Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Кіберфізична охоронна система будинку на базі Arduino
Назва теми

КвРКІ 210249.21.02.40 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент IV курсу, група КІ2-21-2 _____ Іван ТИМЧУК
Підпис Ініціали, прізвище

Керівник _____ Тетяна КИСІЛЬ
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ Тетяна КИСІЛЬ
Підпис, дата Ініціали, прізвище

До захисту допускаю:
зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Ольга ПАВЛОВА
Підпис Ініціали, прізвище

«12» червня 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 10 " 01 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Івану ТИМЧУКУ

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Кіберфізична охоронна система будинку на базі Arduino

Керівник проекту (роботи) Тетяна КИСІЛЬ, к.ф-м.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 07.02.2025 р. № 23

2. Строк подання студентом проекту (роботи) на кафедру 01.06.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Кіберфізична охоронна система будинку на базі Arduino

Проєктування охоронна система будинку з використанням модулів Arduino

Програмно-апаратна реалізація Кіберфізичної охоронної системи будинку з можливостями моніторингу на базі Arduino

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Блок-схема роботи пз

Схема з'єднання компонентів пз

Монтажна схема

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Тетяна КИСІЛЬ, доцент кафедри КІІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІІС		

7. Дата видачі завдання «10» 01 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітки
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2025	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2025	виконан
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2025	виконан
4	Робота над розділом 2 – вибір компонентів для проєктування охороної системи будинку на базі Arduino	01.04.2025	виконан
5	Робота над розділом 3 – проєктування охороної системи будинку на базі Arduino	29.04.2025	виконан
6	Оформлення пояснювальної записки згідно вимог	25.05.2025	виконан
7	Попередній захист ВКР	26.05.2025	виконан
8	Захист ВКР на засіданні ЕК	Червень 2025 року	

Студент _____ Іван ТИМЧУК
Підпис Ініціали, прізвище

Керівник роботи _____ Тетяна КИСІЛЬ
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 210249.21.01.40 ПЗ	Пояснювальна записка	67		
			Графічні матеріали			
2		КвРКІ 210249.21.01.40 1	Блок-Схема роботи ПЗ	1		
3		КвРКІ 210249.21.01.40 Е2	Схема з'єднання -	1		
			компонентів ПЗ			
4		КвРКІ 210249.21.01.40 Е8\3	Монтажна схема	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 210249.21.02.40 ПЗ		
Розробив		Тимчук			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Кисіль		12.06.25		У	1	1
Н. контр.		Кисіль		12.06.25		ХНУ, КІ2-21-2		
Затв.		Павлова		12.06.25				

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Кіберфізична охоронна система будинку на базі Arduino».

Автор роботи: Іван ТИМЧУК.

Керівник роботи: Кисіль Тетяна Миколаївна.

Пояснювальна записка: 67 с., 28 рис., 3 дод., 45 джерел.

Графічна частина: 3 креслення.

ОХОРОННА СИСТЕМА, КІБЕРФІЗИЧНА СИСТЕМА, ЗАХИСТ БУДИНКУ, МОНІТОРИНГ, ARDUINO.

Метою дипломної роботи є визначення умов та особливостей застосування охоронних систем, адаптація її до житлового будинку та забезпечення надійної активної системи моніторингу приміщення з особливостями абгрейду.

Об’єктом дослідження є дієві охоронні системи для моніторингу об'єктів.

Предметом дослідження є створення бюджетної версії охоронної системи з можливістю модифікації.

Під час проведення даного дослідження був використаний метод систематичного огляду літератури та діючих пристроїв для аналізу предметної області та створенню компактної системи для встановлення.

Підпис студента

30.05.2025

Дата

ЗМІСТ

ВСТУП

Забезпечення безпеки об’єктів різного призначення є однією з ключових задач у сучасному світі. Збільшення ризиків, пов’язаних із несанкціонованим доступом, фізичними загрозами чи технічними збоями, вимагає розробки ефективних і економічно доцільних рішень для захисту інфраструктури. У цьому контексті мікроконтролерні платформи, зокрема Arduino, відкривають нові можливості для створення гнучких і доступних систем моніторингу та охорони, які можуть бути адаптовані до різноманітних умов і потреб.

Метою дослідження є аналіз і розробка системи безпеки на базі платформи Arduino з урахуванням реальних вимог до захисту об’єктів. Робота передбачає вивчення принципів проектування таких систем, їхньої апаратної та програмної реалізації, а також оцінку їхньої ефективності в умовах експлуатації на підприємстві з розвиненою інфраструктурою і високими стандартами безпеки.

У процесі дослідження буде розглянуто практичні аспекти створення охоронних систем, включаючи роботу з електронними компонентами, такими як датчики руху, температури чи модулі зв’язку, а також програмування мікроконтролерів для обробки сигналів і реалізації сценаріїв реагування. Передбачається створення прототипу системи безпеки, який може включати функції автоматичного сповіщення, локального моніторингу чи збереження даних про події. Особлива увага приділятиметься забезпеченню надійності системи, її енергоефективності та можливості інтеграції з іншими технологіями.

Дослідження сприятиме поглибленню знань у сфері електроніки, програмування та інформаційних технологій, а також формуванню навичок роботи з апаратними платформами та аналізу реальних задач у галузі безпеки. Отриманий досвід стане основою для подальшого розвитку професійних компетенцій у проектуванні інженерних рішень, що відповідають сучасним вимогам до захисту об’єктів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖУВАНОЇ ПРОБЛЕМИ

1.1 Аналіз предметної області і виявлення наявних проблем кіберфізичних охоронних системи будинку на базі Arduino

Системи безпеки є невід'ємною складовою сучасної інженерної інфраструктури. Вони відіграють ключову роль у захисті житлових, офісних, промислових і стратегічно важливих об'єктів. Їх основна функція - забезпечити надійний захист від зовнішніх і внутрішніх загроз, таких як вторгнення, пожежа, затоплення, витік газу або технічна несправність. У цьому контексті питання ефективності, автономності та доступності систем безпеки є надзвичайно важливими.

За останні десятиліття технології в цій сфері зазнали значної трансформації. На зміну традиційним сигналізаціям з локалізованими голосовими повідомленнями поступово прийшли інтелектуальні системи безпеки, здатні взаємодіяти з користувачем в режимі реального часу, передавати інформацію через інтернет та інтегруватися з мобільними додатками і системами «розумного будинку». Сучасні комерційні рішення, такі як Ajax Systems, Paradox, Eldes та інші, пропонують повністю бездротові рішення з централізованим управлінням, високою чутливістю датчиків і безпечним зв'язком.

Незважаючи на значний прогрес у розвитку систем безпеки, все ще існують певні бар'єри для їх широкого впровадження, особливо в приватному секторі та малому бізнесі. Ці бар'єри включають високу вартість високоякісного обладнання, складність адаптації до нестандартних архітектур, той факт, що багато платформ є технічно закритими і залежать від постійного підключення до Інтернету. Крім того, деякі системи працюють через хмарні сервіси, що потенційно створює ризики кібербезпеки, а в деяких регіонах бракує фахівців для встановлення таких систем.

У цьому контексті мікроконтролерні платформи, такі як Arduino, пропонують нові можливості для розробки доступних, адаптивних та ефективних

систем безпеки. Arduino – це відкрита програмно-апаратна система, яка дозволяє створювати інтерактивні пристрої з високим ступенем кастомізації. Завдяки гнучкій архітектурі Arduino дозволяє реалізовувати системи безпеки, які працюють автономно, реагують на певні події, передають сигнали тривоги і можуть бути налаштовані відповідно до індивідуальних вимог користувача.

Arduino дозволяє створити модульну систему безпеки, яка може взаємодіяти з користувачем через простий веб-інтерфейс або мобільний додаток. Завдяки відкритому вихідному коду систему можна легко адаптувати до конкретних умов, реалізувати кастомні сценарії реагування, інтегрувати в інші системи управління приміщеннями і, що найголовніше, знизити витрати на впровадження, що робить її привабливою як для освітніх проектів, так і для використання в реальному світі.

Таким чином, використання Arduino як основи для побудови системи безпеки не тільки оптимізує витрати, але і дозволяє створити гнучке, надійне і масштабоване рішення, яке може бути ефективно використано для різних цілей в сфері безпеки.

1.2 Початок заснування систем безпеки та їх прогрес у сучасності

Сучасні системи безпеки значно еволюціонували порівняно з традиційними сигналізаціями, які обмежувалися активацією сирени при відчиненні дверей чи вікон. Сьогодні це комплексні електронні рішення, об’єднані в єдину мережу, що забезпечують не лише виявлення порушень, а й оперативне інформування користувачів, передачу даних до охоронних компаній і навіть превентивні заходи. Такі системи здатні автоматично активувати звукові чи світлові сигнали, блокувати доступ до приміщення, надсилати сповіщення родичам чи спеціальним службам, а також зберігати записи подій для подальшого аналізу. Завдяки інтеграції з технологіями «розумного будинку», сучасні системи безпеки стали частиною ширшої екосистеми, що поєднує функції захисту, автоматизації та комфорту.

Історія розвитку систем безпеки бере початок у середині 19 століття. У 1853 році американець Август Поуп зображений на рисунок 1.1 винайшов електромеханічну сигналізацію, яка використовувала електромагнітний дзвінок для сповіщення про відчинення дверей або вікон. Цей пристрій став основою для подальшого розвитку охоронних технологій. У 1858 році Едвін Холмс удосконалив ідею Поупа, запустивши сигналізацію в серійне виробництво, що поклало початок комерційним охоронним послугам. Наприкінці 19 століття, із поширенням телефонного зв'язку, сигналізації отримали можливість передавати тривожні сигнали на відстань, що значно розширило їхнє застосування. У 1940–1950-х роках з'явилися перші системи відеоспостереження, які використовувалися переважно в банківському секторі та державних установах через високу вартість і складність обладнання.

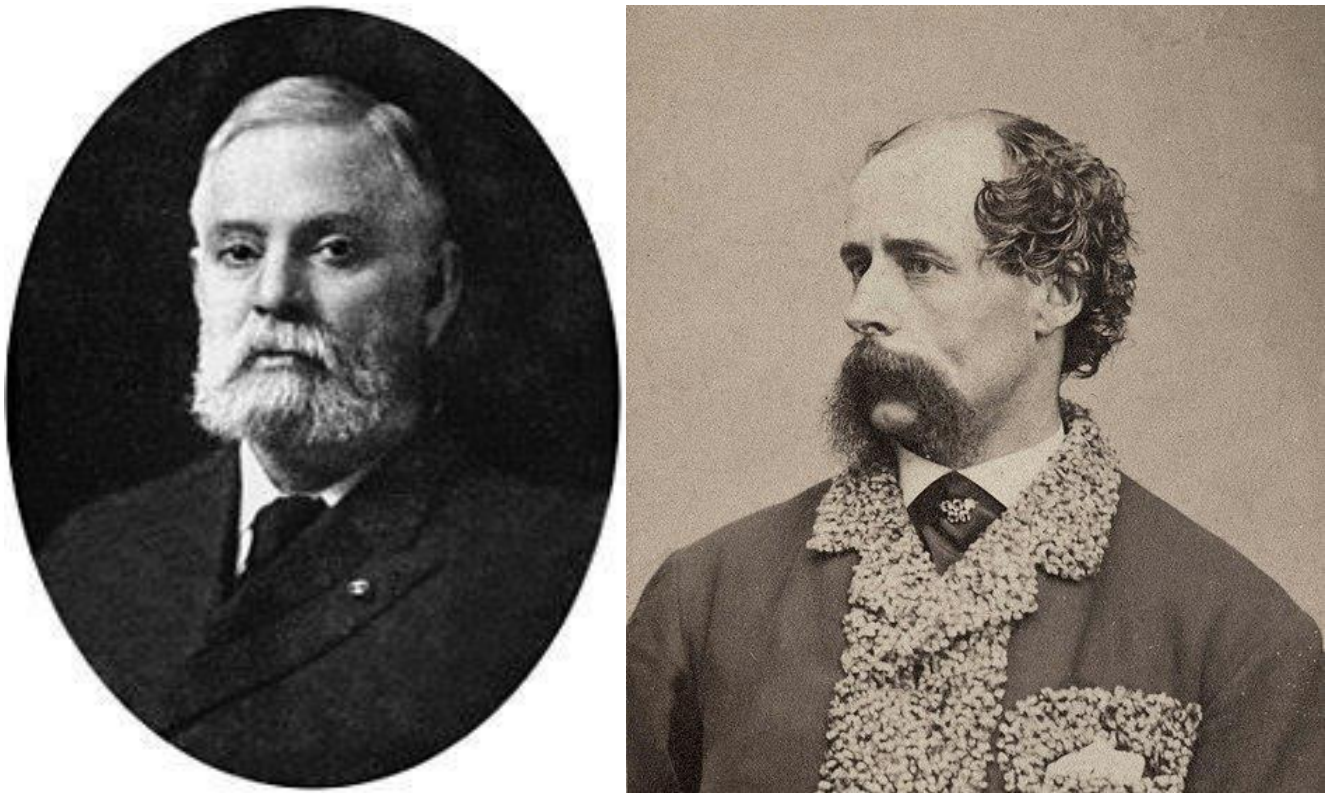


Рисунок 1.1 – Август Поуп та Едвін Холмс

Значний прогрес у розвитку систем безпеки відбувся в 1970–1980-х роках, коли мікроелектроніка дозволила створювати цифрові пристрої з елементами

логічного керування. У цей період почали застосовувати датчики руху на основі інфрачервоних і ультразвукових технологій, а також перші бездротові системи, що використовували радіозв'язок. Це зробило встановлення охоронних систем простішим і доступнішим, усунувши потребу в складному прокладанні кабелів. Наступним важливим етапом стало впровадження GSM-зв'язку та інтернет-технологій у 1990-х роках. Завдяки цьому користувачі отримали можливість отримувати сповіщення через SMS, електронну пошту чи спеціалізовані мобільні додатки, незалежно від їхнього місця перебування.

Починаючи з 2010-х років, системи безпеки стали невід'ємною частиною концепції «розумного будинку». Вони інтегруються з іншими пристроями, такими як розумні розетки, термостати, освітлення, голосові асистенти та камери відеоспостереження, створюючи єдину екосистему для керування домом. Сучасні системи дозволяють користувачам дистанційно контролювати стан об'єктів, отримувати відеопотік у реальному часі, налаштовувати сценарії автоматизації (наприклад, увімкнення світла при виявленні руху) і навіть використовувати штучний інтелект для аналізу подій, наприклад, розпізнавання облич чи виявлення нетипової поведінки.

1.3 Сучасні компанії та застосування їх продукту

Українська компанія Ajax Systems, заснована в 2011 році в Києві, стала одним із лідерів на міжнародному ринку систем безпеки. Завдяки поєднанню інноваційних технологій, високої надійності та естетичного дизайну, продукція Ajax здобула визнання в багатьох країнах. Основна ідея бренду полягає в розробці бездротових охоронних систем, які легко встановлюються, гармонійно вписуються в будь-який інтер'єр і забезпечують комплексний захист. Системи Ajax базуються на централі (хабі), яка координує роботу периферійних пристроїв через захищений радіопротокол Jeweller. Цей протокол гарантує стабільний

зв’язок на відстані до 2 км, захист від перехоплення сигналу та енергоефективність, що дозволяє пристроям працювати від батарейок до 7 років.

Серед найпопулярніших пристроїв Ajax варто виділити Hub 2(Рисунок 1.2), який підтримує фотофіксацію тривог для візуального підтвердження подій, MotionProtect – бездротовий датчик руху з імунітетом до хибних спрацьовувань через рух тварин, DoorProtect – компактний датчик відчинення дверей і вікон, FireProtect – комбінований пожежний датчик, що реагує на дим і підвищення температури, а також StreetSiren – вуличну сирену для гучного сповіщення про загрозу. Усі ці пристрої інтегруються з мобільним застосунком Ajax, який дозволяє користувачам контролювати систему в реальному часі, отримувати push-сповіщення, переглядати історію подій і налаштовувати параметри роботи. Крім того, Ajax підтримує підключення до систем «розумного будинку» та сумісність із камерами відеоспостереження інших виробників, що робить її універсальним рішенням для захисту як приватних, так і комерційних об’єктів.

Розвиток систем безпеки, від простих електромеханічних пристроїв до складних цифрових екосистем, демонструє, як технологічний прогрес змінює підходи до захисту майна та людей. Сучасні рішення, такі як продукція Ajax Systems, поєднують простоту використання, високу надійність і гнучкість, що дозволяє адаптувати їх до різноманітних сценаріїв – від невеликих квартир до великих промислових об’єктів. У контексті роботи над охоронними системами на базі платформ, таких як Arduino, вивчення досвіду компаній на кшталт Ajax може слугувати джерелом ідей для створення доступних і ефективних прототипів, які відповідають сучасним вимогам безпеки.

Компанія Paradox Security Systems, заснована в 1989 році в Канаді, здобула репутацію одного з провідних світових виробників систем безпеки, які вирізняються надійністю, гнучкістю та адаптивністю до різноманітних потреб користувачів. Спочатку спеціалізуючись на розробці дротових сигналізацій, компанія поступово розширила свій асортимент, додавши бездротові рішення, інтегровані системи відеоспостереження та модулі для взаємодії з технологіями

«розумного будинку». Таке поєднання дозволяє Paradox пропонувати комплексні рішення для захисту як приватних, так і комерційних об’єктів, включаючи склади, великі житлові комплекси, офісні центри та промислові підприємства.

