Чернівецький національний університет імені Юрія Федьковича

(повне найменування головного закладу вищої освіти)

Відокремлений структурний підрозділ «Фаховий коледж

Чернівецького національного університету імені Юрія Федьковича»

(повна назва відокремленого структурного підрозділу)

Циклова комісія *комп'ютерна інженерія*

(назва циклової/предметної комісії)

"ПОГОДЖЕНО"
Завідувач
Природничого відділення
(підпис) *Христина МЕЛЬНИЧУК* (ім'я та прізвище)
"27" 08 20 26 року

"ЗАТВЕРДЖУЮ"
Заступник директора
з навчально-методичної роботи
(підпис) *Микола ДЕРЕВ'ЯНЧУК* (ім'я та прізвище)
"28" 08 20 26 року

ПРОГРАМА

навчальної дисципліни

"Основи Інтернету речей"

(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))

обов'язкова

(вказати: обов'язкова/вибіркова)

Освітньо-професійна програма

"Комп'ютерна інженерія"

(назва освітньо-професійної програми)

Спеціальність

123 Комп'ютерна інженерія

(код і назва спеціальності)

Галузь знань

12 Інформаційні технології

(код і назва галузі знань)

Освітньо-професійний ступінь

фаховий молодший бакалавр

(назва освітньо-професійного ступеня)

Мова навчання

українська

(вказати: на якій мові читається предмет)

Чернівці, 2026

Програма навчальної дисципліни *"Основи Інтернету речей"*

(назва навчальної дисципліни)

складена відповідно до освітньо-професійної програми

"Комп'ютерна інженерія"

(назва освітньо-професійної програми)

затвердженої Вченою радою Чернівецького національного університету імені Юрія Федьковича (Протокол № 12 від «2» вересня 2024 року) та введеної в дію наказом ректора № 315 від «28» серпня 2026 року.

Розробники: (вказати авторів, їхні посади, наукові ступені та вчені (педагогічні) звання)

викладач вищої кваліфікаційної категорії, О.Ю. Тащук

Профайл викладача https://ce-college.chnu.edu.ua/tsyklova-komisiia/sklad-tsyklovoi-komisii/tashchuk-oleksandr-yuriiovych/

E-mail o.tashchuk@chnu.edu.ua

Сторінка курсу в Moodle https://moodle.chnu.edu.ua/enrol/index.php?id=5515

Робоча програма обговорена та узгоджена на засіданні циклової комісії

комп'ютерна інженерія

Протокол № 1 від "27" 08 2026 року

Голова циклової комісії _____ *Олександр ТАЩУК*

(підпис) (ім'я та прізвище)

Схвалена Методичною радою

Протокол № 1 від "27" 08 2026 року

Голова методичної ради _____ *Ольга БІЛОКРИЛА*

(підпис) (ім'я та прізвище)

ПЕРЕЗАТВЕРДЖЕНО

Протокол № ____ від _____, 20 __ р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

Протокол № ____ від _____, 20 __ р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

Протокол № ____ від _____, 20 __ р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

1. Мета та завдання навчальної дисципліни

Анотація: дисципліна «Основи інтернету речей» формує системне розуміння принципів побудови та функціонування IoT-систем — від сенсорного вузла і вбудованого програмного забезпечення до мережевого обміну, хмарної платформи, візуалізації даних та керування виконавчими пристроями. Зміст курсу охоплює архітектури Інтернету речей, мікроконтролерні платформи на базі ESP32, цифрові й аналогові сенсори, виконавчі пристрої, інтерфейси GPIO, ADC, PWM, UART, I²C і SPI, безпровідні технології Wi-Fi та Bluetooth Low Energy, прикладні протоколи MQTT, HTTP/REST і CoAP, формати обміну даними, шлюзи, edge/cloud-підходи, платформи Blynk і Node-RED, а також питання інформаційної безпеки, надійності, енергоефективності та діагностування IoT-рішень.

Мета: формування у здобувачів фахової передвищої освіти теоретичних знань і практичних умінь, необхідних для розроблення, підключення, програмування, тестування та експлуатації базових систем Інтернету речей. Дисципліна має забезпечити розуміння взаємодії фізичних пристроїв, мікроконтролерів, мережевих протоколів, сервісів оброблення даних і хмарних платформ; навчити збирати телеметрію із сенсорів, керувати виконавчими механізмами, організовувати двосторонній обмін даними, будувати панелі моніторингу та застосовувати базові засоби захисту підключених пристроїв.

