-протоколи. Механізми безпеки протоколів. Безпечна передача даних. Типові уразливості.

Тема 6. Оновлення ПЗ та безпечне завантаження

OTA-оновлення. Безпечне завантаження. Типові вразливості OTA і Secure Boot.

Змістовий модуль 2. Апаратна безпека IoT.

Тема 7. Мережева безпека та сегментація в IoT

Основні типи фаєрволів. IDS/IPS. Сегментація мереж. VPN, Zero Trust.

Тема 8. Захист кінцевих пристроїв і апаратна безпека IoT

Атаки через побічні канали: деталі та контрзаходи. Інвазивне втручання: види та захист. Неінвазивне зондування: небезпека тестових інтерфейсів. Додаткові заходи фізичної безпеки. Пов'язані концепції: Secure Boot та Root of Trust. Захист від атак через побічні канали. Захищений завантажувач та Root of Trust. Захист ключів та криптографічні модулі. Контроль цілісності та виявлення змін в IoT. Управління ланцюгом постачання.

Тема 9. Аналіз прошивки та реверс-інжиніринг IoT-пристроїв.

Типові формати прошивок. Методи добування прошивки. Статичний аналіз прошивки. Динамічний аналіз. Виявлення вразливостей. Методи ускладнення реверсу. Інструменти автоматизації аналізу.

Тема 10. Захист даних та приватність

Шифрування даних при передачі. Об'єктне шифрування для CoAP: OSCORE. Шифрування даних при зберіганні. Політика мінімізації даних. Управління ключами. Апаратні «корені довіри». Політики та ієрархії ключів. Мінімальні технічні вимоги до IoT-пристрою.

Тема 11. Хмарні та мобільні IoT-платформи

Популярні хмарні IoT-платформи. Архітектура хмарної IoT-системи. Безпека й ідентичність. Безпека API. Автентифікація та контроль доступу. Кібербезпека хмарних сервісів.

Тема 12. Реальні атаки та інциденти

Ботнет Mirai. VPNFilter: складний багатоступеневий ботнет. BrickerBot: постійне виведення пристроїв з ладу. Статистика та інші інциденти

Тема 13. Промисловий IoT та OT-безпека

Стандарти IIoT. Захищені інтерфейси. Перевірена криптографія. Безпека за замовчуванням. Підписані оновлення програмного забезпечення. Автоматичні оновлення.

Тема 14. Дослідження та розробки в області IoT

Автентифікація та контроль доступу. Протоколи автентифікації для IoT: EAP, DTLS, EDHOC. Моделі контролю доступу (DAC, MAC, RBAC, ABAC) для IoT. Управління ідентичностями. Виклики захисту даних. Метод автентифікації на основі криптографії з відкритим ключем.

Тема 15. Майбутнє безпеки IoT та нові виклики

Контекст та тренди. Як 5G та MEC впливають на модель загроз IoT. Як AI змінює загрози для IoT. Регуляторні та стандартні «маяки» на 2025–2027. Патерни захисту для AIoT + 5G.

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

	Кількість годин					
	Лекції	Лабораторні роботи	Інд. роб.	Тре-нінг	Сам. роб.	Контрольні заходи
Змістовий модуль 1. Загрози Інтернет - речей						
Тема 1. Вступ до IoT і основи безпеки	2		2	3	6	Поточне опитування
Тема 2. Уразливості та загрози IoT	2	-			6	
Тема 3. Основи криптографії для IoT	2	2			6	
Тема 4. Аутентифікація та авторизація	2	2			6	
Тема 5. Безпечні протоколи IoT	2	2			6	
Тема 6. Оновлення ПЗ та безпечне завантаження	2	2			6	
Тема 7. Мережева безпека та сегментація в IoT	2				6	
Тема 8. Захист кінцевих пристроїв і апаратна безпека IoT	2				6	
Змістовий модуль 2 Прийоми та заходи безпеки для IoT						
Тема 9. Аналіз прошивки та реверс-інжиніринг IoT-пристроїв	4	2	3	3	6	Поточне опитування
Тема 10. Захист даних та приватність	2	2			6	
Тема 11. Хмарні та мобільні IoT-платформи	2	2			6	
Тема 12. Реальні атаки та інциденти	2	-			6	
Тема 13. Промисловий IoT та OT-безпека	2	-			8	
Тема 14. Дослідження та розробки в області IoT	2	-			7	
Тема 15. Майбутнє безпеки IoT та нові виклики	2	-			6	
Разом	**32**	**14**	**5**	**6**	**93**	