Рисунок 1.2 – Приклад пристрою Ajax - Hub 2[16]

Системи Paradox вирізняються модульною структурою, що забезпечує високу масштабність і можливість адаптації до об’єктів різної складності. Вони підтримують як дротові, так і бездротові компоненти, що дозволяє гнучко проектувати систему залежно від архітектури приміщення, вимог безпеки та бюджету. Наприклад, користувачі можуть комбінувати датчики руху, магнітоконтактні датчики відчинення дверей чи вікон, а також пристрої для зовнішнього спостереження, створюючи багаторівневу систему захисту. Крім того, Paradox пропонує можливість інтеграції з зовнішніми охоронними службами через підтримку сучасних протоколів зв’язку, таких як GSM, IP-мережі та хмарні сервіси, що забезпечує оперативне сповіщення про тривожні події.

Серед найпоширеніших продуктів компанії варто виділити центральні панелі керування MG5050 і EVO192. MG5050 (Рисунок 1.3) – це гібридна панель, яка підтримує до 32 зон безпеки, що робить її оптимальним вибором для середніх

і великих об’єктів. EVO192, своєю чергою, розрахована на складніші системи, дозволяючи організувати до 192 зон і підключати до 254 модулів, що ідеально підходить для масштабних комерційних проєктів. Обидві панелі сумісні з широким набором периферійних пристроїв і забезпечують гнучке налаштування логіки роботи системи.

До популярних компонентів Paradox також належать бездротовий датчик руху PMD2P, який оснащений технологією захисту від хибних спрацьовувань, викликаних рухом тварин вагою до 18 кг. Цей датчик використовує подвійний інфрачервоний сенсор для точного виявлення руху, що підвищує надійність системи. Вуличний датчик DG85 призначений для роботи в складних погодних умовах, таких як дощ, сніг чи сильний вітер, і має посилений захист від зовнішніх впливів, що робить його ефективним для охорони периметру. Тривожна кнопка REM101, компактна й проста у використанні, дозволяє миттєво активувати сигнал тривоги в екстрених ситуаціях, що особливо важливо для об’єктів із високими вимогами до безпеки персоналу.

Додатковою перевагою систем Paradox є їхня сумісність із мобільними застосунками, такими як Insite Gold, які дозволяють користувачам дистанційно контролювати стан системи, отримувати push-сповіщення про події, керувати зонами безпеки та переглядати журнали тривог. Інтеграція з камерами відеоспостереження та іншими пристроями автоматизації підвищує функціональність систем, роблячи їх частиною сучасних екосистем «розумного будинку». Завдяки цьому Paradox забезпечує не лише захист, а й зручність у повсякденному використанні.

Розробка систем безпеки на базі платформ, таких як Arduino, може черпати натхнення з підходів компаній на кшталт Paradox. Зокрема, модульна структура, підтримка різноманітних датчиків і акцент на надійність зв’язку є важливими принципами, які можна адаптувати для створення прототипів охоронних систем. Вивчення досвіду Paradox дозволяє краще зрозуміти сучасні вимоги до безпеки, включаючи енергоефективність, захист від збоїв і зручність керування, що є

цінним для практичної реалізації проєктів у сфері інформаційних технологій та інженерії.

Рисунок 1.3 – Центральні панелі MG5050 і EVO192 [17]

Компанія Eldes, заснована в Литві у 2005 році, спеціалізується на розробці систем безпеки, які поєднують простоту використання, доступність і ефективність. Основний акцент бренду зосереджений на рішеннях для приватних будинків, квартир і малого бізнесу, де важливими є легкість встановлення, гнучке налаштування та надійність роботи. Продукція Eldes вирізняється універсальністю, дозволяючи користувачам адаптувати системи до специфічних потреб, таких як захист від вторгнень, моніторинг приміщень чи інтеграція з автоматизованими системами. Завдяки підтримці різних типів зв'язку – GSM, Wi-Fi та Ethernet – системи Eldes забезпечують стабільну роботу навіть у разі перебоїв з інтернетом або електроживленням.

Системи безпеки Eldes розроблені з урахуванням потреб сучасних користувачів. Вони дозволяють здійснювати налаштування та керування через інтуїтивно зрозумілі мобільні додатки, що значно спрощує експлуатацію. Крім того, пристрої підтримують підключення до центральних станцій моніторингу охоронних компаній, що забезпечує оперативне реагування на тривожні події. Важливою особливістю є сумісність із платформами «розумного будинку», що

дозволяє інтегрувати системи Eldes із пристроями для керування освітленням, клімат-контролем чи іншими автоматизованими функціями. Такий підхід робить продукцію бренду привабливою для користувачів, які прагнуть поєднати безпеку з комфортом.

Серед найпопулярніших продуктів Eldes варто виокремити універсальну центральну панель ESIM384 (Рисунок 1.4), яка підтримує до 144 зон безпеки та дозволяє підключати як дротові, так і бездротові датчики. Ця панель забезпечує гнучке налаштування сценаріїв роботи, наприклад, активацію сирени чи надсилання сповіщень через SMS чи push-повідомлення. Бездротовий датчик спрацьовування EWD3 призначений для виявлення відчинення дверей або вікон і характеризується компактним дизайном та тривалим терміном служби батареї. Портативний охоронний модуль EPIR3 поєднує функції датчика руху та централі, що робить його зручним рішенням для невеликих об’єктів, таких як гаражі чи офіси. Автономна сигналізація PITBULL Alarm PRO є готовим до використання комплектом, який включає датчик руху, сирену та GSM-модуль, забезпечуючи швидке розгортання системи без складного монтажу. Сучасна бездротова клавіатура EWKB5 дозволяє зручно активувати чи деактивувати систему, а також налаштовувати окремі функції завдяки сенсорному інтерфейсу та підтримці персоналізованих кодів доступу.

Продукція Eldes розроблена з акцентом на енергоефективність і надійність. Наприклад, більшість пристроїв здатні працювати від батарей протягом кількох років, а вбудовані механізми захисту від перехоплення сигналу забезпечують безпеку зв’язку. Крім того, системи підтримують резервні канали зв’язку, що дозволяє зберігати функціональність у разі збоїв основного підключення. Такі характеристики роблять Eldes популярним вибором для користувачів, які шукають баланс між вартістю, простотою та якістю.

У контексті розробки охоронних систем на базі мікроконтролерних платформ, таких як Arduino, досвід компанії Eldes може слугувати прикладом ефективного поєднання апаратних і програмних рішень. Зокрема, акцент на

модульності, підтримці різних каналів зв’язку та зручності керування є важливими аспектами, які можна врахувати під час створення прототипів. Вивчення підходів Eldes сприяє кращому розумінню сучасних вимог до систем безпеки, включаючи аспекти енергоефективності, захисту даних і адаптивності до потреб користувачів, що є цінним для практичних проєктів у сфері інформаційних технологій та інженерії.

Рисунок 1.4 – Універсальна централь ESIM384[19]

Поряд із комерційними системами безпеки дедалі більшої популярності набувають відкриті апаратні платформи, серед яких Arduino вирізняється своєю доступністю та універсальністю. Ця технологія була створена в Італії у 2005 році групою розробників на чолі з Массімо Банзі з метою забезпечити студентів і викладачів технічних спеціальностей недорогою альтернативою складним і дорогим мікроконтролерам. Назва Arduino походить від невеликого пабу в Івреа, де розробники часто обговорювали свої ідеї. Завдяки відкритому вихідному коду, великій міжнародній спільноті ентузіастів і простоті використання платформа швидко здобула популярність у всьому світі. Сьогодні Arduino застосовується в

тисячах проєктів, від автоматизації побутових пристроїв до створення складних систем безпеки та моніторингу.

Основна перевага Arduino полягає в її модульній конструкції та гнучкості, що дозволяє створювати системи, адаптовані до специфічних потреб користувачів. До мікроконтролерних плат Arduino можна підключати широкий спектр компонентів, таких як датчики руху, температури, диму, камери, модулі зв'язку (Wi-Fi, GSM, Bluetooth), реле для керування зовнішніми пристроями чи навіть дисплеї для відображення інформації. Програмування платформи здійснюється через середовище Arduino IDE, яке використовує спрощену версію мови C/C++ і підтримує численні бібліотеки для роботи з різними модулями. Це дозволяє навіть початківцям швидко розробляти власні сценарії реагування на події, наприклад, активацію сирени при виявленні руху чи надсилання сповіщень через SMS або інтернет.

Системи безпеки, створені на базі Arduino, вирізняються економічністю та можливістю кастомізації (Рисунок 1.5). Наприклад, за допомогою плати Arduino Uno чи Mega, кількох датчиків і модуля зв'язку можна створити автономну охоронну систему, яка виявлятиме вторгнення, записуватиме відеофрагменти чи надсилатиме повідомлення власнику. Такі системи можуть працювати незалежно від зовнішніх серверів, зберігаючи дані на локальних носіях, наприклад, SD-картах, або інтегруватися в локальні мережі для віддаленого доступу через мобільні додатки чи вебінтерфейси. Крім того, Arduino дозволяє реалізувати складніші функції, такі як аналіз даних із кількох датчиків для зменшення хибних спрацьовувань або інтеграція з платформами «розумного будинку» для автоматизації сценаріїв, наприклад, увімкнення освітлення при виявленні руху.

Гнучкість платформи робить її привабливою для широкого кола застосувань. Для студентських і хобі-проєктів Arduino є ідеальним інструментом завдяки низькій вартості та великій кількості навчальних ресурсів, доступних у спільноті. У сфері малого бізнесу чи індивідуальних технічних об'єктів, таких як склади, майстерні чи приватні будинки, системи на базі Arduino дозволяють

створювати недорогі рішення, які відповідають нестандартним вимогам, наприклад, моніторинг віддалених об’єктів без постійного підключення до інтернету. Водночас відкритість платформи сприяє експериментам і розробці прототипів, які можуть стати основою для комерційних продуктів.

Рисунок 1.5 – Приклад охороної системи на базі «Arduino»

У контексті розробки охоронних систем досвід використання Arduino є цінним для вивчення принципів роботи апаратних і програмних компонентів. Платформа дозволяє поглибити розуміння таких аспектів, як обробка сигналів від датчиків, організація зв’язку через різні протоколи, оптимізація енергоспоживання та створення надійних систем із мінімальними затратами. Ці знання є актуальними для створення прототипів, які можуть конкурувати з комерційними рішеннями в певних нішах, а також для підготовки фахівців у галузі інформаційних технологій та інженерії. Таким чином, Arduino залишається

не лише інструментом для навчання, а й платформою для реалізації практичних проєктів, що відповідають сучасним викликам у сфері безпеки.

1.4 Підходи до вирішення задачі за темою дослідження

У рамках роботи над системою захисту ключову роль «мозку» охоронної підсистеми виконуватиме мікроконтролерна плата Arduino. Вона оброблятиме сигнали від PIR-датчика руху, який реагує на зміни в інфрачервоному спектрі, викликані рухом об’єктів у зоні спостереження. У разі виявлення активності плата активуватиме модуль камери для створення короткого відеозапису, який може слугувати доказовою базою, а також ініціюватиме відправку сповіщень користувачу через доступні канали зв’язку. Додатково система може бути розширена шляхом підключення інших компонентів, наприклад, звукових сигнальних пристроїв або датчиків температури, що дозволить адаптувати її до специфічних умов об’єкта.

Для програмування підсистеми буде використано середовище Arduino IDE, яке базується на мові C/C++. Вибір цього середовища обґрунтований кількома перевагами. По-перше, Arduino IDE містить широкий набір бібліотек для роботи з різними типами сенсорів, камер і модулів зв’язку, що значно прискорює розробку й полегшує інтеграцію компонентів. По-друге, код на C/C++ характеризується високою швидкістю виконання та ефективним використанням обмежених ресурсів мікроконтролера, що забезпечує надійну роботу системи в реальному часі. По-третє, простота синтаксису мови й доступність навчальних матеріалів дозволяють швидко адаптувати програмне забезпечення до вимог проєкту, навіть для розробників із базовим досвідом.

Поєднання апаратної платформи Arduino, яка вирізняється простотою підключення модулів і стабільністю роботи, із чіткою логікою програмування на C/C++ дає змогу створити функціональну охоронну систему без необхідності складних налаштувань. Розроблена підсистема забезпечуватиме оперативне реагування на виявлені події, автоматично записуючи відеофрагменти та

надсилаючи сповіщення, наприклад, через Wi-Fi-модуль (як-от ESP8266) для передачі даних у мережу або GSM-модуль для відправки SMS. Такий підхід дозволяє не лише миттєво інформувати про потенційні загрози, а й зберігати дані для подальшого аналізу. Модульна архітектура системи сприяє її гнучкості, дозволяючи легко додавати нові функції, такі як інтеграція з централізованими системами моніторингу, що може бути актуальним для приватних територій чи офісів закритого призначення

Реалізація цього проєкту сприятиме поглибленню знань у сфері програмування мікроконтролерів і роботи з апаратними компонентами, а також розвитку навичок створення прототипів охоронних систем, які відповідають реальним потребам підприємства. Робота над системою дозволить краще зрозуміти принципи функціонування сенсорних і мережевих технологій, а також навчитися враховувати практичні аспекти, такі як енергоефективність і надійність системи в умовах експлуатації.

Рисунок 1.6 – Приклад захисної системи приватного будинку на основі фото з офіційного сайту «Ajax» [16]

1.5 Висновок до першого розділу

У процесі дослідження охоронних систем проведено аналіз сучасних рішень, таких як Ajax Systems, Paradox Security Systems та Eldes, зосередившись на їхній архітектурі та функціональних можливостях. Вивчення предметної області допомогло розібратися в ключових задачах підсистем безпеки, зокрема у виявленні загроз і передачі даних. Розглянуто типові проблеми комерційних систем, як-от обмежена масштабованість і висока вартість, визначивши шляхи їхнього вдосконалення.

Особливу увагу приділено потенціалу платформи Arduino, яка завдяки модульності та підтримці датчиків є зручним інструментом для кастомізованих систем безпеки. Аналіз показав доцільність її використання для створення системи з відеоспостереженням, обробкою сигналів і сповіщеннями через GSM чи Wi-Fi. Порівняння з комерційними рішеннями сформувало вимоги до економічної та гнучкої системи.

Результати закладають основу для розробки охоронної системи для малих об’єктів, сприяючи розвитку навичок програмування мікроконтролерів і створення надійних рішень.

ПРОЕКТУВАННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ЗАХИСТУ ДЛЯ БУДИНКУ

2.1 Вибір об’єкту для розробки системи

В якості об’єкту для встановлення системи захисту було обрано одноповерховий будинок.

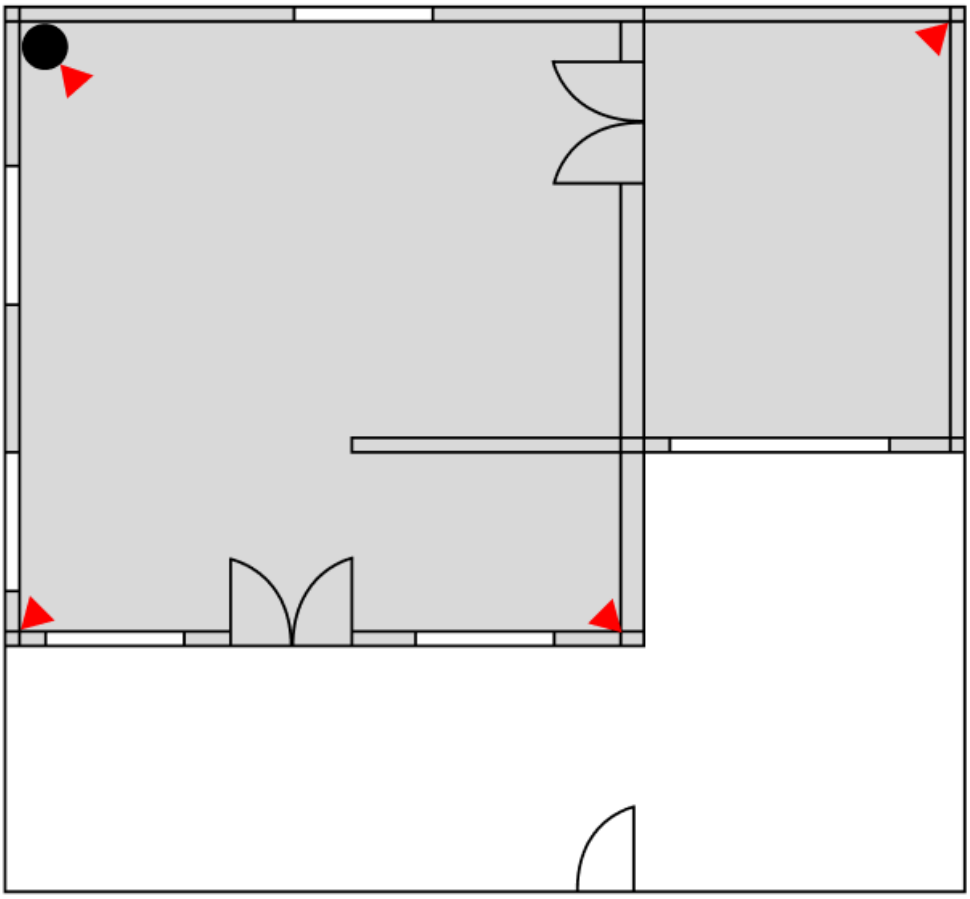


Рисунок 2.1 – Ескіз будинку

На рисунку 2.1 зображено план будинку, який складається з двох основних приміщень, з’єднаних між собою дверима. Будинок оточений парканом, що відображається лінією та визначає межі захищеної території. На плані також позначені вікна, які зображені як білі прямокутники в стінах будинку: Для

розробки системи захисту на базі Arduino необхідно врахувати особливості планування, розташування входів і вікон як потенційних точок проникнення, а також оптимально розмістити компоненти для забезпечення повного покриття внутрішнього простору адже через своєрідне обладнання датчик руху може помічати об’єкти що можуть не становити загрозу.