Завдання: засвоїти понятійний апарат, рівні та типові архітектури IoT; сформувати розуміння ролі сенсорів, виконавчих пристроїв, контролерів, шлюзів, мережі та хмарних сервісів; навчити програмувати ESP32 і використовувати GPIO, ADC, PWM, UART, I²C та SPI; сформувати навички підключення і калібрування сенсорів та керування виконавчими пристроями; опанувати підключення до Wi-Fi і Bluetooth Low Energy, основи мережевої адресації та діагностування з'єднання; навчити застосовувати MQTT, HTTP/REST і CoAP, працювати з JSON та іншими форматами подання телеметрії; ознайомити з Blynk, Node-RED та принципами edge/cloud-оброблення; сформувати навички організації віддаленого моніторингу й керування, подієвої автоматизації, журналювання та зберігання даних; ознайомити з типовими загрозами IoT, автентифікацією, авторизацією, TLS, безпечним зберіганням облікових даних і OTA-оновленням; розвинути вміння інтегрувати компоненти у завершений прототип і аргументовано оцінювати його надійність, енергоспоживання та безпеку.

Предмет навчальної дисципліни: архітектури та компоненти Інтернету речей; вбудовані IoT-вузли на базі мікроконтролерів; сенсори і виконавчі пристрої; периферійні інтерфейси; безпровідний зв'язок; мережеві й прикладні протоколи обміну даними; MQTT-брокери та REST-сервіси; шлюзи; edge- і cloud-обчислення; платформи моніторингу й керування; зберігання та візуалізація телеметрії; безпека, енергоефективність, тестування і супроводження IoT-систем.

Пререквізити: базові знання з програмування, комп'ютерної схемотехніки та архітектури комп'ютерів, комп'ютерних мереж, електроніки й принципів роботи мікроконтролерних систем. Для виконання лабораторних робіт необхідні навички роботи з середовищем розробки, базовими конструкціями мов C/C++, двійковим поданням даних, основами TCP/IP і підключенням електронних компонентів до низьковольтних цифрових систем.

Постреквізити: знання і практичні навички, отримані під час вивчення дисципліни, використовуються у вбудованих системах, комп'ютерних мережах, автоматизації, робототехніці, кібербезпеці, хмарних і периферійних обчисленнях, під час виробничої та переддипломної практики, а також при виконанні курсових і кваліфікаційних робіт, пов'язаних зі Smart Home, промисловим моніторингом, енергоменеджментом, агро-IoT та іншими кіберфізичними системами.

Студент повинен знати:

базові терміни, моделі та рівні архітектури Інтернету речей; призначення сенсорів, виконавчих пристроїв, IoT-вузлів, шлюзів, брокерів і хмарних сервісів; основні можливості ESP32 та принципи використання GPIO, ADC, PWM, UART, I²C і SPI; особливості підключення цифрових і аналогових сенсорів; принципи роботи Wi-Fi, Bluetooth Low Energy

та огляд інших IoT-технологій зв’язку; основи TCP/IP, адресації і мережевого діагностування; моделі обміну MQTT, HTTP/REST та CoAP, рівні QoS і призначення retained message та Last Will у MQTT; структуру JSON і базові способи серіалізації даних; принципи роботи Blynk, Node-RED, edge- та cloud-сервісів; підходи до зберігання, візуалізації та подієвої обробки телеметрії; типові загрози IoT, засоби автентифікації, авторизації, шифрування, TLS і безпечного OTA-оновлення; методи зниження енергоспоживання, підвищення надійності та діагностування підключених пристроїв.