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. Вступ до IoT і основи безпеки	2	2	8
Тема 2. Уразливості та загрози IoT			8
Тема 3. Основи криптографії для IoT			8
Тема 4. Аутентифікація та авторизація	2		8
Тема 5. Безпечні протоколи IoT			8
Тема 6. Оновлення ПЗ та безпечне завантаження			10
Тема 7. Мережева безпека та сегментація в IoT			8
Тема 8. Захист кінцевих пристроїв і апаратна безпека IoT			8
Змістовий модуль 2 Прийоми та заходи безпеки для IoT			
Тема 9. Аналіз прошивки та реверс-інжиніринг IoT-пристроїв	2	2	12
Тема 10. Захист даних та приватність			10
Тема 11. Хмарні та мобільні IoT-платформи			10
Тема 12. Реальні атаки та інциденти	2		10
Тема 13. Промисловий IoT та OT-безпека			10
Тема 14. Дослідження та розробки в області IoT			10
Тема 15. Майбутнє безпеки IoT та нові виклики			10
Разом	**8**	**4**	**138**

5. Тематика лабораторних занять

Лабораторна робота №1

Тема: Розвідка та профілювання IoT-пристрою (Discovery → Enumeration)

Мета. Навчитися виявляти IoT-вузли в мережі, профілювати їх сервіси/ПЗ та побудувати первинну модель загроз.

Завдання.

1. Виконати мережеву розвідку.
2. Зіставити сервіси з відомими CVE.
3. Побудувати коротку модель загроз (STRIDE) і матрицю ризиків.
4. Оцінити поверхню атаки

Лабораторна робота №2

Тема: Криптографія для IoT: AEAD та управління ключами

Мета. Засвоїти шифрування телеметрії з автентифікацією (AEAD) і базові підходи до керування ключами на обмежених пристроях.

Завдання.

1. Реалізувати захист повідомлень датчика у Python (AES-GCM або ChaCha20-Poly1305).
2. Порахувати ентропію даних датчика до/після стиснення, пояснити вплив на трафік.
3. Зробити деривацію ключа з пароля/секрету за HKDF.
   Порівняти енерговитрати/латентність на повідомлення (10^3 вимірів).

Лабораторна робота №3

Тема: Автентифікація пристроїв: X.509 mTLS та ролі доступу (RBAC/ABAC)

Мета. Налаштувати взаємну TLS-автентифікацію пристрою до шлюзу (MQTT) та описати політики доступу.

Завдання.

1. Згенерувати кореневий CA, видати пристрою сертифікат (openssl/cfssl), перевірити ланцюг довіри.
2. Увімкнути mTLS на брокері (наприклад, Mosquitto) та опублікувати/підписатися на топіки sensors/#.
3. Спроєктувати RBAC-матрицю: role × resource (topic) → allow/deny; або правило ABAC (атрибути: тип пристрою, зона, чутливість даних).

Перевірити відмову доступу при підміні сертифіката; зафіксувати в логах reason code та TLS alert.

Лабораторна робота №4

Тема: Безпечні протоколи IoT: MQTT/TLS vs CoAP/DTLS під аналізом трафіку

Мета. Порівняти безпеку та поведінку двох популярних стеків, дослідити рукостискання та захист від MITM.

Завдання.

1. Розгорнути два сценарії: MQTT/TLS і CoAP/DTLS.
2. Захопити трафік у Wireshark, ідентифікувати етапи рукостискання.
3. Імітувати MITM із самопідписаним сертифікатом; довести відмову з'єднання через невірний кореневий CA.
4. Оцінити пропускну здатність для різних QoS (MQTT) та CoAP.