Центральним елементом системи є плата Arduino, об’єднана з датчиком руху та камерою, позначена на плані чорним кружечком. Її розміщено в верхньому лівому куті найбільшого приміщення, поблизу вікна на верхній стіні. Така позиція є стратегічно вигідною, оскільки датчик руху може охоплювати значну частину основного приміщення, яке є головною зоною активності. Розташування біля вікна дозволяє швидко виявляти рух у разі спроби проникнення через нього, а камера, інтегрована з платою, фіксуватиме події в цій зоні. Кутове розміщення також зменшує ризик пошкодження чи відключення пристрою, оскільки він розташований поза основними шляхами руху. Проте близькість до вікна потребує додаткового захисту плати від зовнішніх впливів, наприклад, вологи чи пилу, якщо вікно часто відчиняється.

На плані позначено чотири камери (червоні трикутники), розташовані в кутах приміщень. Їхнє розміщення та обґрунтування вибору наступне:

1. Камера в лівому верхньому куті найбільшого приміщення (розташуванням плати Arduino). Ця камера інтегрована з платою і спрямована на основний простір, охоплюючи зону поблизу вікна на верхній стіні. Її позиція дозволяє контролювати одну з потенційних точок проникнення – вікно, а також значну частину приміщення. Кутове розміщення забезпечує широкий кут огляду та зменшує сліпі зони, що є важливим для раннього виявлення руху.

2. Камера в правому верхньому куті меншого прямокутного приміщення (у верхній частині плану). Це приміщення використовується як вбиральня. Камера спрямована на вхід до цього приміщення та частину основного простору. Її розміщення обґрунтоване необхідністю контролю доступу через двері, що з’єднують основне приміщення з цією кімнатою, а також моніторингу руху

всередині будинку. Позиція в куті забезпечує огляд усієї кімнати, що дозволяє виявляти будь-які дії в цій зоні.

3. Камера в лівому нижньому куті найбільшого приміщення. Ця камера спрямована на зону поблизу зовнішнього входу в нижній частині плану та внутрішнього переходу до нижнього приміщення. Її розміщення дозволяє контролювати головний вхід до будинку, який є основною точкою доступу, а також рух між приміщеннями. Така позиція забезпечує додатковий захист від обходу основного входу та моніторинг можливих спроб проникнення через вікна.

4. Камера в правому нижньому куті нижнього приміщення. Ця камера потрібна для моніторингу простору поблизу основного входу в нижній частині плану. Її вибір обґрунтований необхідністю контролю входу до будинку щоб краще розгледіти потенційну небезпеку адже це приміщення виділене стіною щоб відокремити кухню від основного простору.

Розташування камер у кутах приміщень забезпечує максимальне покриття внутрішнього простору та контроль ключових точок доступу, таких як входи та вікна. Наявність вікон додає додаткові ризики, оскільки вони можуть бути використані для проникнення. Камери в кутах ефективно моніторять ці зони, дозволяючи вчасно виявляти загрози. Плата Arduino з датчиком руху слугує ядром системи, обробляючи сигнали від камер і координуючи реагування, наприклад, активацію сирени, запис відео чи надсилання сповіщень користувачу через GSM або Wi-Fi модулі.

Для підвищення ефективності системи доцільно додатково розмістити датчики вікон (наприклад, магнітоконтактні датчики відчинення) на обох вікнах, щоб отримувати миттєві сигнали в разі їхнього відчинення. Також варто розглянути встановлення зовнішніх датчиків руху вздовж паркану, особливо в зонах поблизу вікон і входів, для моніторингу периметру та раннього виявлення загроз. Інтеграція системи з модулями зв’язку забезпечить оперативне інформування власника про події, навіть якщо він перебуває поза межами об’єкта. Додатково можна передбачити резервне живлення для плати Arduino, щоб

система залишалася функціональною в разі відключення електроенергії, що є важливим для забезпечення безперервного захисту. Але більшість функціональних рішень неможливо через малу кількість модулів Arduino. Для покращення можна розробити систему з декількох модулів що забезпечить кращу систему охорони як в домі так поза межами приміщень.

Такий підхід до проектування системи дозволяє створити надійний захист, адаптований до особливостей об’єкта. Розташування компонентів враховує як внутрішні, так і зовнішні загрози, забезпечуючи комплексний контроль території будинку та прилеглого простору. Розробка такої системи на базі Arduino є економічно вигідним рішенням, яке може бути розширене залежно від потреб, наприклад, шляхом додавання нових датчиків чи інтеграції з платформами «розумного будинку».

Основною метою проекту є розробка плати на базі Arduino, яка інтегрує датчик руху та камеру в єдину систему, здатну самостійно забезпечувати моніторинг і сповіщення без залучення додаткових зовнішніх камер. Такий підхід дозволяє створити компактне й економічно вигідне рішення, де плата виступає центральним елементом, що обробляє сигнали від датчика руху, записує відеодані через вбудовану камеру та ініціює відправку повідомлень користувачу. Це забезпечує автономність системи та зменшує залежність від сторонніх пристроїв, що є важливим для реалізації простих і гнучких охоронних систем.

2.2 Компоненти на їх функції

У сучасному світі технологій питання розробки ефективних і надійних систем автоматизації набуває дедалі більшої актуальності, стаючи невід’ємною частиною як побутового, так і промислового середовища. Розвиток електронних пристроїв та мікроконтролерних платформ, зокрема таких як ESP32, відкриває нові горизонти для створення інноваційних рішень, які здатні відповідати зростаючим вимогам до безпеки, зручності та економічності. У цьому контексті особливу увагу приділяють інтеграції апаратних компонентів (Рисунок 2.2), таких

як датчик руху PIR, модуль камери OV2640, модуль для SD-карти та сама плата ESP32, що дозволяють реалізувати складні функції в єдиній системі, адаптованій до специфічних потреб користувача. Такі системи стають основою для автоматизації різноманітних об’єктів, від приватних помешкань до комерційних споруд, забезпечуючи контроль і моніторинг у реальному часі за допомогою відеоспостереження та сповіщень.

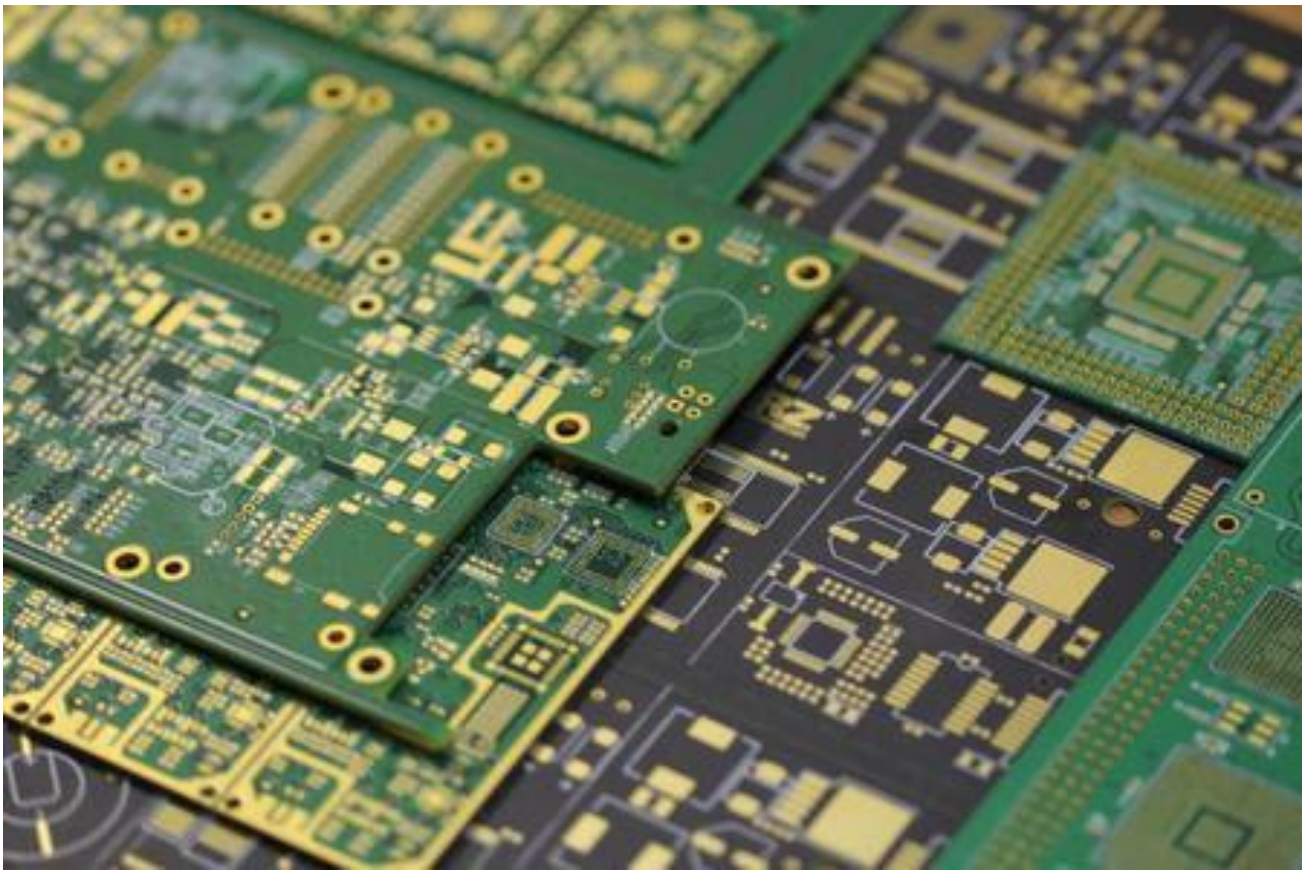


Рисунок 2.2 – Плати для проектів [9]

Розгляд цієї теми є важливим кроком у розумінні принципів побудови сучасних автоматизованих систем, які базуються на поєднанні програмного та апаратного забезпечення, зокрема з використанням ESP32 як центрального елемента обробки даних. Процес розробки таких рішень вимагає глибокого аналізу технічних можливостей компонентів, таких як датчик руху для виявлення об’єктів, камера OV2640 для запису відео, SD-карта для зберігання інформації та Wi-Fi-модуля для передачі даних. Усе це сприяє формуванню цілісного підходу

до проектування, що враховує як функціональність, так і довговічність систем. Особливо актуальним є вивчення взаємодії між цими елементами, які забезпечують безперервну роботу та адаптивність до змін зовнішніх умов, таких як рух чи необхідність відправки сповіщень через Telegram.

Розвиток автоматизації також тісно пов’язаний із потребами сучасного суспільства, де важливим є не лише забезпечення безпеки за допомогою датчика руху та камери OV2640, а й оптимізація ресурсів завдяки ефективному використанню SD-карти для зберігання даних та ESP32 для обробки. У цьому контексті аналіз компонентів стає ключовим етапом, який дозволяє визначити оптимальні шляхи реалізації проєктів із урахуванням економічних і технічних обмежень. Вивчення таких систем сприяє не лише технічному прогресу, а й розширенню знань у сфері електроніки та програмування, що є необхідним для підготовки фахівців у цій галузі. Завдяки цьому процес проектування набуває нового виміру, де кожен компонент, від ESP32 до OV2640, відіграє роль у створенні надійного й функціонального рішення.

Сучасні тенденції вказують на те, що автоматизовані системи, побудовані на базі ESP32, датчика руху, камери OV2640 та модуля SD-карти, все частіше інтегруються в повсякденне життя, стаючи невід’ємною частиною інфраструктури. Це зумовлює необхідність детального дослідження їхньої структури та принципів дії, щоб забезпечити високу якість і відповідність сучасним стандартам. У цьому процесі особливе місце відводиться аналізу взаємозв’язків між різними частинами системи, що дозволяє досягти гармонійного функціонування та підвищити її адаптивність. Такий підхід сприяє не лише технічному вдосконаленню, а й формуванню нових методів роботи з апаратними платформами, які стають основою для інноваційних розробок, таких як відеомоніторинг із відправкою через Telegram.

Розуміння основних принципів, на яких базується автоматизація з використанням ESP32, датчика руху PIR, камери OV2640 та SD-карти, є фундаментом для подальшого розвитку технологій у цій сфері. Воно дозволяє не

лише створювати ефективні рішення, а й прогнозувати їхню поведінку в різних умовах експлуатації, таких як зміна освітлення чи потреба в швидкій передачі даних. Цей аспект є особливо важливим у контексті зростання попиту на системи, які можуть оперативно реагувати на зовнішні стимули та забезпечувати безперервність роботи. Усе це підкреслює значущість теми, яка відкриває можливості для глибшого занурення в світ електронних систем і їхнього впливу на сучасне суспільство. Таким чином, аналіз компонентів, таких як ESP32, PIR, OV2640 та SD-карта, стає не лише технічним завданням, а й стратегічним напрямком для розвитку інноваційних технологій.

2.3 ESP32 та її функціонал

Мікроконтролерна плата ESP32 (Рисунок 2.3) є одним із ключових елементів у сучасних проєктах автоматизації та створення розумних пристроїв. Вона являє собою компактний модуль, який поєднує в собі обчислювальні можливості, бездротові технології зв’язку та широкий набір інтерфейсів для підключення периферійних пристроїв. Робота ESP32 базується на двоядерному процесорі Xtensa LX6, який забезпечує високу продуктивність для обробки даних у реальному часі. Завдяки вбудованим модулям Wi-Fi та Bluetooth, плата здатна забезпечувати стабільне з’єднання з мережею, що дозволяє передавати дані, отримувати команди або інтегруватися з хмарними сервісами.

ESP32 підтримує різноманітні протоколи зв’язку, такі як I2C, SPI, UART, що робить її універсальним рішенням для взаємодії з датчиками, камерами, дисплеями чи модулями пам’яті. Вона також має аналогово-цифрові перетворювачі (ADC), які дозволяють обробляти аналогові сигнали від зовнішніх пристроїв, наприклад, датчиків руху чи температури. Крім того, плата оснащена GPIO-пінами, які можна налаштувати для виконання різноманітних функцій, від керування світлодіодами до обробки складних сигналів. Завдяки низькому енергоспоживанню та підтримці режимів глибокого сну, ESP32 може ефективно працювати в автономних системах, що живляться від батарей.

Рисунок 2.4 – Плата ESP32[22]

Корисність ESP32 полягає в її універсальності та доступності, що робить її ідеальним вибором для широкого спектра проєктів. Вона дозволяє створювати системи автоматизації, такі як розумні будинки, де можна керувати освітленням, температурою чи безпекою через мережу. У проєктах IoT (Інтернет речей) плата забезпечує зв’язок між пристроями та віддаленими серверами, що дає змогу, наприклад, надсилати сповіщення на телефон користувача. Її компактність і низька ціна роблять її доступною для ентузіастів, студентів і розробників, які прагнуть створювати прототипи чи готові продукти без значних витрат. Крім того, широка підтримка спільноти та наявність бібліотек для програмування значно спрощують розробку, дозволяючи швидко втілювати ідеї в життя.

2.4 Датчик руху PIR та його функціонал

Датчик руху PIR (Passive Infrared Sensor) (Рисунок 2.5) є важливим елементом у системах автоматизації та безпеки, призначеним для виявлення руху об’єктів у заданій зоні спостереження. Його функціонування базується на принципі реєстрації інфрачервоного випромінювання, яке генерується живими об’єктами, такими як люди чи тварини, завдяки теплу їхнього тіла. Датчик оснащений піроелектричним елементом, який реагує на зміни інфрачервоного випромінювання в навколишньому середовищі, перетворюючи їх у електричний сигнал. Цей сигнал надходить на плату керування, де обробляється для подальшого виконання запрограмованих дій, таких як активація камери чи надсилання сповіщення.

Робота датчика PIR залежить від його чутливості та кута огляду, які визначають зону покриття. Він зазвичай працює у зв’язці з іншими компонентами системи, реагуючи на рух у межах певного радіуса дії. Датчик має два основні режими роботи: однократне спрацьовування або безперервне виявлення, що налаштовується залежно від потреб системи. Для забезпечення точності він часто оснащений лінзою Френеля, яка фокусує інфрачервоне випромінювання, підвищуючи ефективність виявлення. Завдяки простій конструкції та низькому енергоспоживанню датчик може працювати тривалий час без необхідності частого технічного обслуговування, що робить його практичним для автономних систем.

Корисність датчика руху PIR полягає в його здатності забезпечувати ефективний моніторинг із мінімальними витратами ресурсів. Він широко застосовується в системах безпеки, наприклад, для виявлення несанкціонованого доступу до приміщень, активуючи сигналізацію чи камери. У побутових умовах датчик сприяє економії енергії, автоматично вмикаючи освітлення чи інші пристрої лише за наявності руху. Його доступність і простота інтеграції з мікроконтролерами, такими як ESP32, роблять його популярним вибором для розробників, які створюють прототипи чи повноцінні системи автоматизації. Крім

того, датчик PIR є економічно вигідним рішенням, яке забезпечує надійність і точність у виявленні руху, що робить його незамінним у різноманітних сценаріях використання.