Студент повинен вміти:

налаштовувати середовище розробки та програмувати ESP32; підключати сенсори й виконавчі пристрої, читати цифрові та аналогові сигнали, формувати PWM і використовувати UART, I²C та SPI; виконувати базове калібрування й перевірку достовірності показів; підключати IoT-вузол до Wi-Fi і Bluetooth Low Energy та діагностувати мережеве з’єднання; реалізовувати обмін телеметрією і командами за MQTT та HTTP/REST, формувати і розбирати JSON-повідомлення; працювати з MQTT-брокером, Blynk і Node-RED; створювати прості панелі моніторингу, правила автоматизації та віддалене керування; застосовувати базові механізми автентифікації, контролю доступу і TLS; організовувати журналювання, watchdog, оброблення помилок і повторне підключення; оцінювати споживання ресурсів та енергії; інтегрувати апаратні, мережеві й програмні компоненти у працездатний IoT-прототип, тестувати його та документувати результати.

Компетентності:

ЗК.03 Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК.04 Здатність застосовувати знання у практичних ситуаціях.
ЗК.05 Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК.07 Здатність працювати в команді.
ЗК.08 Здатність вчитися і оволодівати сучасними знаннями.
СК.02 Здатність застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування апаратних, програмних та інструментальних засобів комп’ютерної інженерії.
СК.04 Здатність брати участь у розробці системного та прикладного програмного забезпечення засобів комп’ютерної інженерії з використанням ефективних алгоритмів, сучасних методів і мов програмування.
СК.06 Здатність брати участь у модернізації апаратних та програмних засобів комп’ютерної інженерії.
СК.09 Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.
СК.10 Здатність аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.
СК.13 Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних систем, мереж та їх компонентів шляхом використання аналітичних методів і методів моделювання.
СК.16 Здатність генерувати нові ідеї (креативність).
СК.17 Здатність до абстрактного мислення, аналізу і синтезу.

Програмні результати навчання:

РН.02 Знати і розуміти теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп’ютерної інженерії.
РН.03 Знати сучасні методи та технології для розв’язання прикладних задач комп’ютерної інженерії.
РН.06 Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп’ютерної інженерії.

РН.07 Застосовувати знання для формулювання і розв’язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.
РН.08 Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп’ютерної інженерії для вирішення технічних задач у професійній діяльності.
РН.10 Здійснювати пошук інформації з різних джерел для розв’язання задач комп’ютерної інженерії.
РН.11 Ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів комп’ютерної інженерії.
РН.13 Обґрунтовувати прийняті рішення, оцінювати, оформляти та представляти результати професійної діяльності згідно з діючою нормативною документацією.
РН.18 Системно мислити та застосовувати творчі здібності до формування нових та нестандартних рішень при розв’язуванні задач комп’ютерної інженерії.
РН.19 Вміти використовувати методи аналізу та синтезу при розробці апаратних та програмних засобів комп’ютерної інженерії.
РН.20 Вміти ефективно працювати як індивідуально, так і у складі команди при вирішенні технічних та організаційних задач у професійній діяльності.

2. Опис навчальної дисципліни

2.1. Загальна інформація

Форма навчання	Рік підготовки	Семестр	Кредити	Години	Лекції	Лабораторні	Самостійна робота	Вид підсумкового контролю
Денна	4	8	3	90	24	24	42	залік

Навчальне навантаження становить 90 годин (3 кредити ЄКТС), з яких 24 годин передбачено на лекційні заняття, 24 години — на лабораторні заняття та 54 години — на самостійну роботу. Дисципліна вивчається на четвертому році підготовки у восьмому семестрі та завершується заліком.

2.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Усього	л	п	лаб	інд	с.р.
1	**2**	**3**	**4**	**5**	**6**	**7**
Змістовий модуль 1. Архітектура IoT та апаратні вузли						
Тема 1. Концепція, архітектури та компоненти Інтернету речей. IoT-вузли, шлюзи, edge і cloud-рівні.	15	4	–	4	–	7
Тема 2. Апаратна платформа ESP32, сенсори, виконавчі пристрої та периферійні інтерфейси.	15	4	–	4	–	7
Разом за ЗМ 1	**30**	**8**	**–**	**8**	**–**	**14**
Змістовий модуль 2. Мережеві технології та протоколи IoT						
Тема 3. Безпровідні технології IoT: Wi-Fi, Bluetooth Low Energy та огляд Zigbee/Thread і LoRaWAN.	15	4	–	4	–	7
Тема 4. Прикладні протоколи IoT: MQTT, HTTP/REST, CoAP. Формати даних і моделі обміну повідомленнями.	15	4	–	4	–	7
Разом за ЗМ 2	**30**	**8**	**–**	**8**	**–**	**14**
Змістовий модуль 3. Хмарні платформи, автоматизація та безпека IoT						
Тема 5. Хмарні та edge-платформи IoT. Blynk, Node-RED, телеметрія, візуалізація і автоматизація.	15	4	–	4	–	7
Тема 6. Безпека, надійність, енергоефективність, OTA-оновлення та комплексне тестування IoT-систем.	15	4	–	4	–	7
Разом за ЗМ 3	**30**	**8**	**–**	**8**	**–**	**14**
Усього годин	**90**	**24**	**–**	**24**	**–**	**42**

