МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№503)

ЗАТВЕРДЖУЮ
Гарант освітньої програми
_____ О. Ілляшенко
(підпис) (ініціали та прізвище)
«_29_» __серпня__ 2025 р.

СИЛАБУС *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Побудова та кібербезпека інтернету речей

Галузь знань: 12 «Інформаційні технології»

Спеціальність: 125 «Кібербезпека та зажист інформації»

Освітня програма: «Безпека інформаційних і комунікаційних систем»

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025 року

Харків – 2025 р.

Розробник (и): _Землянко Г.А., доц. каф. 503, д-р філос.__ _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 29 » серпня 2025 р.

Завідувач кафедри д-р техн. наук., проф. _____ Вячеслав ХАРЧЕНКО
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

_____ Ілля МІЦИК
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: *Землянко Георгій Андрійович*

Посада: *доцент кафедри комп'ютерних систем, мереж і кібербезпеки*

Науковий ступінь: *доктор філософії з кібербезпеки та захисту інформації*

Вчене звання: -

E-mail: g.zemlynko@csn.khai.edu

Перелік дисциплін, які викладає:

- *Бази даних,*
- *Програмування систем IoT,*
- *Організація та безпека баз даних,*
- *Блокчейн-технології та безпека криптовалют*

Напрями наукових досліджень:
технології розумного міста та цифрова безпека, системи Інтернету речей (IoT), інформаційна безпека та захист даних, аналіз кіберризиків, системи баз даних, технології розумних мереж, телекомунікації та мережеві технології, інтелектуальні системи, безпека розумних систем.

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	*6 семестр*
Мова викладання	*Українська*
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*Денна: 4 кредитів ЄКТС / 120 годин (64 аудиторних, з яких: лекції – 32, практичні – 32; СРЗ – 56);*
Види навчальної діяльності	*Лекції, лабораторні роботи, самостійна робота*
Види контролю	*Поточний контроль, модульний контроль, іспит*
Пререквізити	*«Вища математика»,* *«Дискретна математика»,* *«Основи функціонування комп'ютерів»,* *«Технології програмування»,* *«Комп'ютерна електроніка»,* *«Архітектура комп'ютерів»,* *«Моделі та структури даних»,* *«Комп'ютерна схемотехніка»,* *«Апаратні та програмні засоби захисту інформації»,* *«Вбудовані системи»,* *«Web-технології».*

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета: формування у здобувачів вищої освіти комплексної системи теоретичних знань та прикладних умінь, необхідних для повного циклу безпечної розробки систем Інтернету речей (IoT). Дисципліна спрямована на освоєння принципів проектування захищених програмно-апаратних комплексів, починаючи від низькорівневого програмування мікроконтролерів та забезпечення апаратної безпеки, до реалізації захищених мережевих протоколів та інтеграції розроблених пристроїв із хмарними сервісами для збору, моніторингу та аналітики даних з урахуванням вимог конфіденційності та цілісності.

Завдання: вивчення архітектури, принципів функціонування та типових вразливостей сучасних мікроконтролерних платформ (зокрема сімейств Arduino та ESP). Курс передбачає детальне освоєння мов програмування (C/C++, Sketch) з використанням стандартів безпечного кодування та спеціалізованих середовищ розробки. Важливою складовою є набуття практичних навичок схемотехнічного підключення, програмного керування різноманітними сенсорами та захисту їх від спуфінг-атак. Окремий акцент робиться на вивченні безпеки дротових (SPI, I2C, UART) та бездротових інтерфейсів, а також реалізації мережевої взаємодії за допомогою стеків протоколів TCP/IP, Wi-Fi, Bluetooth, HTTP та MQTT із застосуванням шифрування (TLS/SSL) та автентифікації для забезпечення надійної комунікації у розподілених інформаційних системах.

Компетентності, які набуваються:

Інтегральна компетентність:

Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності (ЗК)

Після закінчення цієї програми здобувач освіти буде здатен:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професії.