Рисунок 2.5 – датчик PIR [40]

2.5 Модуль камери OV2640 та її функціонал

Модуль камери OV2640 (Рисунок 2.6) є важливим компонентом у системах автоматизації, призначеним для захоплення зображень і відео, що забезпечує можливість візуального моніторингу в різноманітних проєктах. Його функціонування базується на використанні CMOS-сенсора, який перетворює світлові сигнали в цифровий формат, дозволяючи записувати зображення з роздільною здатністю до 2 мегапікселів. Камера працює у зв’язці з мікроконтролером, передаючи дані через інтерфейс, який підтримує швидкий

обмін інформацією. Вона здатна записувати як статичні зображення, так і відеопотік, що робить її придатною для систем, де потрібна фіксація подій у реальному часі.

Рисунок 2.6 – Модуль камери OV2640 [8]

Робота OV2640 залежить від налаштувань, які визначають якість і формат вихідних даних, таких як роздільна здатність, частота кадрів і рівень стиснення. Модуль забезпечує гнучкість у виборі параметрів, що дозволяє адаптувати його до конкретних умов експлуатації, наприклад, для роботи в умовах низької освітленості чи при високій динаміці руху. Камера також підтримує автоматичне регулювання експозиції та балансу білого, що сприяє отриманню чітких зображень у різних середовищах. Завдяки компактним розмірам і низькому енергоспоживанню OV2640 легко інтегрується в портативні системи, забезпечуючи стабільну роботу без значного навантаження на джерело живлення.

Корисність камери OV2640 полягає в її здатності забезпечувати якісний візуальний контроль у проєктах автоматизації та безпеки. Вона дозволяє фіксувати події, що можуть бути використані для подальшого аналізу, наприклад, у системах відеоспостереження чи моніторингу руху. Її сумісність із популярними мікроконтролерами, такими як ESP32, робить її зручним вибором для створення

систем, що потребують передачі зображень через мережу, наприклад, для відправки відео через Telegram. Доступна ціна та широка підтримка програмних бібліотек спрощують її використання, що робить OV2640 привабливим рішенням для розробників, які прагнуть реалізувати функціонал відеозапису без значних витрат. Це забезпечує широкі можливості для застосування в розумних пристроях, від домашньої автоматизації до прототипів IoT.

2.6 Модуль камери OV2640 та її функціонал

Модуль SD-карти (Рисунок 2в.7) є незамінним компонентом у системах автоматизації, призначеним для зберігання великих обсягів даних, що накопичуються в процесі роботи пристроїв. Його функціонування базується на використанні стандартного інтерфейсу SD (Secure Digital), який дозволяє підключати змінні картки пам’яті для запису та зчитування інформації. Модуль взаємодіє з мікроконтролером через протоколи SPI або SDIO, забезпечуючи швидкий обмін даними між пристроєм і носієм. Завдяки цьому він здатен обробляти файли різного формату, включаючи зображення, відео чи текстові записи, що робить його універсальним рішенням для систем, які потребують локального збереження інформації.

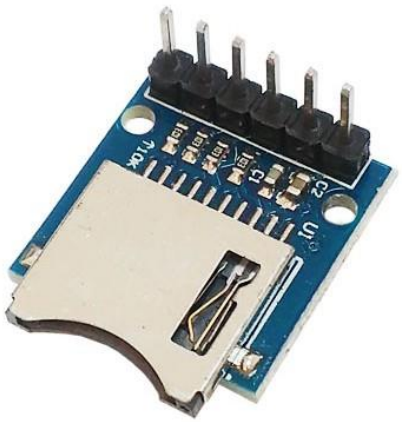


Рисунок 2.7 – Модуля SD-карти [8]

Робота модуля SD-карти залежить від налаштувань, таких як швидкість передачі даних і об’єм доступної пам’яті, які визначаються типом карти (SD, SDHC або SDXC). Він підтримує як одноразовий запис, так і постійне оновлення даних, що дозволяє використовувати його для логування подій чи зберігання медіафайлів у реальному часі. Модуль оснащений контактами для живлення та сигналів, що забезпечують стабільне підключення до мікроконтролера, а також механізмами захисту від перевантажень чи помилок запису. Завдяки компактному дизайну та низькому енергоспоживанню модуль SD-карти легко інтегрується в портативні пристрої, забезпечуючи їхню автономність і гнучкість у роботі.

Корисність модуля SD-карти полягає в його здатності забезпечувати надійне та зручне зберігання даних у системах автоматизації та IoT. Він дозволяє зберігати відеозаписи чи зображення, отримані з камер, такі як OV2640, для подальшого аналізу чи передачі, що є критично важливим у системах безпеки. Його сумісність із платами, такими як ESP32, полегшує створення автономних пристроїв, які можуть працювати без постійного з’єднання з хмарою. Доступна ціна та широка підтримка програмних бібліотек роблять модуль SD-карти привабливим для розробників, які прагнуть реалізувати рішення для логування чи архівування без значних витрат. Це відкриває широкі можливості для застосування в розумних будинках, промислових системах та інших проєктах, де потрібне локальне зберігання інформації.

2.7 Платформа – симулятор Wokwi

Розробка системи автоматизації, що інтегрує апаратні компоненти, такі як мікроконтролер ESP32, датчик руху PIR, камера OV2640 і модуль SD-карти, становить собою складне інженерне завдання, яке вимагає комплексного підходу до проєктування, ретельного тестування, відлагодження та забезпечення безперебійної взаємодії між апаратними і програмними складовими системи. Такі

проєкти характеризуються високим рівнем складності через необхідність синхронізації роботи різнорідних компонентів, кожен із яких має власні технічні особливості та вимоги до програмного забезпечення. У цьому контексті вибір відповідного симуляційного середовища набуває критичного значення, оскільки воно дозволяє розробникам проводити попереднє тестування і відлагодження системи без використання фізичного обладнання, що значно знижує витрати часу та ресурсів на ранніх етапах розробки.

Платформа Wokwi зарекомендувала себе як один із найбільш зручних, ефективних і універсальних інструментів для симуляції складних електронних систем, пропонуючи широкий набір функцій для моделювання поведінки апаратних компонентів у віртуальному середовищі. Її унікальність полягає в можливості створювати реалістичні моделі роботи мікроконтролерів, датчиків і периферійних пристроїв без необхідності фізичного підключення обладнання, що особливо цінно на етапі прототипування. Переваги Wokwi стають особливо очевидними в проєктах, подібних до цього, де потрібно не лише забезпечити коректну роботу мікроконтролера ESP32 для обробки вхідних сигналів, але й імітувати спрацьовування датчика руху PIR, моделювати процес захоплення та обробки відеопотоку через камеру OV2640, а також перевіряти функціонал збереження даних на SD-карту та їх подальшу передачу через Wi-Fi для відправки сповіщень через Telegram.

Крім того, Wokwi дозволяє розробникам тестувати програмний код у реальному часі, виявляти потенційні помилки в логіці роботи системи та оптимізувати її продуктивність ще до розгортання на реальному обладнанні. Це середовище підтримує широкий спектр бібліотек і модулів, які спрощують інтеграцію таких компонентів, як камера OV2640, а також забезпечують можливість налаштування параметрів роботи датчиків і модулів пам’яті. Завдяки гнучкості платформи, розробники можуть швидко адаптувати проєкт до змін у вимогах, що є важливим аспектом при роботі з експериментальними системами автоматизації. Таким чином, використання Wokwi не лише прискорює процес

розробки, але й підвищує надійність і якість кінцевого продукту, забезпечуючи стабільну взаємодію всіх компонентів системи.

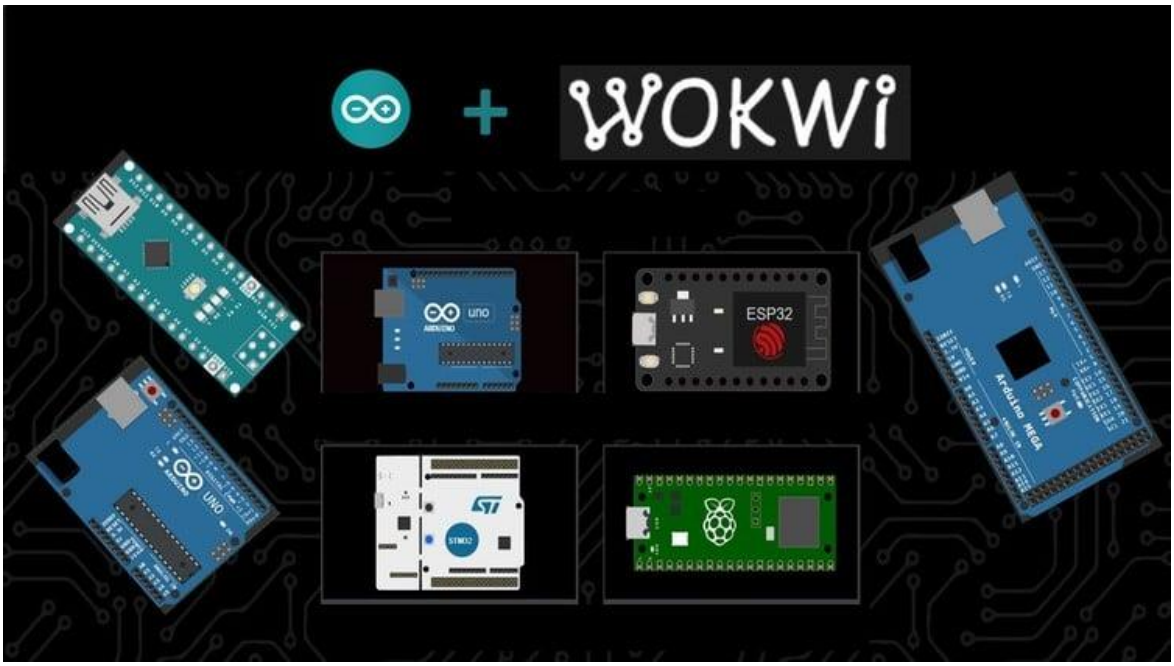


Рисунок 2.8 – Wokwi та сумісність з Arduino [11]

Однією з ключових причин, чому платформа Wokwi є оптимальним вибором для реалізації цього проєкту, є її онлайн-доступність, яка забезпечує зручність і гнучкість у процесі розробки. Завдяки хмарній архітектурі Wokwi розробники можуть працювати над проєктом із будь-якого місця та пристрою, що має підключення до інтернету, будь то персональний комп'ютер, планшет чи навіть смартфон. Така особливість усуває необхідність встановлення спеціалізованого програмного забезпечення на локальний комп'ютер, що значно економить час, зменшує технічні бар'єри та робить платформу доступною для широкого кола користувачів, включаючи студентів, інженерів-початківців і досвідчених розробників. Крім того, онлайн-доступність дозволяє легко ділитися проєктами з колегами чи викладачами, що сприяє співпраці та спрощує процеси рецензування й тестування.

У контексті цього проєкту Wokwi демонструє свої переваги, надаючи можливість швидко та ефективно перевірити взаємодію компонентів системи

автоматизації. Наприклад, платформа дозволяє моделювати сценарії, у яких датчик руху PIR виявляє рух і активує камеру OV2640 для запису відео, після чого дані передаються на SD-карту для зберігання. ESP32, як центральний елемент системи, обробляє ці дії, забезпечуючи синхронізацію між апаратними компонентами та передачу сповіщень через мережу Wi-Fi, наприклад, через месенджер Telegram. Wokwi підтримує широкий спектр віртуальних компонентів (Рисунок 2.9), включаючи мікроконтролер ESP32, датчики руху PIR, камери OV2640 та модулі SD-карт, що дає змогу з високою точністю відтворити апаратне середовище системи ще до її фізичної реалізації. Це дозволяє розробникам тестувати різні конфігурації системи, перевіряти сумісність компонентів і оптимізувати їхню взаємодію.

Крім того, Wokwi пропонує потужні інструменти для налагодження програмного коду в реальному часі, що значно полегшує виявлення та усунення помилок. Наприклад, вбудований серійний монітор дозволяє відстежувати вихідні дані від ESP32, аналізувати сигнали датчика PIR і перевіряти коректність роботи камери OV2640 під час запису. Ці інструменти дають змогу розробникам швидко виявляти логічні чи синтаксичні помилки в коді, а також оптимізувати алгоритми ще до розгортання системи на фізичному обладнанні. Завдяки підтримці популярних бібліотек, таких як Arduino чи MicroPython (Рисунок 2.8), Wokwi забезпечує гнучкість у виборі програмного середовища, що дозволяє адаптувати проєкт до специфічних потреб. Таким чином, використання Wokwi не лише спрощує процес розробки, але й підвищує якість кінцевого продукту, забезпечуючи стабільність і надійність роботи системи автоматизації.

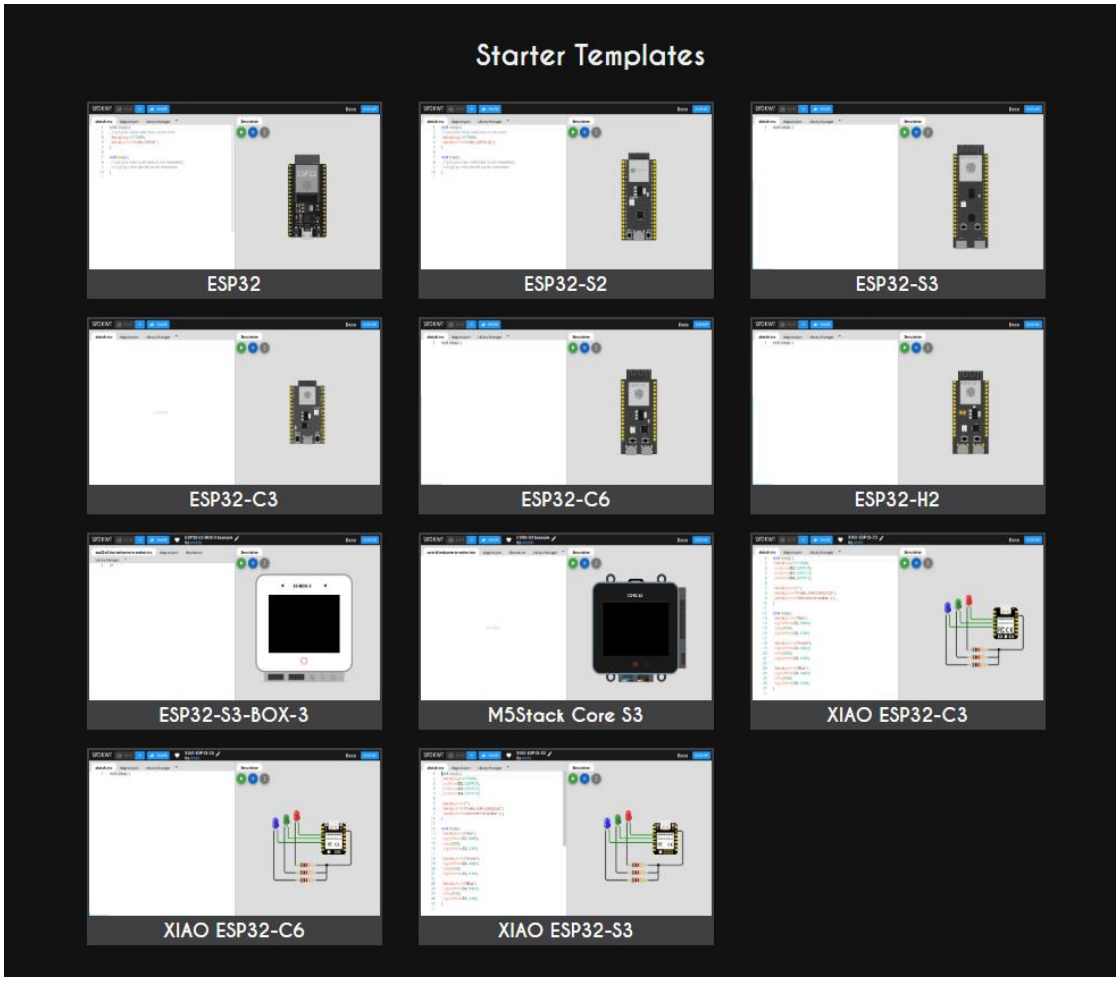


Рисунок 2.9 – Різноманітність Esp32 на платформі Wokwi [11]

Важливою перевагою Wokwi є безпека експериментів, адже віртуальні компоненти неможливо пошкодити, на відміну від їхніх фізичних аналогів. Для цього проєкту це означає, що розробник може без ризиків тестувати різні сценарії роботи системи, наприклад, імітувати рух для перевірки реакції датчика PIR, змінювати параметри камери OV2640 для оцінки якості запису чи експериментувати з налаштуваннями Wi-Fi для відправки відео через Telegram. Такий підхід дозволяє уникнути типових проблем, пов’язаних із неправильним підключенням чи програмними збоями, які могли б призвести до пошкодження реального обладнання. Wokwi також підтримує симуляцію мережевих протоколів, таких як HTTP чи MQTT, що є важливим для тестування передачі даних через Telegram, навіть якщо реальне з’єднання з мережею недоступне. Це створює

ідеальні умови для ітеративного тестування, коли потрібно швидко перевірити ідею чи внести зміни до системи.

Інші розробники обирають Wokwi через її гнучкість і доступність для користувачів із різним рівнем досвіду. Платформа дозволяє створювати спільні проєкти, ділитися ними з іншими учасниками команди чи спільнотою, що сприяє обміну знаннями та швидкому вирішенню технічних питань. Для студентів і ентузіастів Wokwi є економічно вигідним рішенням, адже безкоштовна версія платформи надає доступ до більшості необхідних функцій, таких як симуляція ESP32, датчиків і базових мережевих протоколів. Розробники також цінують інтеграцію Wokwi з популярними інструментами, такими як Visual Studio Code (Рисунок 2.10), що дозволяє працювати в знайомому середовищі, підвищуючи продуктивність і комфорт під час програмування. Ці особливості роблять Wokwi популярним вибором серед тих, хто працює над проєктами автоматизації, де швидкість ітерацій, економія ресурсів і підтримка спільноти відіграють вирішальну роль.