3. Теми лекційних занять

№	Назва теми	Кількість годин
ЗМ 1. Архітектура IoT та апаратні вузли		
1	Інтернет речей: поняття, сфери застосування, M2M та кіберфізичні системи. Рівні й типові архітектури IoT: пристрій, шлюз, мережа, edge/cloud, застосунок.	4
2	IoT-вузол на базі ESP32. GPIO, ADC, PWM, UART, I²C і SPI. Сенсори та виконавчі пристрої, узгодження сигналів, живлення й базове керування енергоспоживанням.	4
ЗМ 2. Мережеві технології та протоколи IoT		
3	Безпровідний зв’язок в IoT. Wi-Fi і Bluetooth Low Energy; принципи вибору технології. Огляд Zigbee/Thread і LoRaWAN. Адресація, підключення та мережеве діагностування.	4
4	Протоколи прикладного рівня IoT. MQTT: брокер, topic, publish/subscribe, QoS, retained message, Last Will. HTTP/REST і CoAP. JSON та інші формати телеметрії.	4
ЗМ 3. Хмарні платформи, автоматизація та безпека IoT		
5	IoT-платформи та оброблення даних. Blynk, Node-RED, шлюзи, edge/fog і cloud. Збір, зберігання, візуалізація телеметрії, правила автоматизації та віддалене керування.	4
6	Безпека і життєвий цикл IoT. Автентифікація, авторизація, TLS, захист облікових даних, OTA-оновлення, watchdog, журналювання, енергоефективність, тестування та супроводження.	4
	Усього	**24**

4. Теми лабораторних занять

№	Назва теми	Кількість годин
ЗМ 1. Архітектура IoT та апаратні вузли		
1	Налаштування середовища розробки для ESP32. Завантаження першої програми, робота із Serial Monitor, цифрові входи та виходи GPIO.	2
2	Робота з аналоговими сигналами: ADC і PWM. Зчитування аналогового сенсора та керування яскравістю світлодіода або іншим виконавчим пристроєм.	2
3	Підключення цифрових сенсорів і модулів за I²C, SPI або UART. Зчитування даних та виведення показів на локальний індикатор.	2
4	Побудова локального сенсорного вузла: періодичне опитування датчиків, фільтрація/перевірка даних, керування виконавчим пристроєм за заданою умовою.	2
ЗМ 2. Мережеві технології та протоколи IoT		
5	Підключення ESP32 до Wi-Fi. Отримання мережевих параметрів, перевірка доступності вузлів, повторне підключення та діагностування збоїв зв’язку.	2
6	HTTP/REST у IoT: формування GET/POST-запитів, обмін JSON-даними з вебсервісом та реалізація простого HTTP-сервера на ESP32.	2
7	MQTT: підключення клієнта до брокера, publish/subscribe, робота з topics, QoS, retained messages і Last Will.	2
8	Bluetooth Low Energy: виявлення пристроїв, GATT-сервіси та характеристики, передавання телеметрії або команд між ESP32 і клієнтським пристроєм.	2
ЗМ 3. Хмарні платформи, автоматизація та безпека IoT		
9	Підключення ESP32 до Blynk. Передавання телеметрії, створення віджетів панелі та реалізація віддаленого керування виконавчим пристроєм.	2
10	Node-RED для IoT: приймання MQTT/HTTP-даних, побудова потоку оброблення, візуалізація показів і формування подієвих сповіщень.	2
11	Базовий захист IoT-вузла: керування обліковими даними, автентифікація, TLS-з’єднання, аналіз журналів і підготовка безпечного OTA-оновлення.	2
12	Комплексний IoT-прототип: сенсор → ESP32 → мережа → MQTT/хмарна платформа → панель моніторингу → команда виконавчому пристрою; тестування та аналіз надійності.	2
	Усього	**24**