ЗК3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ЗК4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК5. Здатність до пошуку, оброблення та аналізу інформації.

Спеціальні (фахові) компетентності (ФК)

Після закінчення цієї програми здобувач буде здатен:

ФК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

ФК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

ФК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання (ПРН)

ПРН1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

4. Зміст навчальної дисципліни

Змістовний модуль 1. *Інструментальні засоби програмування МПС та основи апаратної безпеки*

Тема 1. Вступ. Види ПЗ МПС та поверхня атак IoT

Анотація: огляд класифікації мікропроцесорних систем (універсальні, вбудовані, SoC, мікроконтролери) та сфер їх застосування (IoT, «розумні» речі). Розглядається модель загроз для IoT-систем, поняття поверхні атаки та стандарти безпеки (OWASP IoT Top 10). Розглядаються інструментальні засоби розробника: редактори, компілятори, симулятори, програматори та інтегровані середовища (IDE).

Теми лекції №1: Класифікація МПС. Застосування МПС (моніторинг, управління, Internet of Things). Ключові вектори атак на вбудовані системи. Вимоги до кібербезпеки в IoT. Види програмного забезпечення: редактори, компілятори, інтерпретатори, симулятори. Інтегровані середовища розробки.

Самостійна робота здобувача: опрацювання матеріалу лекцій, формування питань до викладача. Вивчення класифікації та архітектури сучасних МПС та основних вразливостей "розумних" пристроїв.

Тема 2. Відкриті платформи. Екосистема Arduino та ризики використання Open Source Hardware

Анотація: вивчення концепції відкритих платформ на прикладі екосистеми Arduino. Розгляд формфакторів (Uno, Mega, Nano), питань сумісності (Shield), використання сторонніх бібліотек та методології швидкого прототипування. Аналіз ризиків використання сторонніх бібліотек (Supply Chain Attacks) та апаратних закладок.

Теми лекції №1: Відкриті платформи. Екосистема Arduino. Формфактор Uno, Mega, Nano, Mini. Сумісність за конструктивом, середовищем розробки, Shield та бібліотеками. Сторонні програмні засоби. Проблеми безпеки відкритих платформ. Клони апаратного забезпечення та ризики їх використання.

Самостійна робота здобувача: опрацювання матеріалу лекцій, формування питань до викладача. Огляд можливостей платформи Arduino та сумісних модулів , аналіз безпеки сторонніх бібліотек.

Тема 3. Інтегроване середовище розробки IDE Arduino та статичний аналіз коду

Анотація: детальний розгляд програмної моделі мікроконтролера (пам'ять, порти, таймери, інтерфейси) та роботи з ними в IDE Arduino.

Конфігурація середовища для різних ОС, робота з бібліотеками. Моделювання роботи МК. Основи безпечного завантаження (Secure Boot) та захисту прошивки від зчитування.

Теми лекції №1: Програмна модель МК у складі модулів Arduino. Внутрішні периферійні пристрої (цифрові/аналогові лінії, пам'ять, таймери, UART, SPI, I2C). Захист пам'яті мікроконтролера (Flash, EEPROM, RAM).

Теми лекції №2: Інтегроване середовище розробки IDE Arduino (Windows, Linux, Android, Web). Конфігурація та розширення бібліотек. Інструменти статичного аналізу коду для пошуку вразливостей.

Теми лабораторних занять №1: Розробка та налагодження програм для AVR-мікроконтролерів в середовищі Proteus. Аналіз потенційних вразливостей у коді.

Самостійна робота здобувача: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи №1, формування питань до викладача. Встановлення та налаштування IDE, вивчення методів захисту інтелектуальної власності у прошивках.

Тема 4. Управління простим введенням - виведенням через порти МК та фізична безпека

Анотація: вивчення методів керування портами введення-виведення (GPIO) для взаємодії з датчиками та виконавчими механізмами. Обробка переривань. Загрози фізичного доступу до портів. Атаки на інтерфейси вводу-виводу.