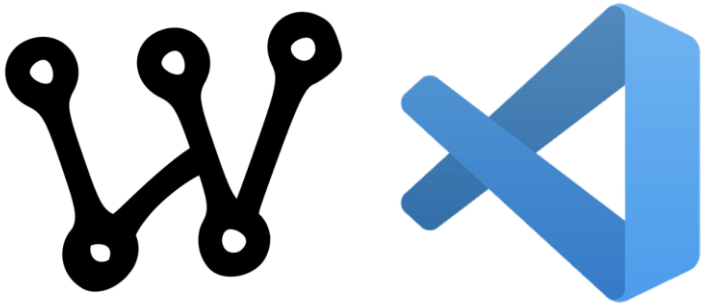


Рисунок 2.10 – Сумісність з Visual Studio [40]

Історія створення симуляторів для Arduino бере свій початок із популяризації цієї платформи на початку 2000-х років, коли Arduino стало доступним інструментом для ентузіастів, студентів і розробників. Спочатку тестування проєктів на Arduino вимагало фізичного обладнання, що створювало певні труднощі, особливо для новачків, які могли допускати помилки в

підключенні чи програмуванні. Це призводило до пошкодження компонентів або значних витрат часу на відлагодження. Зростання популярності Arduino підштовхнуло спільноту до створення віртуальних середовищ, які могли б імітувати роботу плати та її взаємодію з датчиками, дисплеями чи іншими модулями. Перші симулятори, такі як AVR Simulator, з'явилися як інструменти для моделювання AVR-контролерів, на яких базується Arduino Uno, але вони мали обмежені можливості й часто потребували глибоких технічних знань для налаштування.

З часом з'явилися більш зручні платформи, такі як Tinkercad Circuits (Рисунок 2.11), запущений Autodesk у 2010-х роках, який запропонував інтуїтивний drag-and-drop інтерфейс для створення схем і написання коду. Tinkercad став популярним серед новачків завдяки простоті використання, але його обмеження, такі як відсутність підтримки складних компонентів чи мережевих протоколів, спонукали до створення нових рішень. Саме в цьому контексті з'явився Wokwi, який запустили у 2019 році, щоб закрити прогалини попередніх симуляторів. Wokwi швидко здобув популярність завдяки підтримці сучасних плат, таких як ESP32, і можливості симуляції складних сценаріїв, таких як зв'язок через Wi-Fi чи Bluetooth. Розробники Wokwi зробили акцент на доступності, додавши онлайн-інтерфейс і підтримку спільноти, що дозволило платформі стати однією з провідних для проєктів на базі Arduino.

Розвиток симуляторів для Arduino також пов'язаний із глобальними тенденціями в освіті та технологіях, де віртуальні інструменти стали важливим елементом навчання. Вони дозволяють студентам і розробникам експериментувати з апаратним забезпеченням без фінансових ризиків, що особливо актуально в умовах обмеженого доступу до фізичних ресурсів. Wokwi, зокрема, стала популярною завдяки своїй орієнтації на IoT-проєкти, де потрібна симуляція мережевих протоколів і взаємодія з хмарними сервісами. Для цього проєкту Wokwi забезпечує ідеальні умови, адже дозволяє протестувати всі

аспекти системи — від виявлення руху до передачі даних — у віртуальному середовищі, що значно прискорює процес розробки.

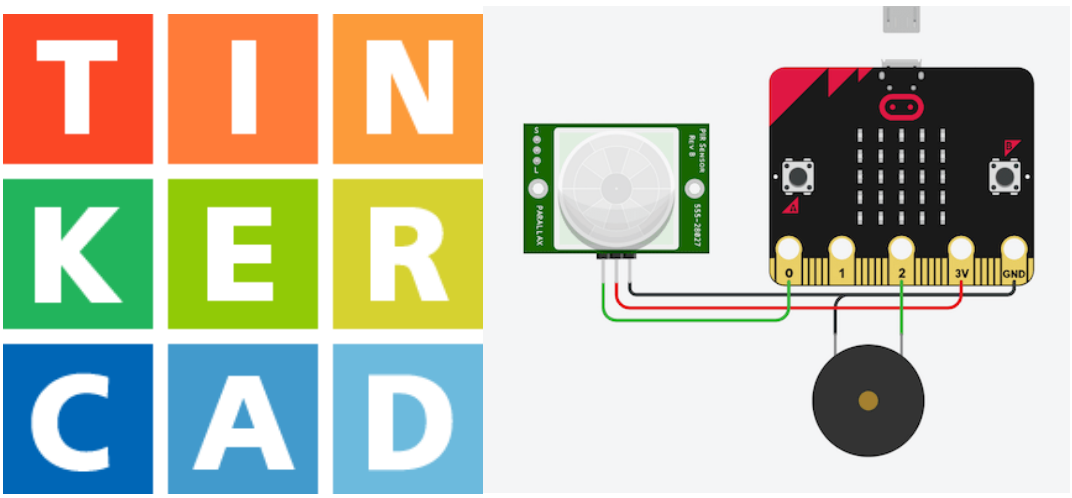


Рисунок 2.11 – TinkerCad та його плата [40]

Поява хмарних платформ, таких як Wokwi, кардинально змінила підхід до розробки мікроконтролерних систем, зробивши процес створення та тестування прототипів значно ефективнішим і доступнішим. Якщо раніше розробники були змушені покладатися виключно на фізичні плати, датчики та інші апаратні компоненти, що вимагало значних фінансових і часових витрат, то сучасні симуляційні середовища, такі як Wokwi, дозволяють створювати повноцінні віртуальні прототипи, які точно відтворюють поведінку реальних систем. Це не лише знижує витрати на закупівлю обладнання, але й мінімізує ризики пошкодження компонентів під час експериментів, а також прискорює ітеративний процес розробки. Wokwi стала яскравим прикладом того, як інноваційні технології можуть демократизувати доступ до розробки, роблячи її доступною для широкого кола користувачів — від школярів, які тільки починають вивчати програмування та електроніку, до досвідчених інженерів, які створюють складні промислові рішення.

У контексті цього проєкту, який передбачає розробку захисної системи на базі мікроконтролера ESP32, датчика руху PIR, камери OV2640 і модуля SD-

карти, Wokwi демонструє свої унікальні можливості для симуляції складних систем автоматизації. Платформа дозволяє моделювати повний цикл роботи системи: від виявлення руху датчиком PIR до активації камери для запису відео, збереження даних на SD-карту та передачі сповіщень через Wi-Fi. Такий підхід дає змогу розробникам перевірити коректність взаємодії компонентів і оптимізувати програмну логіку ще до закупівлі фізичного обладнання. Наприклад, Wokwi дозволяє точно відтворити поведінку ESP32 під час обробки сигналів від датчика, імітувати якість відеозапису камери OV2640 і перевірити стабільність роботи SD-карти в різних сценаріях. Це значно знижує ризик виникнення помилок на етапі фізичної реалізації проєкту

Таким чином, використання Wokwi для цього проєкту забезпечує економічно вигідний і ефективний спосіб розробки, дозволяючи розробникам зосередитися на створенні надійної програмної логіки та оптимізації взаємодії апаратних компонентів без необхідності інвестувати в дороге обладнання на початкових етапах. Популярність Wokwi серед користувачів пояснюється не лише її простотою доступу через хмарний інтерфейс, але й широкими можливостями симуляції, які охоплюють широкий спектр мікроконтролерів і периферійних пристроїв. Крім того, платформа підтримується активною спільнотою розробників, яка постійно створює нові бібліотеки, приклади коду та навчальні матеріали, що полегшують освоєння інструменту. Wokwi також інтегрується з сучасними засобами розробки, такими як Arduino IDE чи PlatformIO, що забезпечує гнучкість у виборі програмного середовища.

Історія розвитку симуляторів для Arduino та інших мікроконтролерних платформ є прикладом швидкої еволюції інструментів, які суттєво змінили підхід до створення електронних систем. На початкових етапах симулятори представляли собою прості емулятори базового рівня, які дозволяли моделювати лише окремі аспекти роботи мікроконтролерів, такі як виконання базових команд або обробка простих сигналів. Вони часто мали обмежений функціонал, вимагали значних ресурсів комп’ютера і не могли повноцінно відтворювати складні

взаємодії між апаратними компонентами. Однак із прогресом у сфері програмного забезпечення та хмарних технологій сучасні симулятори, такі як Wokwi, досягли нового рівня розвитку, пропонуючи потужні рішення, що відповідають високим вимогам сучасних інженерних задач. Ці інструменти дозволяють розробникам створювати деталізовані віртуальні прототипи, які точно імітують поведінку реальних систем, включаючи складні сценарії роботи з датчиками, модулями пам’яті та мережевими інтерфейсами.

Крім того, Wokwi вирізняється своєю здатністю інтегруватися з популярними середовищами розробки, такими як Arduino IDE, PlatformIO чи MicroPython, що забезпечує гнучкість у виборі інструментів програмування. Активна спільнота користувачів платформи постійно створює нові бібліотеки, навчальні посібники та приклади проєктів, що значно полегшує освоєння Wokwi для новачків і розширює її можливості для професіоналів. Ця платформа також підтримує інструменти для налагодження, такі як серійний монітор і симуляція мережевих підключень, що дозволяють виявляти помилки та оптимізувати код ще до його розгортання на фізичному обладнанні. Таким чином, Wokwi не лише спрощує процес розробки, але й робить її більш економічно вигідною, дозволяючи зосередитися на творчих аспектах проєктування. Завдяки своїм можливостям і доступності Wokwi стала незамінним інструментом для сучасних проєктів автоматизації, сприяючи швидкому втіленню ідей і підвищенню якості кінцевих продуктів.

2.8 Висновок до другого розділу

Інтеграція мікроконтролера ESP32, датчика руху PIR, камери OV2640 і модуля SD-карти в систему автоматизації демонструє ефективне поєднання апаратних і програмних компонентів для створення рішень у сфері безпеки. Проект, призначений для приватного будинку, підвищує безпеку завдяки швидкому виявленню руху, запису відео та сповіщень через Telegram. Дані

зберігаються на SD-карті для аналізу, а ESP32 забезпечує синхронізацію та дистанційне керування через Wi-Fi.

Платнаформа Wokwi стала ключовою для тестування проєкту, дозволяючи відлагоджувати систему у віртуальному середовищі. Вона підтримує компоненти, як-от ESP32 і PIR, допомагаючи виявляти помилки та оптимізувати код без фізичного обладнання. Wokwi, з її інтуїтивним інтерфейсом і підтримкою спільноти, спрощує розробку, роблячи її доступною для інженерів і студентів. Цей проєкт підкреслює роль симуляторів у створенні інноваційних систем автоматизації.

РОЗРОБКА КІБЕРФІЗИЧНОЇ СИСТЕМИ ЗАХИСТУ ДЛЯ БУДИНКУ

3.1 Розбір апаратної частини схеми

У рамках розробки апаратної частини кіберфізичної системи захисту для будинку, реалізованої через симуляційне середовище Wokwi, було використано кілька ключових апаратних модулів, які разом формують функціональний прототип системи відеоспостереження з інтеграцією датчиків, обробкою даних і можливістю зберігання інформації. Основна мета проєкту полягала в створенні ефективної системи, яка забезпечує моніторинг безпеки будинку шляхом виявлення руху, запису відеоданих і сповіщення користувача через сучасні канали комунікації. Оскільки плата ESP32-CAM, яка зазвичай використовується для таких завдань, не підтримується в симуляторі Wokwi, було прийнято рішення адаптувати функціонал системи за допомогою плати ESP32 Dev Module. Цей вибір дозволив ефективно імітувати ключові можливості ESP32-CAM, включаючи обробку сигналів, керування камерою та передачу даних, завдяки гнучкому налаштуванню GPIO-пінів і сумісності з програмними бібліотеками. У рамках проєкту також передбачено відправку зображень через Telegram-бота, що забезпечує зручний і швидкий дистанційний моніторинг, дозволяючи користувачу отримувати сповіщення про виявлені події в реальному часі.

Плата ESP32 Dev Module що зображена на рисунку 3.1 виступає центральним елементом системи, виконуючи роль основного контролера, який координує роботу всіх підключених модулів. Вона відповідає за обробку вхідних сигналів від датчика руху PIR, ініціалізацію та керування камерою OV2640 для захоплення зображень, а також збереження даних на SD-карту та їх передачу через Wi-Fi для відправки сповіщень через Telegram. Вибір ESP32 Dev Module у симуляторі Wokwi зумовлений її універсальністю та можливістю адаптації до вимог проєкту, зокрема завдяки підтримці гнучкого налаштування пінів і сумісності з широким спектром бібліотек, таких як Arduino та ESP-IDF. У процесі

розробки використано адаптивний програмний код, який враховує особливості симуляційного середовища Wokwi, дозволяючи точно моделювати поведінку системи в умовах, максимально наближених до реальних. Наприклад, код забезпечує коректну імітацію ініціалізації камери OV2640, обробки сигналів від датчика руху PIR і передачі даних через віртуальний Wi-Fi-модуль.

Крім того, використання ESP32 Dev Module у симуляторі дозволило протестувати ключові аспекти роботи системи, такі як синхронізація між компонентами, стабільність обробки даних і коректність відправки сповіщень. У процесі моделювання було приділено особливу увагу оптимізації взаємодії між модулями, щоб забезпечити швидке реагування системи на виявлення руху та ефективне використання ресурсів мікроконтролера. Адаптивний код, розроблений для Wokwi, включає спеціальні налаштування для віртуального середовища, які дозволяють імітувати поведінку апаратних компонентів, таких як затримки в обробці сигналів чи обмеження пропускної здатності мережі. Це забезпечує можливість виявлення потенційних проблем, таких як помилки в логіці роботи чи перевантаження процесора, ще до реалізації системи на фізичному обладнанні. Таким чином, використання ESP32 Dev Module у поєднанні з симулятором Wokwi дозволило створити гнучкий і ефективний прототип, який демонструє потенціал кіберфізичної системи захисту для будинку.

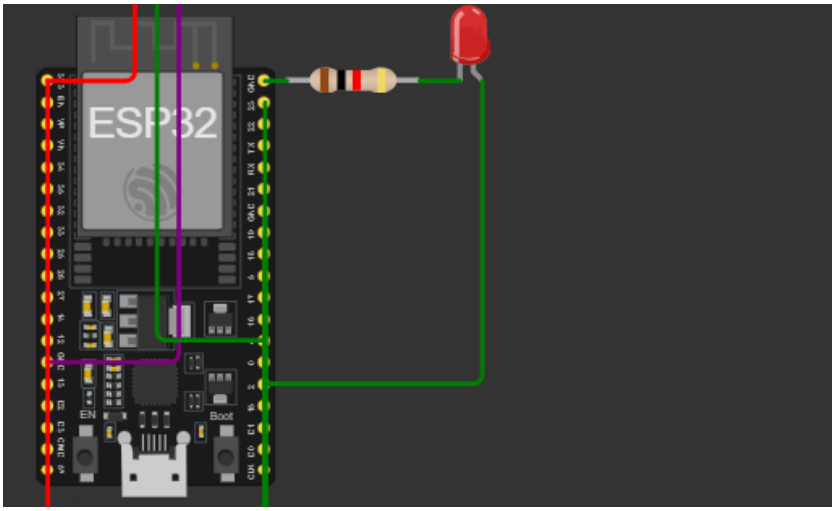


Рисунок 3.1 – Плата ESP32 [8]

Камера OV2640 відіграє ключову роль у системі відеоспостереження, забезпечуючи захоплення зображень, необхідних для моніторингу зони спостереження та виявлення потенційних загроз у приватному будинку. Цей модуль є центральним компонентом проєкту, оскільки дозволяє фіксувати візуальні дані, які обробляються та передаються для подальшого аналізу чи сповіщення користувача. У симуляційному середовищі Wokwi, де фізична камера OV2640 недоступна, її роботу імітує зелений світлодіод (LED), підключений до GPIO 2 плати ESP32 Dev Module через резистор номіналом 220 Ом. Цей LED загоряється щоразу, коли система виконує дію, еквівалентну "фіксації" зображення, що дозволяє розробникам візуально відстежити логіку спрацьовування камери в програмному коді. Такий підхід забезпечує ефективну перевірку алгоритмів керування камерою та їх інтеграції з іншими компонентами системи в умовах віртуального середовища.

У реальній системі камера OV2640 підключається до плати ESP32 через I2C-інтерфейс, використовуючи піни SDA (GPIO 26) і SCL (GPIO 27) для передачі даних. Цей інтерфейс забезпечує швидке та надійне з’єднання між камерою та мікроконтролером, дозволяючи передавати зображення високої якості для подальшої обробки або збереження. У симуляторі Wokwi, де фізична передача даних через I2C неможлива, функціонал камери замінено на умовну візуальну індикацію через LED, що відображає моменти ініціалізації та захоплення зображень. Така імітація є достатньою для тестування логіки роботи системи, зокрема перевірки коректності алгоритму, який відповідає за обробку зображень і їх відправку через Telegram-бота для дистанційного сповіщення користувача. Наприклад, у симуляції можна відстежити, як спрацьовування датчика руху PIR активує "захоплення" зображення, що супроводжується увімкненням LED що зображений на рисунку 3.2, а потім перевірити, чи правильно формується команда для передачі даних через віртуальний Wi-Fi-модуль.