5. Самостійна робота

№	Назва теми для самостійного опрацювання	Кількість годин
ЗМ 1. Архітектура IoT та апаратні вузли		
1	Еволюція IoT, M2M і кіберфізичних систем; референтні моделі, цифрові двійники та типові сценарії застосування.	3
2	Архітектура сімейства ESP32, пам’ять, периферія, FreeRTOS у складі SDK, режими сну та керування енергоспоживанням.	4
3	Характеристики сенсорів: точність, роздільна здатність, похибка, калібрування, фільтрація та перевірка достовірності вимірювань.	3
4	Поглиблене опрацювання UART, I²C, SPI, 1-Wire; адресація периферії, часові параметри шин та діагностування помилок обміну.	4
ЗМ 2. Мережеві технології та протоколи IoT		
5	Порівняння Wi-Fi, BLE, Zigbee/Thread, LoRaWAN і стільникових технологій за дальністю, швидкістю, енергоспоживанням і топологією.	3
6	Мережева взаємодія IoT-вузла: IPv4/IPv6, DHCP, DNS, NAT, NTP, повторне підключення і поведінка при нестабільному каналі.	4
7	MQTT 5.0: рівні QoS, retained message, Last Will, session state, keep alive, шаблони topics та організація надійного обміну.	3
8	HTTP/HTTPS, REST і CoAP; кодування телеметрії за допомогою JSON/CBOR, ідемпотентність запитів та оброблення помилок.	4
ЗМ 3. Хмарні платформи, автоматизація та безпека IoT		
9	Шлюзи, edge/fog/cloud-обчислення в IoT; локальна попередня обробка даних, затримка, автономність і масштабування системи.	3
10	Зберігання часових рядів, візуалізація, тригери, сповіщення та автоматизація в Blynk, Node-RED та аналогічних IoT-платформах.	4
11	Модель загроз IoT: слабкі паролі, витік секретів, незахищені канали, підміна вузлів; PKI, TLS, контроль доступу та безпечне OTA.	3
12	Надійність і супроводження IoT: watchdog, журналювання, відмовостійкість, оновлення, енергоефективність, тестування та оцінювання якості сервісу.	4
	Усього	**42**

6. Методи навчання

Вивчення дисципліни поєднує лекційне опрацювання архітектури та протоколів Інтернету речей із лабораторним конструюванням і програмуванням реальних або модельованих IoT-вузлів. На лекціях аналізуються взаємозв’язки між сенсорним рівнем, вбудованим програмним забезпеченням, мережевою інфраструктурою, прикладними протоколами, шлюзами та хмарними сервісами. Лабораторні заняття спрямовані на формування вмінь працювати з ESP32, сенсорами, виконавчими пристроями, Wi-Fi, BLE, MQTT, HTTP/REST, Blynk і Node-RED, а також інтерпретувати результати вимірювань, мережеві стани та журнали подій.

Пояснювально-ілюстративний метод застосовується для системного подання архітектурних і протокольних рішень; проблемне навчання — під час вибору способу підключення сенсорів, технології зв’язку, протоколу обміну, структури topics або політики керування енергоспоживанням; частково-пошуковий і дослідницький методи — під час лабораторних робіт, де здобувач змінює параметри вузла, виконує вимірювання, аналізує трафік і логи, порівнює альтернативні реалізації та обґрунтовує висновки. Практичні ситуації моделюються як завершені ланцюги «фізичний параметр — сенсор — контролер — мережа — сервіс — користувач/виконавчий пристрій».

Для організації освітнього процесу використовуються електронний курс Moodle, плати ESP32 або їх програмні моделі, Arduino IDE та/або ESP-IDF, серійний монітор, MQTT-брокер, HTTP-сервіси, Blynk, Node-RED, інструменти мережевого діагностування та засоби візуалізації телеметрії. Самостійна робота включає опрацювання технічної документації, підготовку схем підключення, аналіз протоколів, виконання розрахунково-аналітичних завдань, дослідження енергоспоживання і безпеки та підготовку до захисту лабораторних робіт.