Лабораторна робота №5

Тема: Захищене оновлення ПЗ та Secure Boot (ланцюг довіри)

Мета. Реалізувати підписане OTA-оновлення та перевірку підпису на пристрої/емуляторі; продемонструвати відхилення підробки.

Завдання.

1. Зібрати мінімальну "прошивку" (ESP32/Raspberry Pi user-space образ), розмістити OTA-артефакт на мікросервісі (Docker).
2. Підписати образ (RSA-2048/Ed25519).
3. Налаштувати перевірку під час завантаження: відмова старта при невалідному підписі.
4. Спробувати «атаку» – підмінити байт у файлі; показати, що перевірка падає, OTA відхиляється.

Лабораторна робота №6

Тема: Аналіз прошивки та реверс-інжиніринг IoT

Мета. Отримати навички статичного/динамічного аналізу прошивок і виявлення вразливостей/секретів.

Завдання.

1. Витягнути файлову систему binwalk/unsquashfs, пошук секретів (strings, trufflehog, gitleaks), перевірити слабкі хеші паролів (/etc/shadow).
2. Запустити прошивку у QEMU/Firmadyne; ідентифікувати відкриті сервіси, провести сканування nmap.
3. Статичний аналіз у Ghidra: знайти небезпечні виклики (strcpy, system), намітити потенційну переповнену буфером ділянку.
4. Зібрати SBOM (syft) і прогнати сканер вразливостей (grype); сформувати звіт із CVE-пріоритизацією.

6. Самостійна робота

Для самостійної роботи кожному студенту пропонується виконання наскрізного завдання.

Приклади завдань:

1. Розвідка та модель загроз IoT-пристрою
2. Порівняння протоколів MQTT vs CoAP
3. AEAD у IoT-телеметрії
4. mTLS для автентифікації пристрою
5. Захищене оновлення ПЗ (Secure Boot + OTA)
6. Аналіз прошивки (theory-first)
7. Сегментація та фільтрація в IoT-мережі
8. Приватність і мінімізація даних
9. План реагування на інцидент IoT
10. SBOM та керування вразливостями
11. Легковагові криптопримітиви для MCU
12. OT-безпека: Modbus/TCP кейс
13. Zero-Trust для IoT-сегменту
14. Тренд-огляд: майбутні виклики IoT-безпеки
15. Порівняння продуктивності: програмна криптографія vs TPM-операції
16. Віддалена атестація MQTT-клієнта з TPM
17. Запечатування секрету до стану системи (PolicyPCR) (з TPM 2.0)
18. Базова ідентичність пристрою (EK/AK) та цитування PCR (з TPM 2.0)
19. Генерація ключа на чипі та TLS-клієнтська автентифікація
20. ECDH-узгодження сесійного ключа на SE та HKDF-деривація

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

Назва: Довірена IoT-платформа: практикум з віддаленої атестації на Raspberry Pi з TPM 2.0.

Тема: Глибоке занурення у технології безпеки IoT-пристроїв на прикладі Raspberry Pi з апаратним модулем довіреної платформи (TPM 2.0). Учасники вивчатимуть механізм *віддаленої атестації* – перевірки цілісності пристрою стороннім сервером – з використанням TPM для забезпечення довіри до завантаження та стану системи.

Очікувані цілі та результати навчання.

Розуміння TPM 2.0. Студенти пояснюють призначення TPM (Trusted Platform Module) і його можливості в IoT (захищене зберігання ключів, генерація випадкових чисел, платформи довіри тощо).

Механізм віддаленої атестації. Учасники розуміють, як працює віддалена атестація пристрою: що таке регістри конфігурації платформи (PCR), як формується хеш-вимір платформи та підписується TPM для перевірки на сервері.

Практичні навички з tpm2-tools. Студенти навчаться використовувати утиліти **tpm2-tools** для реальних задач: читання та розширення PCR, створення криптоключів в TPM (Endorsement Key, Attestation Key), генерування та перевірка квоти (quote) TPM.

Налаштування безпечного завантаження/стану. Учасники налаштують Raspberry Pi з TPM 2.0, увімкнуть підтримку TPM (SPI/I2C), зможуть зчитати вимірювання стану системи та забезпечити їх перевірку сервером.