Крім того, використання LED як індикатора в симуляторі дозволяє розробникам детально аналізувати послідовність дій у коді, виявляти можливі помилки в логіці або затримки в обробці сигналів. У процесі розробки було враховано особливості симуляційного середовища Wokwi, що дало змогу адаптувати програмний код для точного відтворення поведінки камери OV2640 у реальних умовах. Наприклад, код включає умовні оператори, які імітують часові характеристики роботи камери, такі як затримки при ініціалізації або обробці зображень, що забезпечує реалістичність тестування. Такий підхід не лише полегшує налагодження алгоритмів, але й дозволяє оптимізувати взаємодію між камерою, мікроконтролером і Telegram-ботом ще до реалізації системи на фізичному обладнанні. Таким чином, імітація роботи OV2640 у Wokwi забезпечує надійний і економічно ефективний спосіб розробки, дозволяючи зосередитися на програмній логіці та інтеграції компонентів системи відеоспостереження.

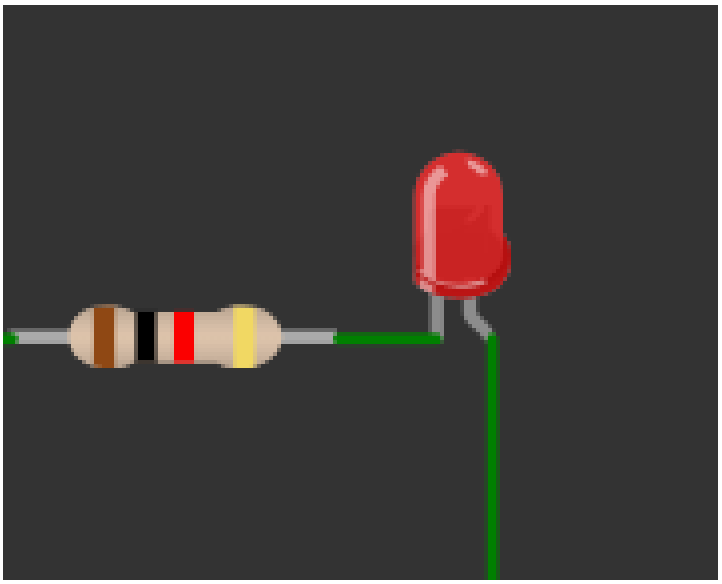


Рисунок 3.2 – LED [9]

Датчик руху PIR що зображена на рисунку 3.3, підключений до піна GPIO 7 плати ESP32 Dev Module, відіграє ключову роль у системі відеоспостереження, виконуючи функцію ініціатора подій шляхом виявлення руху в заданій зоні спостереження. Цей компонент є важливим елементом системи, оскільки саме він

запускає весь ланцюжок автоматизованих дій, спрямованих на забезпечення безпеки будинку. При виявленні руху датчик генерує вихідний сигнал логічного рівня "HIGH", який надходить на плату ESP32, сигналізуючи про початок процесу зйомки камерою OV2640 та подальшої обробки даних. У рамках проєкту датчик руху PIR налаштований на високу чутливість, що дозволяє ефективно імітувати реальні сценарії, такі як виявлення людини чи іншого об’єкта, що рухається в зоні спостереження. Такий рівень чутливості забезпечує надійне спрацьовування системи навіть у складних умовах, наприклад, за слабкого освітлення або при мінімальних рухах.

У симуляційному середовищі Wokwi датчик руху PIR відтворюється як віртуальний компонент, що дає змогу розробникам тестувати реакцію системи на зміну його стану без використання фізичного обладнання. У Wokwi можливо змоделювати різні сценарії, такі як періодичне чи раптове спрацьовування датчика, що дозволяє перевірити коректність алгоритмів обробки сигналів і їх вплив на інші компоненти системи. Наприклад, коли датчик переходить у стан "HIGH", система активує камеру для фіксації зображення, а плата ESP32 обробляє сигнал і запускає процес відправки сповіщення через Telegram-бота. Це забезпечує можливість відпрацювання сценаріїв автоматизації, таких як миттєве повідомлення користувача про виявлення руху в зоні спостереження. У симуляторі також можна налаштувати параметри датчика, такі як час затримки після спрацьовування або чутливість, що дозволяє адаптувати його поведінку до специфічних умов проєкту.

Крім того, використання віртуального датчика PIR у Wokwi сприяє детальному аналізу логіки роботи системи, дозволяючи виявляти потенційні помилки, такі як хибні спрацьовування чи затримки в обробці сигналів. Наприклад, розробники можуть протестувати, як система реагує на серію швидких змін стану датчика, що імітує повторні рухи в зоні спостереження, або перевірити стабільність роботи при тривалому навантаженні. Такий підхід забезпечує можливість оптимізації програмного коду, зокрема алгоритмів, які

координують взаємодію між датчиком, камерою та модулем передачі даних. Завдяки симуляції в Wokwi розробники можуть не лише перевірити коректність роботи системи, але й удосконалити її ефективність, зменшивши час реакції на події та підвищивши надійність сповіщень через Telegram. Таким чином, датчик руху PIR у поєднанні з можливостями симулятора Wokwi відіграє важливу роль у створенні надійної кіберфізичної системи захисту, забезпечуючи її готовність до реальних умов експлуатації.

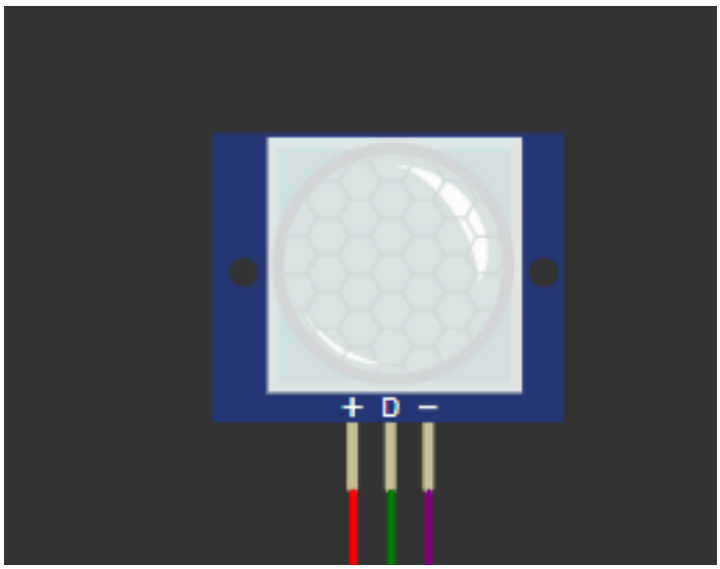


Рисунок 3.3 – Датчик руху PIR [10]

Модуль SD-карти що зображена на рисунку 3.4, підключений до плати ESP32 Dev Module через SPI-інтерфейс із використанням пінів GPIO 5 (CS), GPIO 23 (MOSI), GPIO 19 (MISO) та GPIO 18 (SCK), відіграє ключову роль у системі відеоспостереження, забезпечуючи локальне зберігання зображень, захоплених камерою OV2640. Ця функція є критично важливою для забезпечення надійності системи, особливо в умовах тимчасової відсутності зв'язку з мережею Wi-Fi, що може статися через нестабільне інтернет-з'єднання або технічні збої. Локальне зберігання даних на SD-карті дозволяє системі продовжувати функціонувати автономно, зберігаючи зображення для подальшого аналізу чи передачі, коли зв'язок буде відновлено. Такий підхід гарантує, що жодна важлива подія, зафіксована датчиком руху PIR, не буде втрачена, що робить модуль SD-карти

незамінним компонентом для створення надійної кіберфізичної системи захисту будинку.

У симуляційному середовищі Wokwi модуль SD-карти відтворюється як віртуальний компонент, який імітує операції запису та читання файлів, дозволяючи розробникам перевірити коректність роботи системи щодо обробки та збереження даних. У Wokwi можливо моделювати повний цикл роботи з SD-картою, включаючи ініціалізацію модуля, запис зображень у відповідному форматі (наприклад, JPEG) та перевірку їхньої цілісності перед відправкою через Telegram-бота. Така імітація дає змогу протестувати, як плата ESP32 координує операції між камерою OV2640 і SD-картою, а також оцінити продуктивність системи в різних сценаріях, наприклад, при інтенсивному записі даних або в умовах обмеженого обсягу пам’яті. У симуляції також можна перевірити стабільність роботи SPI-інтерфейсу, зокрема правильність налаштування пінів і швидкість передачі даних, що дозволяє виявити потенційні помилки в програмному коді ще до реалізації системи на фізичному обладнанні.

Наявність SD-карти в системі значно підвищує її надійність, оскільки вона забезпечує резервне копіювання даних, що є особливо важливим для сценаріїв, коли зображення потрібно зберегти для подальшого аналізу, наприклад, для розслідування інцидентів або моніторингу активності в зоні спостереження. У реальних умовах SD-карта дозволяє зберігати великий обсяг даних, що дає змогу користувачу переглядати історичні записи, навіть якщо вони не були передані через мережу в момент зйомки. У симуляторі Wokwi розробники можуть протестувати різні аспекти роботи з SD-картою, такі як форматування файлів, управління пам’яттю та обробка помилок, наприклад, у разі переповнення карти або збою при записі. Це дозволяє оптимізувати програмний код, забезпечуючи ефективне використання ресурсів і стабільність роботи системи. Таким чином, модуль SD-карти, завдяки своїй інтеграції через SPI-інтерфейс і можливостям симуляції в Wokwi, є важливим елементом системи, що забезпечує надійність,

автономність і гнучкість у збереженні даних для кіберфізичної системи захисту будинку.

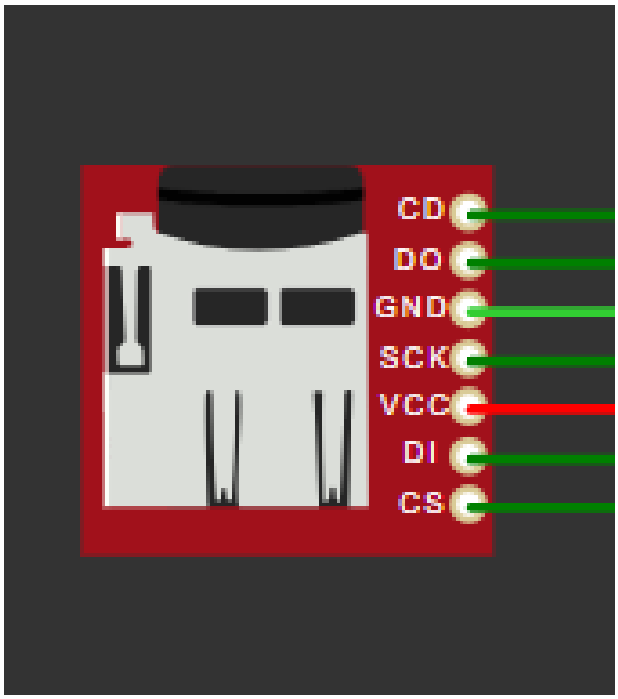


Рисунок 3.4 – Модуль SD-карти [24]

3.2 Схема підключень та обгрунтування

Схема підключення кіберфізичної системи захисту для будинку побудована навколо плати ESP32 Dev Module, яка виконує роль центрального вузла управління, забезпечуючи координацію роботи всіх апаратних компонентів системи. Ця плата була обрана завдяки своїй універсальності, підтримці широкого набору інтерфейсів і можливості адаптації до вимог проєкту в симуляційному середовищі Wokwi, де вона ефективно імітує функціонал плати ESP32-CAM. Схема включає кілька ключових модулів — датчик руху PIR, світлодіод (LED) для імітації камери OV2640 і модуль SD-карти, — кожен із яких підключений до відповідних пінів ESP32 для забезпечення стабільної взаємодії та виконання функціональних завдань системи, таких як виявлення руху, фіксація зображень і збереження даних. Обґрунтування вибору схеми підключення базується на

необхідності створення надійної, енергоефективної та гнучкої системи, яка може бути протестована у віртуальному середовищі перед фізичною реалізацією.

Датчик руху PIR підключений до піна GPIO 7 плати ESP32 Dev Module, що дозволяє отримувати сигнали про виявлення руху в зоні спостереження. Живлення датчика забезпечується від стабілізованого джерела 3.3V, доступного на платі, а заземлення (GND) підключено до відповідного піна ESP32 для створення повного електричного кола. Таке підключення гарантує стабільну роботу датчика та швидке передавання сигналу логічного рівня "HIGH" при виявленні руху, що є основою для активації подальших дій системи, таких як запуск зйомки. У симуляторі Wokwi це підключення дозволяє точно відтворити поведінку датчика, що сприяє тестуванню логіки роботи системи в різних сценаріях.

Світлодіод (LED), який у симуляції Wokwi імітує роботу камери OV2640, підключений до піна GPIO 2 через резистор номіналом 220 Ом, що обмежує струм і запобігає пошкодженню компонента. Увімкнення LED відповідає моменту "захоплення" зображення, що дозволяє розробникам візуально відстежувати спрацьовування камери в процесі тестування. Такий підхід є ефективним для перевірки коректності алгоритмів у симуляційному середовищі, де фізична камера недоступна, але потрібно оцінити логіку активації та обробки даних. У реальній системі камера OV2640 підключалася б через I2C-інтерфейс, але в симуляції LED забезпечує достатній рівень імітації для відпрацювання сценаріїв зйомки та відправки зображень через Telegram-бота.

Модуль SD-карти підключений до плати ESP32 через SPI-інтерфейс, який забезпечує швидку та надійну передачу даних для збереження зображень. У схемі використано піни GPIO 5 (CS, чип-селект), GPIO 23 (MOSI, передача даних від контролера до модуля), GPIO 19 (MISO, передача даних від модуля до контролера) і GPIO 18 (SCK, тактовий сигнал). Живлення SD-карти здійснюється через джерело 3.3V і заземлення (GND) від плати ESP32, що забезпечує стабільну роботу модуля. У симуляторі Wokwi модуль SD-карти імітує операції запису та

читання файлів, дозволяючи перевірити, як система обробляє зображення перед їхньою відправкою через мережу. Таке підключення обґрунтоване необхідністю створення надійного резервного копіювання даних, що є критично важливим для забезпечення функціональності системи в умовах нестабільного мережевого з'єднання. Завдяки ретельно продуманій схемі підключення та можливостям симуляції в Wokwi, система забезпечує стабільну взаємодію всіх компонентів, що є основою для створення ефективної кіберфізичної системи захисту будинку що зображена на рисунку 3.5.

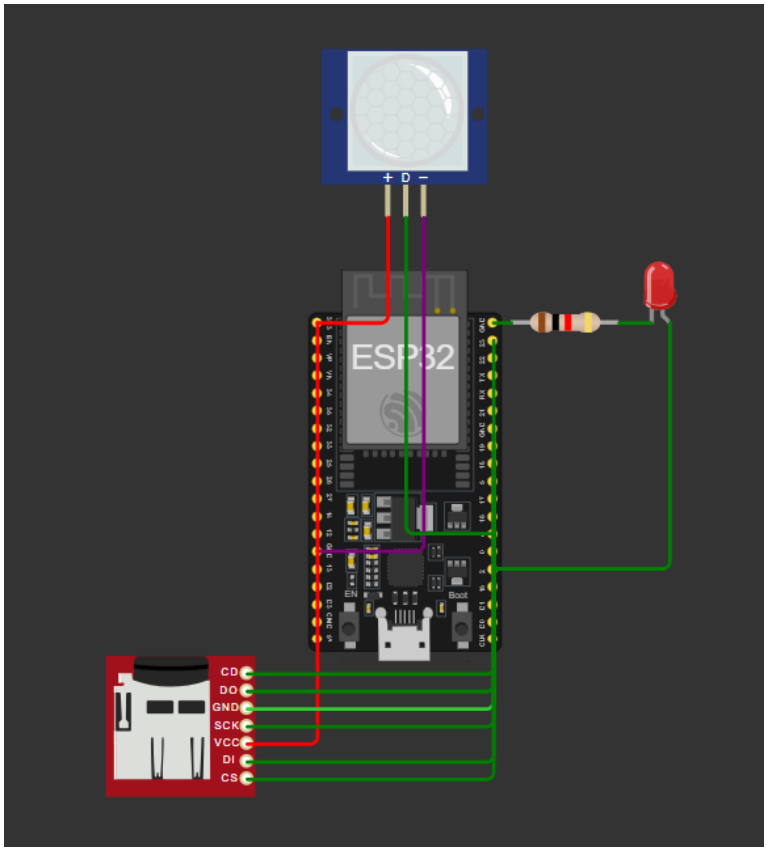


Рисунок 3.5 – Схема підключень у симуляції [40]

Така конфігурація пінів для підключення компонентів системи була ретельно обрана з урахуванням їхньої сумісності та необхідності уникнення конфліктів між різними модулями, що забезпечує стабільну та ефективну роботу системи. Наприклад, пін GPIO 5 для сигналу чип-селект (CS) модуля SD-карти був вибраний через його доступність і відсутність перетинання з іншими

активними пінами, що використовуються для датчика руху чи імітації камери. Лінії SPI-інтерфейсу, а саме GPIO 23 (MOSI), GPIO 19 (MISO) і GPIO 18 (SCK), відповідають стандартній конфігурації апаратного SPI на платі ESP32 Dev Module, що гарантує високу швидкість і надійність передачі даних між мікроконтролером і SD-картою. Використання апаратного SPI, а не програмного, дозволяє оптимізувати продуктивність системи, зменшуючи навантаження на процесор і забезпечуючи стабільну роботу навіть при інтенсивному записі даних. У симуляційному середовищі Wokwi ця схема підключення дає змогу точно відтворити взаємодію всіх компонентів, дозволяючи розробникам перевірити, як система реагує на виявлення руху датчиком PIR, записує зображення на SD-карту та імітує відправку даних через Telegram-бота.