7. Система контролю та оцінювання

Методи контролю передбачають оцінювання теоретичної підготовки, практичних умінь програмування і підключення IoT-вузлів та здатності пояснювати роботу мережевих і хмарних механізмів. Поточне оцінювання здійснюється за результатами лабораторних робіт, модульних контрольних робіт, тестування в Moodle, усного опитування, аналізу програмного коду, схем підключення, телеметрії та журналів, а також виконання індивідуальних завдань. Захист лабораторної роботи передбачає демонстрацію працездатності вузла або моделі, пояснення структури програми, параметрів мережевого обміну, інтерпретацію отриманих даних і відповіді на контрольні запитання.

Форми контролю: у 8 семестрі здійснюються поточний і модульний контроль та підсумковий залік. У разі організації освітнього процесу в дистанційній або змішаній формі тестування, подання звітів, демонстрація програмних моделей, хмарних панелей і частина захистів можуть проводитися засобами Moodle та відеоконференцій із дотриманням вимог до ідентифікації здобувача та академічної доброчесності.

Політика академічної доброчесності. Лабораторні, самостійні та контрольні завдання виконуються самостійно з коректним зазначенням використаних джерел, бібліотек, фрагментів коду, схем, конфігурацій і зовнішніх матеріалів. Використання інструментів штучного інтелекту допускається як допоміжного засобу для пояснення, пошуку помилок, перевірки коду або аналізу журналів за умови, що здобувач розуміє результат, може відтворити основні кроки та зазначає факт і спосіб використання такого інструменту. Не допускається подання автоматично згенерованих звітів, програм або результатів експериментів як власної самостійної роботи без перевірки й пояснення.

Розподіл балів у 8 семестрі (залік)

Вид роботи	Лабораторні роботи 1–12	**Модульні контрольні роботи**	**Самостійна робота / активність**	**Разом**
Поточний контроль	30	15	5	50
Залік				50

Семестрова оцінка визначається як сума балів за поточну роботу (до 50 балів) і результат підсумкового заліку (до 50 балів), максимальна кількість — 100 балів.

Критерії оцінювання відповідей студентів

Рівень	**Бали**	**Критерії оцінювання**
Високий	90–100 %	Повне і коректне розуміння теоретичного матеріалу; правильне пояснення архітектури IoT та взаємодії її рівнів; коректне застосування інтерфейсів, мережевих протоколів і сервісів; відсутність принципових помилок у схемі, програмі та інтерпретації телеметрії; здатність самостійно формулювати висновки і порівнювати альтернативні рішення.
Достатній	70–89 %	Матеріал засвоєно в цілому правильно; допускаються поодинокі неточності, що не змінюють суті відповіді; практичне завдання виконано коректним методом, але можливі незначні похибки у схемі підключення, коді, налаштуваннях або аргументації.
Середній	50–69 %	Засвоєно основні положення, однак наявні суттєві прогалини в поясненні взаємозв’язків між пристроєм, мережею та сервісом; практичне завдання виконано частково, з помилками у підключенні, логіці програми, налаштуванні протоколу або інтерпретації результатів.
Початковий	0–49 %	Відсутнє системне розуміння ключових понять; відповідь містить принципові змістові помилки; студент не може пояснити роботу базового IoT-вузла, організувати коректний обмін даними або

		виконати практичне завдання на рівні, достатньому для досягнення програмних результатів навчання.

8. Критерії оцінювання навчальних досягнень студентів під час проведення підсумкового контролю

Залік у 8 семестрі проводиться в усній, письмовій або комбінованій формі. Залікове завдання може містити два теоретичні питання та одне практичне завдання, пов’язане з архітектурою IoT, підключенням сенсора чи виконавчого пристрою, периферійними інтерфейсами ESP32, налаштуванням Wi-Fi/BLE, побудовою MQTT-обміну, HTTP/REST-запитом, формуванням JSON, роботою з Blynk або Node-RED, аналізом телеметрії, базовим захистом або діагностуванням IoT-вузла. Максимальна оцінка за залік становить 50 балів.

Під час оцінювання враховуються повнота і точність відповіді, коректне використання термінології, розуміння причинно-наслідкових зв’язків між апаратним, мережевим і програмним рівнями, правильність схеми підключення та алгоритму, здатність інтерпретувати телеметрію й мережеві стани та обґрунтовувати вибір технології. Практичне завдання оцінюється не лише за кінцевим результатом, а й за правильністю послідовності дій, електричною і інформаційною безпечністю виконаних операцій та здатністю пояснити їх вплив на систему.