Теми лекції №1: Управління введенням-виведенням даних через порти МК. Зв’язок з датчиками та виконуючими пристроями. Використання переривань. Захист від дребезгу контактів як елемент надійності. Фізичні вектори атак через GPIO.

Теми лабораторних занять №1: Синтез цифрової системи керування на основі платформи Arduino з реалізацією програмного захисту від помилкових спрацювань.

Самостійна робота здобувача: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи №1, формування питань до викладача. Опрацювання матеріалу щодо електричного підключення периферії до портів МК.

Тема 5. Виведення символьної і графічної інформації на LCD / OLED / TFT / E-ink

Анотація: організація людино-машинного інтерфейсу. Робота з різними типами дисплеїв (LCD, OLED, TFT) через паралельні та послідовні інтерфейси.

Теми лекції №1: Типи дисплеїв (LCD, OLED, TFT, E-ink). Інтерфейси підключення. Бібліотеки для роботи з графікою та текстом.

Теми лабораторних занять №1: Розробка і налагодження програм виводу інформації з використанням символьних та графічних дисплеїв.

Самостійна робота здобувача: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи №1, формування питань до викладача. Вивчення бібліотек для роботи з дисплеями.

Тема 6. Програмування режимів роботи таймерів та забезпечення відмовостійкості

Анотація: теоретичні основи використання таймерів у задачах реального часу, формування часових інтервалів та генерація імпульсних послідовностей (PWM). Використання сторожового таймера (Watchdog Timer - WDT) для захисту від зависань та DoS-станів.

Теми лекції №1: Програмування режимів роботи таймерів. Задачі реального часу. Формування часових інтервалів та імпульсних послідовностей. Забезпечення безперервності роботи системи за допомогою WDT.

Теми лабораторних занять №1: Розробка і налагодження програм виводу інформації з використанням символьних та графічних дисплеїв.

Самостійна робота здобувача: опрацювання матеріалу лекцій, формування питань до викладача. Вивчення регістрів керування таймерами та налаштування Watchdog для підвищення надійності..

Модульний контроль 1

Вид контролю: тестовий модульний контроль.

Змістовний модуль 2. *Оптимізація та захист програмних засобів МПС*

Тема 7. Програмування асинхронного та синхронного обміну та перехоплення даних

Анотація: реалізація обміну даними між МК та зовнішніми пристроями. Програмування UART, SPI, I2C. Використання таймерів для синхронізації обміну. Аналіз загроз: сніффінг (Sniffing), атаки «Людина посередині» (MITM) на шинах UART/SPI/I2C.

Теми лекції №1: Програмування асинхронного та синхронного послідовного обміну МК з зовнішніми пристроями індикації, перетворення сигналів та збереження даних. Вразливості дротових інтерфейсів. Методи захисту цілісності даних при передачі.

Тема лабораторної роботи №1: Програмування режимів роботи таймерів-лічильників AVR мікроконтролерів.

Тема лабораторної роботи №2: Організація асинхронного обміну в AVR-мікроконтролерах. Дослідження передачі даних та можливості їх перехоплення.

Самостійна робота здобувача: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи №1 та №2, формування питань до викладача. Опрацювання протоколів передачі даних UART та методів їх аналізу за допомогою логічних аналізаторів.

Тема 8. Програмування аналогового інтерфейса МК та атаки на сенсори

Анотація: робота з АЦП та ЦАП. Підключення аналогових датчиків. Використання інтерфейсу SPI для роботи з зовнішніми АЦП/сенсорами. Проблема довіри до даних сенсорів. Спуфінг аналогових сигналів (Sensor Spoofing) та методи фільтрації.

Теми лекції №1: Програмування аналогового інтерфейсу МК з датчиками у задачах моніторингу і управління виконуючими та аудіо пристроями. Атаки на виконавчі механізми шляхом підміни даних датчиків.

Тема лабораторної роботи №1: Програмна підтримка обміну по послідовному периферійному інтерфейсу SPI.

Самостійна робота здобувача: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи №1, формування питань до викладача. Вивчення особливостей оцифрування сигналів та програмної фільтрації шумів як методу протидії атакам..