Вирішення практичних завдань. По завершенні тренінгу студенти вмітимуть реалізувати базову схему віддаленої атестації: сформувати на пристрої доказ цілісності системи (атестаційні дані) та успішно верифікувати його на стороні сервера, виявляючи несанкціоновані зміни.

Завдання 1. Базова робота з TPM (PCR та генерація ключів)

Завдання 2. Реалізація віддаленої атестації пристрою

Завдання 3. Перевірка засвоєння – виявлення втручання

8. Методи навчання.

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

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;
– підсумковий екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

11. 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.	Підсумкове тестування за темами №1-15.	Визначається як середнє арифметичне з оцінок за виконання трьох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання наскрізного завдання.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання - max 40 балів

Виконання лабораторних робіт:

90-100 балів: здобувач освіти самостійно, без помилок, виконав усі кроки лабораторної роботи, правильно задокументував етапи та вільно оперує поняттями та принципами цифрової криміналістики.

75-89 балів: здобувач освіти виконав завдання лабораторної роботи, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи.

60-74 балів: здобувач освіти виконав завдання лабораторної роботи, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених у лабораторній роботі завдань є поверхневим.

1-59 балів: здобувач освіти не зміг виконати завдання лабораторної роботи або результати були повністю невірними. Не продемонстрував базових навичок роботи з програмним забезпеченням.

Підсумкове модульне тестування - вид контролю, при якому засвоєний здобувачем теоретичний та практичний матеріал оцінюється у форматі тестування. Тестування містить 20 запитань кожна правильна відповідь дає 5 балів, максимум 100 балів.

Тренінг:

90-100 балів: здобувач самостійно, без помилок, виконав усі етапи завдання, правильно задокументував усі етапи роботи, та вільно оперує поняттями та принципами тестування на проникнення;

75-89 балів: здобувач виконав завдання, але з кількома дрібними помилками, які не вплинули на кінцевий результат (наприклад, неточна послідовність дій), виникали питання під час роботи;

60-74 балів: здобувач виконав завдання, але з суттєвими помилками, наприклад, не з першого разу. Розуміння поставлених завдань є поверхневим;

1-59 балів: здобувач не зміг виконати завдання або результати були повністю невірними. Не продемонстрував базових навичок роботи з наданим програмним забезпеченням.

Самостійна робота:

90–100 балів: звіт охоплює всі ключові аспекти обраної теми, демонструючи глибоке розуміння предмета. Дослідження містить не лише опис, але й глибокий аналіз, порівняння різних підходів та методів, а також обґрунтовані висновки. Використані сучасні та актуальні джерела інформації, що свідчить про обізнаність здобувачів освіти з останніми тенденціями у цифровій криміналістиці. Здобувач освіти вільно володіє матеріалом, виступає впевнено та відповідає на всі запитання.

75–89 балів: звіт розкриває основні питання теми, але може бути менш деталізованим. В роботі присутні аналітичні елементи, але вони можуть бути не достатньо глибокими. Використані джерела інформації є релевантними, але можуть бути не найновішими. Здобувач освіти демонструє знання матеріалу, але може мати незначні труднощі з відповідями на додаткові питання.

60–74 балів: звіт охоплює лише основні аспекти теми. Можуть бути пропущені важливі деталі. Робота має описовий характер, аналіз та висновки є поверхневими. Здобувач освіти не завжди впевнено відповідає на запитання. Виступ може бути нечітким.

1–59 балів: зміст звіту не відповідає темі або є компіляцією застарілих даних. Робота є прямим копіюванням без самостійного опрацювання.

Екзамен - вид підсумкового контролю, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу. Екзаменаційний білет складається з двох блоків.

Перший блок містить два теоретичних запитань, за кожне з яких можна отримати від 0 до 30 балів, що в підсумку дає максимально 60 балів. За відповідь на питання здобувач отримує 16–30 балів, якщо у повному обсязі володіє навчальним матеріалом, всебічно, самостійно та аргументовано відповідає на питання білету і 1–15 балів – якщо володіє

навчальним матеріалом не в повному обсязі, викладає його фрагментарно, допускаючи при цьому суттєві неточності.