Шкала оцінювання: національна та ЄКТС

Сума балів	Оцінка ЄКТС	Оцінка за національною шкалою (екзамен)	Оцінка за національною шкалою (залік)
90–100	A	відмінно	зараховано
80–89	B	добре	зараховано
70–79	C	добре	зараховано
60–69	D	задовільно	зараховано
50–59	E	задовільно	зараховано
35–49	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0–34	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

9. Перелік питань для підсумкового контролю

9.1. Питання до заліку (8 семестр)

№	Питання
1	Поняття Інтернету речей (IoT). Основні ознаки та відмінність IoT від традиційних мережевих систем.
2	IoT, M2M і кіберфізичні системи: спільні риси та відмінності.
3	Типові рівні архітектури IoT та функції сенсорного, мережевого, сервісного й прикладного рівнів.
4	Призначення IoT-вузла, шлюзу, edge-вузла, хмарної платформи та користувацького застосунку.
5	Сенсори й виконавчі пристрої в IoT. Основні характеристики сенсорів та критерії їх вибору.
6	Мікроконтролер ESP32 як апаратна платформа IoT: процесор, пам’ять, Wi-Fi/Bluetooth і периферія.
7	Цифрові входи/виходи GPIO. Режими роботи, підтягувальні резистори та правила безпечного підключення.
8	Аналого-цифрове перетворення на ESP32. ADC, роздільна здатність, діапазон і похибки вимірювання.
9	Широтно-імпульсна модуляція (PWM) та керування виконавчими пристроями.
10	Інтерфейс I²C: адресація, лінії SDA/SCL, master/slave та типові застосування.
11	Інтерфейс SPI: сигнали, принцип обміну та порівняння з I²C.
12	Інтерфейс UART: асинхронний послідовний обмін, параметри порту та діагностування.
13	Калібрування, фільтрація і перевірка достовірності даних сенсорів.
14	Керування енергоспоживанням IoT-вузла. Режими сну, duty cycle та компроміс між автономністю і доступністю.
15	Wi-Fi в IoT: підключення до точки доступу, отримання IP-параметрів і повторне підключення.
16	Bluetooth Low Energy: центральні та периферійні пристрої, GATT, services і characteristics.
17	Призначення Zigbee/Thread і типові сфери застосування цих технологій в IoT.
18	LoRaWAN: призначення, особливості далекого зв’язку та обмеження пропускної здатності.
19	IPv4/IPv6, DHCP, DNS і NAT у контексті підключених IoT-пристроїв.
20	Синхронізація часу в IoT. Протокол NTP та роль коректного часу в телеметрії й журналах.
21	Протокол MQTT: архітектура client–broker, модель publish/subscribe та сфери застосування.
22	MQTT topics: структура імен, wildcard-символи та принципи організації ієрархії тем.
23	Рівні QoS у MQTT: at most once, at least once, exactly once та їх вплив на надійність.
24	Retained message, Last Will and Testament, keep alive та session state у MQTT.
25	HTTP/HTTPS у системах IoT. Методи GET, POST, PUT, DELETE та коди стану.
26	Архітектурний стиль REST і його застосування для API підключених пристроїв.
27	CoAP: призначення, особливості та відмінності від HTTP у ресурсно обмежених системах.
28	JSON як формат обміну даними. Структура об’єктів і масивів, переваги та обмеження для телеметрії.
29	MQTT-брокер: функції, маршрутизація повідомлень, автентифікація клієнтів і базові налаштування.
30	Хмарна IoT-платформа: основні функції керування пристроями, телеметрією, користувачами й подіями.
31	Blynk: модель пристрою, datastreams, dashboards, події та віддалене керування.
32	Node-RED: потоки, nodes, messages і застосування для інтеграції та автоматизації IoT.
33	Шлюзи та edge/fog-обчислення. Переваги локального оброблення даних.
34	Зберігання телеметрії та часових рядів. Вимоги до структури, часових міток і агрегації даних.
35	Побудова панелей моніторингу, графіків, порогових умов, тригерів і сповіщень.
36	Віддалене керування виконавчими пристроями. Підтвердження команд, стани та безпечна логіка.
37	Типові загрози IoT: слабкі облікові дані, незахищені інтерфейси, перехоплення трафіку та підміна пристроїв.
38	Автентифікація та авторизація IoT-пристроїв і користувачів. Принцип найменших привілеїв.
39	TLS у IoT: призначення сертифікатів, шифрування каналу та перевірка автентичності сервера/клієнта.
40	Зберігання Wi-Fi-паролів, токенів і ключів. Підходи до безпечного provisioning облікових даних.
41	OTA-оновлення прошивки: призначення, ризики, цілісність, відкат і безпечне розгортання.
42	Watchdog, оброблення виняткових ситуацій, журналювання та автоматичне відновлення IoT-вузла.
43	Методи підвищення надійності передавання даних: буферизація, повторні спроби, підтвердження та ідемпотентність.
44	Оптимізація енергоспоживання сенсорного вузла та оцінювання автономності живлення.
45	Тестування і діагностування IoT-систем: Serial Monitor, мережеві журнали, MQTT-клієнти, вимірювання затримки і втрат.