Тема 9. Швидка розробка додатків з використанням графічного програмування, хмарних сервісів та безпека хмарної інтеграції

Анотація: огляд сучасних методів Low-code/No-code розробки для IoT та інтеграція з хмарними платформами. Питання автентифікації пристроїв (Tokens, API Keys). Захист каналів керування через хмару.

Теми лекції №1: Швидка розробка додатків. Графічне програмування (Blockly, FLProg тощо). Інтеграція з хмарними сервісами. Безпека IoT-платформ. Використання MQTT over SSL/TLS.

Самостійна робота здобувача: опрацювання матеріалу лекцій, формування питань до викладача. Ознайомлення з хмарними платформами IoT (Blynk, AWS IoT, Arduino Cloud) та налаштування політик доступу до пристроїв.

Тема 10. Безпечне кодування та оптимізація програм

Анотація: методи оптимізації коду за розміром та швидкодією. Використання асемблерних вставок у С-код. Типові помилки при програмуванні на С (переповнення буфера, робота з пам'яттю) та методи їх уникнення.

Теми лекції №1: Оптимізація програм з використанням вставок на мові С та Асемблера. Робота з пам'яттю. Профілювання коду. Середовища розробки. Принципи безпечного кодування (Secure Coding) для вбудованих систем. Захист стеку.

Самостійна робота здобувача: опрацювання матеріалу лекцій, формування питань до викладача. Вивчення базових команд Асемблера для цільової архітектури та механізмів експлуатації вразливостей переповнення.

Тема 11. Програмування режимів енергозбереження МК та атаки виснаження

Анотація: стратегії зниження енергоспоживання у вбудованих системах. Режими сну (Sleep modes) та керування тактовою частотою. Атаки на виснаження батареї (Sleep Deprivation Attacks) та методи протидії.

Теми лекції №1: Управління активністю внутрішніх пристроїв МК. Режими сну (Idle, Power Down тощо). Управління тактовою частотою. Енергетична безпека IoT-пристроїв.

Самостійна робота здобувача: опрацювання матеріалу лекцій, формування питань до викладача. Аналіз методів енергозбереження в батарейних пристроях та оцінка впливу кібератак на час автономної роботи.

Тема 12. Елементи операційних систем реального часу у програмних засобах вбудованих системах та ізоляція процесів

Анотація: основи багатозадачності. Використання RTOS (FreeRTOS) на мікроконтролерах (STM32). API операційних систем. Забезпечення ізоляції задач у RTOS. Пріоритети та захист від інверсії пріоритетів.

Теми лекції №1: Управління багатозадачністю. Функції API. Малоресурсні операційні системи у комбінованих системах. Безпека в середовищі FreeRTOS. Розмежування доступу до ресурсів.

Тема лабораторної роботи №1: Розробка та налагодження програм для STM32.

Самостійна робота здобувача: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з індивідуальної лабораторної роботи №1, формування питань до викладача. Вивчення архітектури ARM Cortex-M та основ RTOS та механізмів захисту пам'яті (MPU) в RTOS.

Модульний контроль 2
Вид контролю: тестовий модульний контроль.

5. Індивідуальні завдання

Виконання індивідуальних завдань у межах дисципліни не передбачено.

6. Методи навчання

Лекції з елементами інтерактиву (пояснення з використанням презентацій, прикладів коду, міні-опитувань). *Лабораторні заняття* – розробка програм у середовищах програмування, розв'язування задач у командах та індивідуально. *Робота в малих групах* – колективний аналіз програмних фрагментів, обговорення рішень. *Використання системи онлайн-тестування*. *Самостійна робота* – індивідуальні завдання, робота з електронними матеріалами та онлайн-курсами. *Консультації* – індивідуальні та групові (очно або онлайн) для підтримки та корекції навчального процесу.

7. Методи контролю

Поточний контроль: опитування на практичних заняттях; завантаження у систему Mentor звіту лабораторних робіт за варіантом.