Використання симулятора Wokwi значно прискорює процес розробки, оскільки дозволяє тестувати апаратну логіку системи без необхідності використання фізичних компонентів. У віртуальному середовищі можна моделювати різні сценарії, такі як спрацьовування датчика руху, запис даних на SD-карту чи обробка зображень, і перевіряти коректність роботи системи в реальному часі. Це дає змогу виявити потенційні проблеми, такі як неправильне налаштування пінів, конфлікти між інтерфейсами чи затримки в обробці сигналів, ще на етапі симуляції. Наприклад, Wokwi дозволяє відстежувати, як плата ESP32 обробляє сигнали від датчика PIR і активує імітацію зйомки через увімкнення LED на GPIO 2, а також перевірити, чи коректно дані записуються на віртуальну SD-карту через SPI-інтерфейс. Такий підхід не лише економить час і ресурси, але й підвищує надійність системи, дозволяючи розробникам удосконалити програмний код перед його розгортанням на реальному обладнанні.

Особливу увагу в проєкті приділено налаштуванню камери OV2640 у програмному коді, де вручну визначені піни для передачі даних (Y2-Y9 для відеоданих, VSYNC, HREF і PCLK для синхронізації), що відповідає реальній конфігурації плати ESP32-CAM. Хоча в симуляторі Wokwi фізична камера недоступна, ці піни не використовуються напряму, а їхнє визначення в коді

забезпечує підготовку системи до переходу на реальне обладнання, зберігаючи сумісність із апаратною частиною. У симуляції робота камери імітується через увімкнення LED на GPIO 2, що відображає момент "захоплення" зображення, а відправка зображень через Telegram-бота замінена на вивід відповідних повідомлень у Serial Monitor. Це дозволяє розробникам перевірити логіку обробки подій, наприклад, коректність активації камери після сигналу від датчика руху PIR, а також переконатися, що система правильно формує команди для передачі даних через віртуальний Wi-Fi-модуль. Такий підхід забезпечує детальне тестування всіх етапів роботи системи, від виявлення руху до збереження та передачі даних, що робить симуляцію в Wokwi незамінним інструментом для створення надійної кіберфізичної системи захисту будинку.

3.3 Принцип роботи в реальному житті

Кіберфізична система захисту, розроблена в рамках цього проєкту, призначена для встановлення в зонах, що потребують постійного моніторингу, наприклад, у коридорі складу, де зберігаються цінні матеріали, або в приватному будинку для забезпечення безпеки. Центральним елементом системи є плата ESP32 Dev Module, яка виконує функцію головного контролера, ініціалізуючи та координуючи роботу всіх підключених компонентів: датчика руху PIR, камери OV2640 і модуля SD-карти. Процес ініціалізації включає налаштування пінів GPIO, запуск SPI- та I2C-інтерфейсів для взаємодії з модулями, а також підключення до локальної Wi-Fi мережі для забезпечення дистанційного зв’язку. Завдяки інтеграції з Telegram-ботом система здатна відправляти сповіщення користувачу в реальному часі, що робить її зручною для віддаленого моніторингу та оперативного реагування на події.

Датчик руху PIR, який є ключовим елементом системи, постійно сканує зону спостереження, використовуючи інфрачервоне випромінювання для виявлення змін у тепловому полі середовища. Цей принцип роботи, характерний

для більшості сучасних PIR-датчиків, таких як ті, що застосовуються в системах безпеки Ajax або Hikvision, дозволяє ефективно виявляти рух живих об’єктів, наприклад, людини чи тварини, навіть у темряві. Датчик налаштований на високу чутливість, що забезпечує надійне спрацьовування в реальних умовах, наприклад, у слабо освітленому складському приміщенні. Підключення до локальної Wi-Fi мережі дозволяє платі ESP32 взаємодіяти з Telegram-ботом, забезпечуючи відправку сповіщень користувачу про виявлені події, що значно підвищує зручність і функціональність системи.

Коли датчик PIR виявляє рух, наприклад, якщо людина входить у зону спостереження о 02:00 ночі, він генерує сигнал логічного рівня "HIGH" на піні GPIO 7. Плата ESP32 миттєво обробляє цей сигнал, активуючи камеру OV2640 для фіксації зображення. У реальній системі камера OV2640, яка зазвичай має роздільну здатність 2 МП (1600x1200 пікселів), створює знімок у форматі JPEG із заданими параметрами якості, наприклад, якість 10, що дозволяє економити місце на SD-карті без значної втрати деталізації. Ця функція подібна до механізмів, що використовуються в професійних камерах відеоспостереження, таких як Dahua або Axis, де зображення оптимізуються для ефективного зберігання. Знімок одразу записується на SD-карту через SPI-інтерфейс, що забезпечує надійне резервне копіювання даних, навіть якщо Wi-Fi з’єднання тимчасово недоступне. Це гарантує збереження критичної інформації для подальшого аналізу, наприклад, для розслідування інцидентів або моніторингу активності.

Після запису зображення на SD-карту ESP32 надсилає його через Wi-Fi до Telegram-бота, який доставляє сповіщення користувачу разом із прикріпленим зображенням. Цей процес забезпечує оперативне інформування про події, що дозволяє власнику швидко реагувати на потенційні загрози, наприклад, викликаючи охорону або перевіряючи ситуацію через додаткові канали. У реальних умовах система може бути налаштована на періодичну зйомку або серійну фотозйомку при тривалому виявленні руху, що підвищує її ефективність у складних сценаріях. Таким чином, принцип роботи системи в реальному житті

демонструє її здатність забезпечувати надійний моніторинг, локальне зберігання даних і дистанційне сповіщення, що робить її цінним рішенням для забезпечення безпеки в приватних будинках або комерційних приміщеннях.

Рисунок 3.6 – Камера типу Dahua[29]

Після виявлення руху та захоплення зображення камерою OV2640 плата ESP32 через вбудований Wi-Fi модуль відправляє отримане зображення Telegram-боту, який, у свою чергу, надсилає його власнику об’єкта для оперативного інформування. Цей процес, залежно від швидкості та стабільності Wi-Fi мережі, займає від кількох секунд до кількох десятків секунд, що можна порівняти з роботою сучасних камер відеоспостереження, таких як Xiaomi Yi або Wyze що зображена на рисунку 3.8, які надсилають push-сповіщення через спеціалізовані додатки. Наприклад, якщо рух було виявлено о 02:00 ночі, власник отримує сповіщення в Telegram-чати вже о 02:01, разом із повідомленням "Тривога: Виявлено рух!" і прикріпленим зображенням у форматі JPEG. Це дозволяє негайно оцінити ситуацію: якщо на зображенні видно сторонню особу чи підозрілу активність, власник може швидко вжити заходів, наприклад, викликати охоронну службу, зв’язатися з сусідами або активувати додаткові системи безпеки, такі як сирена чи освітлення.

Розглянемо детальний сценарій, у якому зловмисник намагається проникнути на склад через бічні двері в нічний час. Прилад встановлений у стратегічно важливій зоні: датчик руху PIR налаштований так, щоб охоплювати всю зону входу, а камера OV2640 спрямована безпосередньо на двері, забезпечуючи чітке захоплення зображень. О 03:15 ночі зловмисник відчиняє двері, і його теплове випромінювання, викликане рухом, активує датчик PIR. Датчик миттєво генерує сигнал логічного рівня "HIGH" на піні GPIO 7, який передається до плати ESP32. Система негайно реагує, активуючи камеру OV2640, яка робить знімок із роздільною здатністю 2 МП у форматі JPEG. У реальних умовах OV2640 підтримує нічну зйомку за наявності інфрачервоного (ІЧ) підсвічування, подібно до камер Arlo або Ring, що дозволяє зафіксувати чіткий силует людини навіть у повній темряві, якщо ІЧ-підсвітка додатково встановлена.

Зображення, отримане камерою, одразу записується на SD-карту через SPI-інтерфейс, що забезпечує надійне резервне копіювання даних у разі втрати мережевого з’єднання, наприклад, через навмисне відключення Wi-Fi зловмисником або технічний збій. Паралельно ESP32 відправляє зображення через Telegram-бота, використовуючи вбудований Wi-Fi модуль. Власник складу, який перебуває вдома або в іншому місці, отримує сповіщення о 03:16, що містить зображення та текстове повідомлення про тривогу. Переглянувши знімок, він бачить невідому особу біля дверей складу і негайно викликає охоронну службу, яка прибуває на місце через 10 хвилин. Ця швидка реакція дозволяє запобігти потенційній крадіжці або пошкодженню майна. Локальне зберігання на SD-карті відіграє ключову роль, оскільки зображення залишається доступним для подальшого аналізу навіть у разі фізичного пошкодження приладу зловмисником. Така функція подібна до можливостей професійних камер відеоспостереження Reolink або Amcrest, які зберігають записи на карті пам’яті для використання як доказів у правоохоронних органах.

Крім того, система може бути налаштована для виконання додаткових дій у реальних умовах, наприклад, активації звукової сигналізації чи увімкнення

освітлення в зоні спостереження, що може відлякати зловмисника. У разі тривалого виявлення руху датчик PIR може ініціювати серію знімків, які також зберігаються на SD-карті та відправляються через Telegram, що забезпечує повніший огляд ситуації. Ця гнучкість і надійність системи, підкріплена локальним зберіганням і дистанційним сповіщенням, робить її ефективним рішенням для захисту складських приміщень, приватних будинків або інших об’єктів, де потрібен постійний моніторинг. Завдяки інтеграції з Telegram-ботом і резервному копіюванню на SD-карті система забезпечує оперативність, безпеку даних і можливість швидкого реагування, що відповідає вимогам сучасних систем безпеки.

Рисунок 3.7 – Камера типу Reolink [28]

У реальних умовах експлуатації кіберфізична система захисту, побудована на базі плати ESP32 Dev Module, може стикатися з низкою викликів, таких як перебої в електроживленні, нестабільне Wi-Fi з’єднання або зовнішні перешкоди, які впливають на роботу датчика руху. Для забезпечення надійності та стабільності системи ці потенційні проблеми було враховано під час розробки програмного забезпечення та апаратної конфігурації. Зокрема, плата ESP32 запрограмована на періодичну перевірку стану Wi-Fi мережі, що дозволяє

виявляти втрату з’єднання та автоматично відновлювати його, коли мережа знову стає доступною. У разі невдалої спроби відправки зображення через Telegram-бота, наприклад, через тимчасову відсутність мережі, система виконує повторні спроби передачі даних із заданим інтервалом, що є стандартною практикою в сучасних системах відеоспостереження, таких як Wyze Cam або Blink Outdoor. Цей механізм гарантує, що важливі сповіщення та зображення дійдуть до користувача, навіть якщо мережеве з’єднання зазнає тимчасових збоїв.

Для підвищення надійності системи в умовах перебоїв із електроживленням передбачено можливість підключення резервного джерела живлення, наприклад, акумулятора, який може підтримувати роботу приладу протягом кількох годин. Це дозволяє системі продовжувати фіксувати події та зберігати зображення на SD-карту навіть за відсутності основного живлення, що є критично важливим для забезпечення безпеки в таких місцях, як склади чи приватні будинки. Крім того, датчик руху PIR, підключений до GPIO 7, має вбудовану програмну затримку (debounce) у 5 секунд, яка запобігає помилковим спрацьовуванням, викликаним короткочасними змінами в зоні спостереження, наприклад, рухом тварин, коливаннями температури або вібраціями від зовнішніх джерел, таких як проїжджаючий транспорт. Цей механізм подібний до технологій, застосованих у професійних датчиках руху від компаній Bosch або Paradox, де алгоритми фільтрації забезпечують високу точність виявлення реальних подій.

У реальних сценаріях використання затримка в 5 секунд дозволяє системі ігнорувати незначні рухи, наприклад, переміщення домашніх тварин, таких як кішки чи невеликі собаки, або тимчасові зміни теплового поля, викликані протягами чи нагріванням поверхонь сонцем. Це підвищує ефективність системи, зменшуючи кількість хибних сповіщень і дозволяючи користувачу зосередитися на дійсно важливих подіях. Наприклад, у випадку, коли датчик PIR виявляє рух людини в зоні спостереження, система активує камеру OV2640 лише після підтвердження стабільного сигналу, що забезпечує економію ресурсів і зниження навантаження на SD-карту та Wi-Fi модуль. У симуляції Wokwi ці механізми

також можна протестувати, налаштувавши віртуальний датчик PIR для імітації різних типів руху та перевіряючи, як система обробляє сигнали з урахуванням затримки та фільтрації.

Крім того, програмний код для ESP32 включає механізми діагностики, які дозволяють системі реєструвати помилки, такі як невдалі спроби запису на SD-карту чи проблеми з ініціалізацією камери, і повідомляти про них через Serial Monitor у симуляції або через Telegram у реальних умовах. Це забезпечує додатковий рівень контролю, дозволяючи користувачу або розробнику швидко виявляти та усувати несправності. Таким чином, завдяки продуманому програмному забезпеченню, яке враховує можливі перебої в живленні, нестабільність мережі та хибні спрацьовування датчика, система демонструє високу надійність і готовність до роботи в реальних умовах, подібно до комерційних рішень, таких як камери Yi або Ajax, забезпечуючи ефективний захист об’єктів і комфорт для користувача.

Рисунок 3.8 – Камера типу Wyze Cam [31]

Крім того, камера OV2640 у реальній системі може бути значно вдосконалена шляхом додавання інфрачервоних (ІЧ) діодів, які забезпечують ефективну нічну зйомку, що є критично важливим для моніторингу в умовах

низького освітлення або повної темряви. ІЧ-підсвітка дозволяє камері фіксувати чіткі зображення навіть уночі, що значно підвищує якість і розбірливість знімків, подібно до технологій, застосованих у професійних камерах відеоспостереження, таких як Arlo або Ring. Наприклад, при виявленні руху в темному коридорі складу о 03:00 ночі ІЧ-діоди автоматично активуються, забезпечуючи достатнє освітлення для камери OV2640, яка може захоплювати зображення з роздільною здатністю до 2 МП у форматі JPEG. Це дозволяє чітко розпізнавати об’єкти чи особи, що є важливим для ідентифікації потенційних загроз і подальшого аналізу подій.

Модуль SD-карти, інтегрований у систему через SPI-інтерфейс, підтримує цикли перезапису, що забезпечує ефективне використання доступного простору пам’яті. Ця функція подібна до механізмів, застосованих в автомобільних відеореєстраторах, таких як BlackVue або Thinkware, де старі файли автоматично перезаписуються, коли SD-карта заповнена. У системі захисту це дозволяє зберігати нові зображення без необхідності ручного очищення пам’яті, що особливо корисно в умовах тривалого використання, наприклад, при цілодобовому моніторингу складу чи приватного будинку. Для оптимізації простору зображення зберігаються з налаштуваннями якості JPEG, які балансують між чіткістю та розміром файлів, що зменшує частоту перезапису та подовжує термін служби SD-карти. У реальних умовах користувач може налаштувати систему так, щоб зберігати лише критичні зображення, наприклад, ті, що пов’язані з тривожними подіями, а решту перезаписувати після певного періоду.

Усе це забезпечує високу надійність системи в реальних умовах експлуатації, дозволяючи власнику об’єкта оперативно реагувати на потенційні загрози. Наприклад, у разі отримання сповіщення через Telegram-бота з прикріпленим зображенням, власник може негайно оцінити ситуацію та прийняти рішення, наприклад, викликати охорону або перевірити об’єкт самостійно. Локальне зберігання даних на SD-карті додає додатковий рівень безпеки, оскільки

зображення залишаються доступними навіть у разі відключення Wi-Fi чи пошкодження приладу. Крім того, система може бути доповнена функціями, такими як автоматичне надсилання серії знімків у разі тривалого виявлення руху, що забезпечує більш повну картину події. Ці можливості, у поєднанні з підтримкою нічного режиму камери OV2640 та ефективним управлінням пам’яттю SD-карти, роблять систему гнучким і надійним рішенням для захисту об’єктів, подібно до комерційних систем безпеки, таких як Reolink або Dahua що зображені на рисунку 3.6 та 3.7. Таким чином, розроблена кіберфізична система не лише забезпечує оперативне реагування на загрози, але й гарантує збереження важливих даних для подальшого аналізу, що підвищує її цінність для користувачів.

3.4 Робота з TelegramBot

Розроблена система відеоспостереження, побудована на базі ESP32 Dev Module, інтегрує функцію віддаленого сповіщення через Telegram-бота, що є ключовим елементом для оперативного інформування користувача про виявлені події. Telegram-бот виконує роль посередника між апаратною частиною системи та власником об’єкта, забезпечуючи передачу текстових повідомлень і зображень у реальному часі.

Telegram-бот налаштований для автоматичного реагування на тригери, отримані від системи відеоспостереження. Його функціонал включає три основні етапи: сповіщення про виявлення руху, підготовку та відправку зображення, а також звіт про статус операції. Ця логіка забезпечує користувачу чітке розуміння того, що відбувається в зоні спостереження, і дозволяє швидко реагувати на потенційні загрози.