№	Питання
46	Архітектура системи Smart Home як приклад IoT: сенсори, контролер, мережа, платформа та виконавчі пристрої.
47	Застосування IoT у промисловості, енергетиці, агросекторі, транспорті та міській інфраструктурі.
48	Наскрізний маршрут даних «сенсор → ESP32 → мережа → брокер/хмара → база/панель → команда виконавчому пристрою».
49	Порівняння MQTT, HTTP/REST і CoAP та обґрунтування вибору протоколу для конкретного IoT-сценарію.

10. Рекомендована література

10.1. Основна (базова)

1. King A. Programming the Internet of Things. Sebastopol : O'Reilly Media, 2021. 421 p. ISBN 978-1-4920-8140-1.

2. Bahga A., Madisetti V. Internet of Things: A Hands-On Approach. VPT, 2014. 446 p. ISBN 978-0-9960255-1-5.

3. Buyya R., Dastjerdi A. V. (eds.). Internet of Things: Principles and Paradigms. Morgan Kaufmann, 2016. ISBN 978-0-12-805395-9.

4. McEwen A., Cassimally H. Designing the Internet of Things. Chichester : Wiley, 2013. 336 p. ISBN 978-1-118-43062-0.

10.2. Допоміжна

1. Banks A., Briggs E., Borgendale K., Gupta R. (eds.). MQTT Version 5.0 [Електронний ресурс]. OASIS Standard. 07 March 2019. URL: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html (дата звернення: 24.09.2026).

2. Espressif Systems. ESP-IDF Programming Guide [Електронний ресурс]. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/ (дата звернення: 24.09.2026).

3. Node-RED. User Guide [Електронний ресурс]. URL: https://nodered.org/docs/user-guide/ (дата звернення: 24.09.2026).

Інформаційні ресурси

1. Освітньо-професійна програма «Комп'ютерна інженерія» спеціальності F7 Комп'ютерна інженерія ВСП «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича». URL: https://media.chnu.edu.ua/media/gzppl0ds/f7-ce-2025-college.pdf (дата звернення: 24.09.2026).

2. Електронний курс «Основи інтернету речей» у Moodle Чернівецького національного університету імені Юрія Федьковича. URL: https://moodle.chnu.edu.ua/course/view.php?id=5515 (дата звернення: 24.09.2026).

3. Espressif Systems. ESP-IDF Programming Guide [Електронний ресурс]. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/ (дата звернення: 24.09.2026).

4. Blynk Documentation [Електронний ресурс]. URL: https://docs.blynk.io/ (дата звернення: 24.09.2026).

5. Node-RED Documentation [Електронний ресурс]. URL: https://nodered.org/docs/ (дата звернення: 24.09.2026).

6. OASIS. MQTT Version 5.0 [Електронний ресурс]. URL: https://www.oasis-open.org/standard/mqtt-v5-0-os/ (дата звернення: 24.09.2026).

7. Espressif Systems. Arduino ESP32 Documentation [Електронний ресурс]. URL: https://docs.espressif.com/projects/arduino-esp32/en/latest/ (дата звернення: 24.09.2026).