Модульний контроль: складання модульного контролю.

Підсумковий контроль: іспит.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Лабораторні заняття	0…7	3	0…21
Модульний контроль 1	0…20	1	0…20
Змістовий модуль 2			
Лабораторні заняття	0…7	4	0…28
Модульний контроль 2	0…21	1	0…21
Усього за семестр			**0…100**

Підсумкова модульна оцінка з навчальної дисципліни формується до початку семестрового контролю на основі суми балів модульних оцінок (кількість балів, отриманих здобувачем вищої освіти під час виконання модульного контролю) і результатів поточного контролю. За згодою здобувача, який набрав від 60 до 100 балів, підсумкова модульна оцінка може зараховуватися як контрольний захід – семестрова оцінка.

Здобувачі, які отримали менше 60 балів, атестуються оцінкою «незадовільно» і вважаються такими, що мають академічну заборгованість. Вони зобов'язані проходити процедуру контрольного заходу підсумкового (семестрового) контролю з метою ліквідації академічної заборгованості в період екзаменаційних сесій та канікул.

Під час складання контрольного заходу підсумкового (семестрового) контролю здобувач має можливість отримати максимум 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувача протягом семестру

Відмінно (90–100). Теоретичний зміст дисципліни (курсу) засвоєний здобувачем повністю, необхідні практичні навички роботи з навчальним матеріалом повністю сформовані, усі навчальні завдання, що передбачені силабусом, виконані в повному обсязі, робота без помилок або з однією незначною помилкою.

Добре (75–89). Теоретичний зміст курсу засвоєний повністю, практичні навички роботи з навчальним матеріалом в основному сформовані, усі навчальні завдання, що передбачені силабусом, виконані, якість виконання жодного з них не оцінено мінімальною кількістю балів, деякі види завдань виконані з помилками, робота має декілька незначних помилок або одну-дві значні помилки.

Задовільно (60–74). Теоретичний зміст дисципліни засвоєний частково, деякі практичні навички роботи з навчальним матеріалом не сформовані, частина передбачених силабусом завдань не виконана або якість виконання деяких з них оцінено кількістю балів, близькою до мінімальної, відповідь (в усній або письмовій формі) фрагментарна, непослідовна.

Незадовільно (0-59). Здобувач має фрагментарні знання, що базуються на попередньому досвіді, але не здатен формулювати визначення понять, класифікаційні критерії та тлумачити їхній зміст, не може використовувати знання під час вирішення практичних завдань.

Відповідно до п. 3.2. Положення про рейтингове оцінювання досягнень студентів у Національному аерокосмічному університеті «Харківський авіаційний інститут» здобувачу можуть призначатися бали за інші активності, пов'язані з навчальною дисципліною, які нараховуються та можуть бути враховані в загальній оцінці за семестр. Бали, зокрема, можуть призначатися за такі активності, пов'язані з навчальною дисципліною, як:

- участь у науковому комунікативному заході (конференції, семінарі, круглому столі тощо) із написанням тез наукової доповіді за предметом навчальної дисципліни (20 балів);
- участь у другому турі Всеукраїнської олімпіади відповідного напряму (20 балів);
- участь (прослуховування) не менше у 5 вебінарах, пов'язаних з навчальною дисципліною (3-15 балів);
- участь у тренінгу, пов'язаному з навчальною дисципліною (15 балів);
- проходження онлайн-курсу, пов'язаного з навчальною дисципліною (20 балів);
- участь та отримання рейтингового місця в тематично пов'язаному із предметом навчальної дисципліни студентському конкурсі (30 балів);
- розробленні та створення дидактичного матеріалу за тематикою предмета навчальної дисципліни (15 балів) (підтвердження – наявність дидактичного матеріалу);
- проведення правоосвітнього заходу з учнями шкіл та інших навчальних закладів за тематикою навчальної дисципліни (20 балів);
- написання реферату /презентації, доповіді (5 балів);
- інші активності, пов'язані з навчальною дисципліною, за попереднім погодженням із науково-педагогічним працівником, який викладає навчальну дисципліну.