Другий блок містить практичне завдання:

30 – 40 балів - доповідь охоплює всі основні аспекти обраної теми, демонструючи глибоке розуміння предмету дисципліни. Здобувач вільно володіє матеріалом, відповідає впевнено на всі запитання.

21–30 балів - доповідь розкриває основні питання теми, але може бути недостатньо деталізованою; є аналітичні елементи, але вони можуть бути не достатньо глибокими. Здобувач демонструє знання матеріалу, але має незначні труднощі з відповідями на додаткові питання.

11–20 балів - відповідь охоплює лише основні аспекти теми, бути пропущені важливі деталі. Здобувач не завжди впевнено відповідає на запитання.

1–10 балів - відповідь містить значні помилки або не зовсім відповідає завданню.

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)

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

№	**Найменування**	**Номер теми**
1.	Мультимедійний проектор	1 - 15
2.	Комп'ютерна лабораторія. Доступ до Інтернету.	1 - 15
3.	Одноплатні комп'ютери Raspberry Pi	2 - 15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Architecture of Internet of Things (IoT). https://www.geeksforgeeks.org/computer-networks/architecture-of-internet-of-things-iot/

2. NIST SP 800-183. Networks of 'Things'. https://csrc.nist.gov/pubs/sp/800/183/final#:~:text=possible%20nefarious%20intent,all%20distributed%20systems%20that%20employ

3. OWASP Internet of Things. https://owasp.org/www-project-internet-of-things/

4. NIST SP 800-213. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. https://csrc.nist.gov/pubs/sp/800/213/final#:~:text=Organizations%20will%20increasingly%20use%20Internet,actions%20an%20organization%20will%20expect

5. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf

6. MQTT Message Data Integrity - MQTT Security Fundamentals. https://www.hivemq.com/blog/mqtt-security-fundamentals-mqtt-message-data-integrity/

7. Heightened DDoS Threat Posed by Mirai and Other Botnets | CISA.

https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

8. RFC 9200: Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth). https://www.rfc-editor.org/rfc/rfc9200.html.

9. IoT Protocols and Standards Worth Exploring in 2024 | EMQ.
https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m

10. MQTT vs CoAP: Comparing Protocols for IoT Connectivity | EMQ.
https://www.emqx.com/en/blog/mqtt-vs-coap

11. OTA IoT Breakdown: What OTA Is and How It Works in IoT.
https://memfault.com/blog/ota-for-iot/

12. Network Firewalls vs. Application Firewalls | Linode Docs.
https://www.linode.com/docs/guides/network-firewalls-vs-application-firewalls/

13. Enabling a Fast and Secure VPN for IoT devices using WireGuard.
https://www.netmaker.io/resources/vpn-for-iot-devices

14. Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8320-draft.pdf

15. A Review of IoT Firmware Vulnerabilities and Auditing Techniques.
https://www.mdpi.com/1424-8220/24/2/708

16. OWASP IoTGoat – Deliberately Insecure IoT Firmware.
https://www.oneconsult.com/en/blog/iot-ot-security/owasp-iotgoat-deliberately-insecure-iot-firmware/

17. NIST Special Publication 800-57 Part 1 Revision 5. Recommendation for Key Management: Part 1 – General . https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt1r5.pdf

18. Автентифікація та безпека: захист API і контроль доступу.
https://jackcode.io/ua/trending/api-integration/authentication-security/

19. The Top Internet of Things (IoT) Cybersecurity Breaches in 2025 – Asimily. https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2025/

20. The Top Internet of Things (IoT) Cybersecurity Breaches in 2025
https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2025/

21. What is the Mirai Botnet?
https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

22. IoT SECURITY GUIDE. https://www.dsci.in/files/content/knowledge-centre/2023/IoT-Security-Guide.pdf

23. Guide to Attribute Based Access Control (ABAC) Definition and Considerations https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

24. GSMA 5G Security Guide v3.0 (2024). https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/07/FS.40-v3.0-002-19-July.pdf?utm_source=chatgpt.com

25. FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://csrc.nist.gov/pubs/fips/203/final?utm_source=chatgpt.com

26. 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.

27. 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.