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Здобувачі, які за певних обставин не можуть регулярно відвідувати практичні заняття, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання. Здобувачі, які станом на початок екзаменаційної сесії мають понад 70 % невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Дотримання вимог академічної доброчесності. Під час вивчення навчальної дисципліни здобувачі мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності

в лабораторній роботі здобувача є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману. Під час виконання індивідуальної самостійної роботи до захисту допускаються роботи, які містять не менше 60 % оригінального тексту при перевірці на плагіат.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення та інформаційні ресурси

1. Mentor KHAI. Сайт дистанційного навчання Національного аерокосмічного університету "XAI" . URL: https://mentor.khai.edu/course/view.php?id=1614.
2. Проектування та аналіз електричних схем в програмному середовищі Proteus VSM. Методичні вказівки до самостійної роботи студентів курсу "Проектування мікропроцесорних систем керування технологічними процесами". Медвідь В.Р., Пісьціо В.П., Тернопіль: ТНТУ, 2018 - 26 с. URL: http://elartu.tntu.edu.ua/bitstream/lib/26397/1/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%BA%D0%B0%20Proteus%202018_v2.pdf.
3. Методичні вказівки до лабораторних робіт з дисципліни «Електротехніка та електроніка» для студентів спеціальності 122 «Комп'ютерні науки і інформаційні технології» денної форм навчання / Укл.: А.В. Пархоменко, О.М. Гладкова. – Запоріжжя: ЗНТУ, 2016. – 41 с. URL: http://eir.zntu.edu.ua/bitstream/123456789/840/1/Laboratory_classes_discipline_Electrical_engineering.pdf
4. Посібник користувача по Proteus. URL: http://avr.ru/tools/proteus/guide

11. Рекомендована література

Базова

1. Шпак Ю.А. Програмування мовою С для та мікроконтролерів. 2-е видання. – Київ, МК Прес, 2011 – 544с.
2. Апаратна частина платформи Arduino - https://dspace.duet.edu.ua/jspui/bitstream/123456789/849/1/НМП%20Arduino.pdf
3. Ardublock – графічна мова програмування для Arduino. - https://bluebeehive.eu/wp-content/uploads/2021/10/ArduBlock_tutorial.pdf
4. Bluetooth модуль HC-06 підключення до Arduino. Керування пристроями з телефону. - http://asac.kpi.ua/article/view/292238
5. Проекти з Arduino. - http://arduino-diy.com/arduino_proekty-0
6. Prohrammyrovanye arduyno. *Arduyno v Ukrayne*. URL: https://doc.arduino.ua/ru/prog.
7. *Biudzhet uchasti | Hromadskyi Proekt Boiarska hromada*. URL: https://gb.mistoboyarka.gov.ua/files/project/1632/documents/15120646387546_15120630653179 96.pdf.

Допоміжна

1. Троелсен Е. Мова програмування C# і платформа .NET 2.0. - М.: Вільямс, 2007. - 1168 с.

2. Voss W. Controller area network prototyping with arduino. Copperhill Media Corporation, 2014. 44 p.

3. Blum J. Exploring arduino: tools and techniques for engineering wizardry. Wiley & Sons, Incorporated, John, 2013. 384 p.

4. Smart technology / ed. by F. Torres Guerrero et al. Cham : Springer International Publishing, 2018. URL: https://doi.org/10.1007/978-3-319-73323-4.

5. Business, human rights, technology, and transitional justice in latin america / ed. by S. Smart. Cham : Springer Nature Switzerland, 2025. URL: https://doi.org/10.1007/978-3-031-89828-0

6. Knopf G. K., Bassi A. S. Smart biosensor technology. Taylor & Francis Group, 2018. 577 p.

7. Paramanik S., Sarker K. Smart grid technology with smart devices and smart technology for smart cities. Cambridge Scholars Publisher, 2019.

8. Technology for smart futures / ed. by M. Dastbaz, H. Arabnia, B. Akhgar. Cham : Springer International Publishing, 2018. URL: https://doi.org/10.1007/978-3-319-60137-3.

9. Kovar D. Internet of things applications : introduction to internet of things: industrial internet of things. Independently Published, 2021.

10. Helman T. Types of internet of things : define internet of things: internet of things examples. Independently Published, 2021.

11. Friess P., Vermesan O. Internet of things. New York : River Publishers, 2022. URL: https://doi.org/10.1201/9781003338659.

12. Інформаційні ресурси

1. “Chto takoe IoT? – Opysanye Ynterneta veshchei – AWS.” Amazon Web Services, Inc. [Online]. Available: https://aws.amazon.com/ru/what-is/iot

2. IBM. “What is the internet of things (iot)? | IBM.” IBM. [Online]. Available: https://www.ibm.com/think/topics/internet-of-things

3. “Internet of things, iot.” IT-Enterprise — tsyfrova transformatsiia biznes-protsesiv, ERP| it.ua. [Online]. Available: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot

4. “The role of iot in smart cities.” Asimily. [Online]. Available: https://asimily.com/blog/the-role-of-iot-in-smart-cities

5. “Smart city iot: Benefits & use cases.” Sand Technologies. [Online]. Available: https://www.sandtech.com/insight/smart-city-iot-benefits-use-cases

6. “The relationship between IoT and smart cities.” Telefónica. [Online]. Available: https://www.telefonica.com/en/communication-room/blog/the-relationship-between-iot-and-smart-cities

7. A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier, and S. Zailani, “The big picture on the internet of things and the smart city: A review of what we know and what we need to know,” *Internet of Things*, vol. 19, p. 100565, Aug. 2022. Accessed: Nov. 22, 2025. [Online]. Available: https://doi.org/10.1016/j.iot.2022.100565

8. “Internet of things for smart cities.” IEEE Xplore. [Online]. Available: https://ieeexplore.ieee.org/document/6740844

9. J. Locke. “IoT smart city applications (2025).” IIoT Devices and Services for M2M Networking | Digi International. [Online]. Available: https://www.digi.com/blog/post/iot-smart-city-applications

10. M. Zaman, N. Puryear, S. Abdelwahed, and N. Zohrabi, “A review of iot-based smart city development and management,” *Smart Cities*, vol. 7, no. 3, pp. 1462–1500, Jun. 2024. Accessed: Nov. 22, 2025. [Online]. Available: https://doi.org/10.3390/smartcities7030061

11. Smart city security: protecting critical infrastructure with iot - device authority. *Device Authority*. URL: https://deviceauthority.com/smart-city-security-protecting-critical-infrastructure-with-iot.

12. Houichi M., Jaidi F., Bouhoula A. Cyber security within smart cities: a comprehensive study and a novel intrusion detection-based approach. *Computers, materials & continua*. 2024. P. 1–10. URL: https://doi.org/10.32604/cmc.2024.054007 .

13. Cybersecurity R. U. OT \& iot cybersecurity for smart cities – ensuring resilience in the digital urban ecosystem. URL: https://medium.com/@RocketMeUpCybersecurity/ot-iot-cybersecurity-for-smart-cities-ensuring-resilience-in-the-digital-urban-ecosystem-29c41cae5832.

14. Moradeyo A., Abike O., Samuel A. H. Smart cities' cybersecurity and iot: challenges and future research directions. 2021. URL: https://www.researchgate.net/publication/390303077_Smart_Cities'_Cybersecurity_and_IoT_Challenges_and_Future_Research_Directions .

15. Smart cities and internet of things (iot): a review of emerging technologies and challenges / P. A. Adepoju et al. *International journal of research and innovation in social science*. 2025. Vol. IX, no. I. P. 1536–1549. URL: https://doi.org/10.47772/ijriss.2025.9010127.

16. Why cybersecurity is a top priority in IoT and smart cities. *Silicon Republic*. URL: https://www.siliconrepublic.com/enterprise/ul-iot-ioe-smart-cities-cybersecurity.