Спочатку бот надсилає повідомлення про підключення до плати"Бот під'єднано до ESP32 №5612". Сповіщення про виявлення руху Коли датчик руху PIR, підключений до GPIO 7, виявляє рух у зоні спостереження

(наприклад, о 04:32 ночі), ESP32 Dev Module обробляє сигнал і активує камеру OV2640 для створення знімка. Одразу після цього Telegram-бот надсилає перше повідомлення в чат користувача: "Тривога: Виявлено рух!" що зображено на рисунку 3.9. Це повідомлення слугує миттєвим сигналом для власника, що в зоні моніторингу відбувається активність.

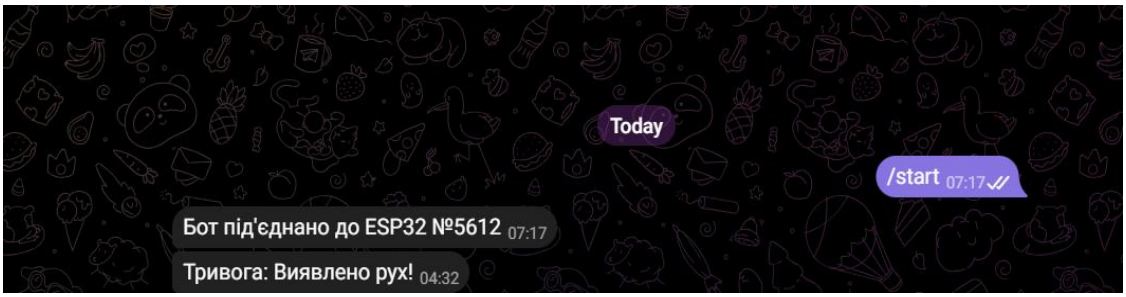


Рисунок 3.9 – Сповіщення про приєднання і тривогу

Після захоплення зображення камерою OV2640 (у реальному житті це JPEG-зображення з роздільною здатністю 2 МП), знімок зберігається на SD-карті через SPI-інтерфейс для резервного копіювання. У цей момент Telegram-бот надсилає наступне повідомлення: "Фото зроблено, відправляємо в Telegram...". Це повідомлення інформує користувача про те, що система переходить до етапу передачі зображення, що займає кілька секунд залежно від швидкості Wi-Fi з’єднання. ESP32 через вбудований Wi-Fi модуль передає зображення до Telegram-серверів, використовуючи API бота.

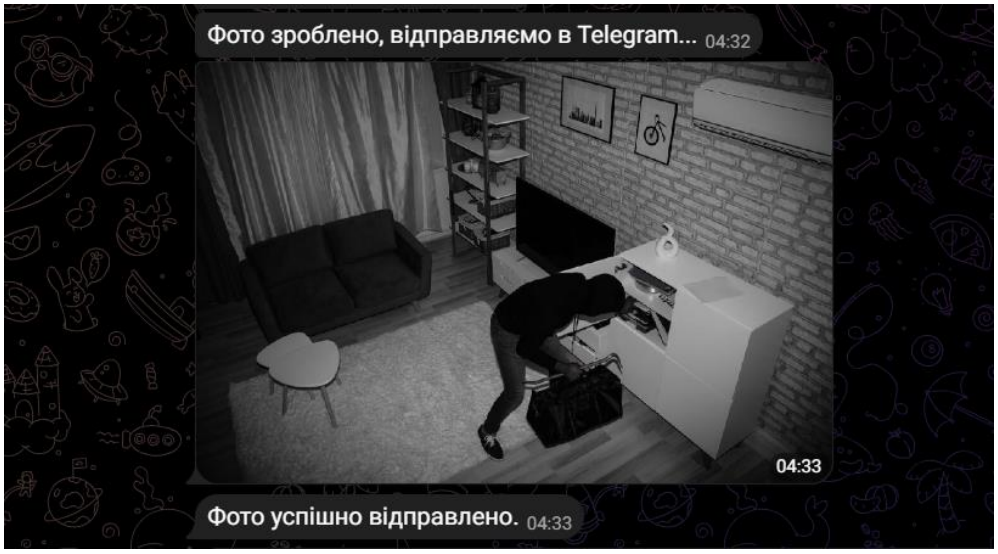


Рисунок 2.10 – Сповіщення про відправку і знімок

У разі успішної відправки зображення (наприклад, о 04:33, коли власник отримує знімок із силуетом) що зображено на рисунку 3.10, Telegram-бот надсилає завершальне повідомлення: "Фото успішно відправлено". Це підтвердження дозволяє користувачу бути впевненим, що зображення доставлено, і він може оцінити ситуацію, наприклад, викликати охорону, якщо бачить зловмисника. Якщо ж відправка не вдається через нестабільне Wi-Fi з'єднання, перебої в електроживленні чи інші технічні проблеми, бот надсилає повідомлення: "Не вдалося відправити фото" що зображено на рисунку 3.11. У такому випадку зображення залишається на SD-карті, і система може спробувати повторну відправку після відновлення зв'язку, подібно до механізмів повторної передачі в камерах Wyze Cam.

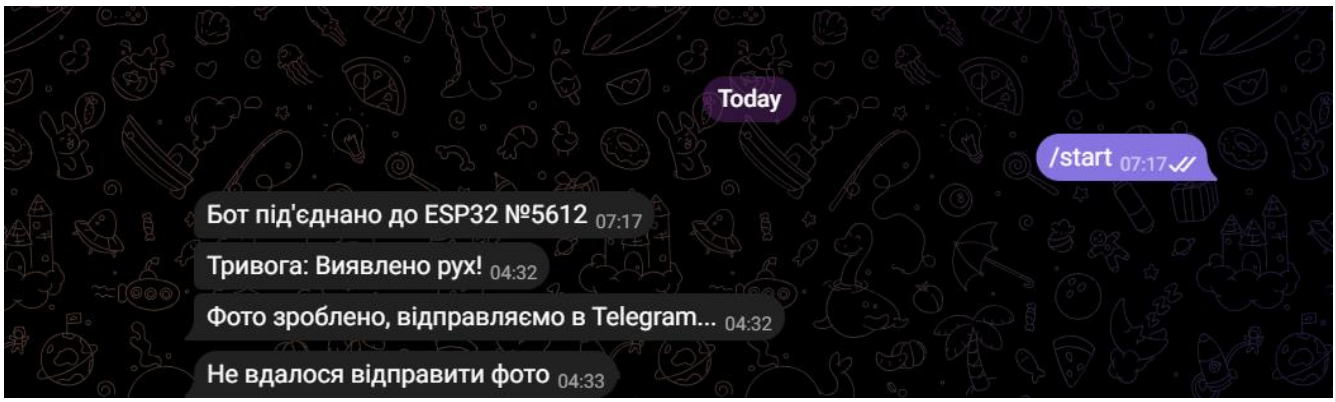


Рисунок 3.11 – Повідомлення про проблему

Для реалізації цієї логіки Telegram-бот використовує бібліотеку UniversalTelegramBot, яка забезпечує стабільну взаємодію з API Telegram. ESP32 Dev Module періодично перевіряє стан мережі, щоб гарантувати доставку повідомлень, а також має механізм повторних спроб у разі невдачі. У реальному сценарії це дозволяє системі працювати надійно навіть у складних умовах, наприклад, під час тимчасових збоїв у мережі складу. Користувач отримує чіткий ланцюжок повідомлень: від сповіщення про рух до підтвердження доставки зображення, що робить систему зручною та інформативною для моніторингу.

3.5 Висновок до третього розділу

У процесі розробки проекту було створено плату з компонентами, яка успішно інтегрована та підключена. Розроблено код, що дозволив через симуляцію сформувати функціональну плату та налаштувати підключення Telegram-бота. Створення бота спрямоване на забезпечення швидкої обробки даних, оптимізацію сповіщень і зручного управління системою. Тестування в симуляційному середовищі підтвердило коректність роботи як апаратної, так і програмної частин, а також стабільність передачі інформації. Отримані результати вказують на готовність системи до практичного використання та її потенціал для подальшого розширення функціоналу.

ВИСНОВОК

У цій роботі розроблено економічну, результативну та зручну у впровадженні систему спостереження, створену на основі платформи ESP32 Dev Module, для забезпечення захисту приватних осель. Запропоноване рішення об'єднує сенсор руху PIR, камеру OV2640 і модуль для зберігання даних на SD-карті, що дозволяє виявляти активність, записувати зображення та надсилати повідомлення через Telegram-бота. Результати тестування у симуляторі Wokwi підтвердили стабільність обробки сигналів, швидке збереження інформації та надійну передачу фотографій, що свідчить про можливість практичного застосування системи.

Однією з головних переваг створеної системи є її доступність і гнучкість у модифікації. Застосування ESP32 Dev Module разом із бюджетними елементами, такими як сенсор руху PIR і камера OV2640, забезпечує низьку вартість без компромісів у функціональності. Завдяки модульному підходу систему можна легко адаптувати до різних умов використання, додаючи нові компоненти за потребою.

Можливість інтеграції з Telegram-ботом і локальним збереженням даних на SD-карті є ще однією значущою особливістю. Це гарантує оперативне сповіщення користувача про зафіксовані події та створення резервних копій, що підвищує надійність роботи навіть при нестабільному інтернет-з’єднанні. Тестування у Wokwi дало змогу вдосконалити алгоритми, забезпечивши швидку реакцію на рух і оптимальне використання ресурсів.

Теоретичний аналіз допоміг визначити найкращі параметри для компонентів і їхньої взаємодії, а тестування у Wokwi підтвердило правильність функціонування системи у віртуальних умовах. Отримані дані вказують на перспективність таких рішень для захисту майна, відкриваючи шлях до їхнього подальшого розвитку та впровадження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Al-Fuqaha A., Guizani M., Mohammadi M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials. 2015. Vol.17(4). P. 2347-2376. URL: https://ieeexplore.ieee.org/document/7156143 (дата звернення: 11.05.2025)

2. Gubbi J., Buyya R., Marusic S. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013. Vol.29(7). P. 1645-1660. URL: https://www.sciencedirect.com/science/article/pii/S0167739X13000241 (дата звернення: 11.05.2025)

3. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. Computer Networks. 2010. Vol.54(15). P. 2787-2805. URL: https://www.sciencedirect.com/science/article/pii/S1389128610001568 (дата звернення: 11.05.2025)

4. Sicari S., Rizzardi A., Grieco L. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks. 2015. Vol.76. P. 146-164. URL: https://www.sciencedirect.com/science/article/pii/S1389128614003917 (дата звернення: 11.05.2025)

5. Banzi M., Cuartielles D. Getting Started with Arduino: The Open Source Electronics Prototyping Platform. Maker Media, Inc. 2011. 128 p. URL: https://www.arduino.cc/en/Guide (дата звернення: 12.05.2025)

6. Margolis M. Arduino Cookbook. O'Reilly Media. 2011. 724 p. URL: https://www.oreilly.com/library/view/arduino-cookbook/9781449320697/ (дата звернення: 12.05.2025)

7. McRoberts M. Beginning Arduino. Apress. 2010. 417 p. URL: https://link.springer.com/book/10.1007/978-1-4302-3240-7 (дата звернення: 12.05.2025)

8. Espressif Systems. ESP32 Series Datasheet. 2023. URL: https://www.espressif.com/en/support/documents/technical-documents (дата звернення: 12.05.2025)

9. Adafruit. OV2640 Camera Module Guide. 2022. URL: https://learn.adafruit.com/adafruit-ov2640-camera (дата звернення: 12.05.2025)

10. Arduino. PIR Motion Sensor Tutorial. 2021. URL: https://www.arduino.cc/en/Tutorial/PIRMotionSensor (дата звернення: 12.05.2025)

11. Wokwi. Wokwi Arduino Simulator Documentation. 2023. URL: https://docs.wokwi.com/ (дата звернення: 12.05.2025)

12. Ray P. P. A survey on Internet of Things architectures. Journal of King Saud University - Computer and Information Sciences. 2018. Vol.30(3). P. 291-319. URL: https://www.sciencedirect.com/science/article/pii/S1319157817300836 (дата звернення: 12.05.2025)

13. Li S., Xu L. D., Zhao S. 5G Internet of Things: A survey. IEEE Internet of Things Journal. 2018. Vol.5(5). P. 2322-2333. URL: https://ieeexplore.ieee.org/document/8366117 (дата звернення: 13.05.2025)

14. Kumar S., et al. Smart security solutions using IoT. International Journal of Electrical and Computer Engineering. 2020. Vol.10(3). P. 2345-2352. URL: https://ijece.iaescore.com/index.php/IJECE/article/view/21598 (дата звернення: 13.05.2025)

15. Kolias C., Kambourakis G., Stavrou A. Intrusion detection in IoT: A survey. ACM Computing Surveys. 2017. Vol.50(3). P. 1-36. URL: https://dl.acm.org/doi/10.1145/3057266 (дата звернення: 13.05.2025)

16. Ajax Systems. Ajax Security Systems Documentation. 2023. URL: https://support.ajax.systems/en/ (дата звернення: 13.05.2025)

17. Paradox Security Systems. Product Catalog 2023. URL: https://www.paradox.com/en/products (дата звернення: 13.05.2025)

18. Eldes. Eldes Security Systems Manual. 2022. URL: https://www.eldesalarms.com/support/manuals (дата звернення: 13.05.2025)

19. IEEE. IEEE Standard for IoT Security. 2020. URL: https://standards.ieee.org/standard/2410-2020.html (дата звернення: 13.05.2025)

20. European Union Agency for Cybersecurity (ENISA). IoT Security Good Practices. 2021. URL: https://www.enisa.europa.eu/publications/iot-security-good-practices (дата звернення: 13.05.2025)

21. Chen H., et al. A review of security and privacy issues in IoT. Journal of Network and Computer Applications. 2019. Vol.126. P. 45-62. URL: https://www.sciencedirect.com/science/article/pii/S1084804518303770 (дата звернення: 13.05.2025)

22. Arduino. Arduino IDE User Manual. 2023. URL: https://www.arduino.cc/en/Guide/Environment (дата звернення: 13.05.2025)

23. Espressif Systems. ESP-IDF Programming Guide. 2023. URL: https://docs.espressif.com/projects/esp-idf/en/latest/ (дата звернення: 14.05.2025)

24. Adafruit. SD Card Module Guide. 2022. URL: https://learn.adafruit.com/adafruit-micro-sd-breakout-board-card (дата звернення: 14.05.2025)

25. IEEE. IEEE 802.11 Standard for Wireless LAN. 2021. URL: https://standards.ieee.org/standard/802_11-2020.html (дата звернення: 14.05.2025)

26. Kumar A., et al. IoT-based smart home security system. IEEE Transactions on Industrial Informatics. 2019. Vol.15(4). P. 2243-2250. URL: https://ieeexplore.ieee.org/document/8493456 (дата звернення: 14.05.2025)

27. Mishra B., et al. Security challenges in IoT devices. International Journal of Advanced Computer Science and Applications. 2018. Vol.9(1). P. 23-30. URL: https://thesai.org/Publications/ViewPaper?Volume=9&Issue=1&Code=IJACSA&SerialNo=3 (дата звернення: 14.05.2025)

28. Reolink. Reolink Camera User Manual. 2023. URL: https://support.reolink.com/hc/en-us/articles/360009675054 (дата звернення: 14.05.2025)

29. Dahua Technology. Dahua Security Camera Guide. 2022. URL: https://www.dahuasecurity.com/support/technical-support (дата звернення: 14.05.2025)

30. Arlo Technologies. Arlo Security Camera Manual. 2023. URL: https://www.arlo.com/en-us/support/ (дата звернення: 14.05.2025)

31. Wyze Labs. Wyze Cam User Guide. 2022. URL: https://support.wyze.com/hc/en-us/articles/360016684671 (дата звернення: 14.05.2025)

32. Ring. Ring Security Camera Documentation. 2023. URL: https://support.ring.com/hc/en-us (дата звернення: 14.05.2025)

33. Bosch Security Systems. Motion Detector Guide. 2021. URL: https://www.boschsecurity.com/us/en/product/ (дата звернення: 14.05.2025)

34. Hikvision. Hikvision Camera Installation Manual. 2022. URL: https://www.hikvision.com/en/support/technical-support (дата звернення: 15.05.2025)

35. Raspberry Pi Foundation. Raspberry Pi Camera Module Guide. 2023. URL: https://www.raspberrypi.com/documentation/accessories/camera.html (дата звернення: 15.05.2025)

36. IEEE. IEEE Standard for Ethernet. 2020. URL: https://standards.ieee.org/standard/802_3-2018.html (дата звернення: 15.05.2025)

37. International Electrotechnical Commission (IEC). IEC 62368-1 Safety Standard. 2021. URL: https://webstore.iec.ch/publication/62605 (дата звернення: 15.05.2025)

38. European Telecommunications Standards Institute (ETSI). ETSI TS 103 645 IoT Security Standard. 2020. URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.01_60/ts_103645v020101p.pdf (дата звернення: 15.05.2025)

39. Arduino. ESP32-CAM Development Guide. 2023. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32s2/api-reference/peripherals/camera.html (дата звернення: 15.05.2025)

40. Wokwi. ESP32 Dev Module Simulation Guide. 2023. URL: https://wokwi.com/parts/esp32-dev-module (дата звернення: 15.05.2025)

41. IEEE. IEEE 802.15.4 Standard for Low-Rate Wireless Networks. 2020. URL: https://standards.ieee.org/standard/802_15_4-2020.html (дата звернення: 15.05.2025)

42. International Organization for Standardization (ISO). ISO/IEC 27001 Information Security Management. 2013. URL: https://www.iso.org/standard/54534.html (дата звернення: 15.05.2025)

43. Adafruit. PIR Sensor Datasheet. 2022. URL: https://www.adafruit.com/product/189 (дата звернення: 15.05.2025)

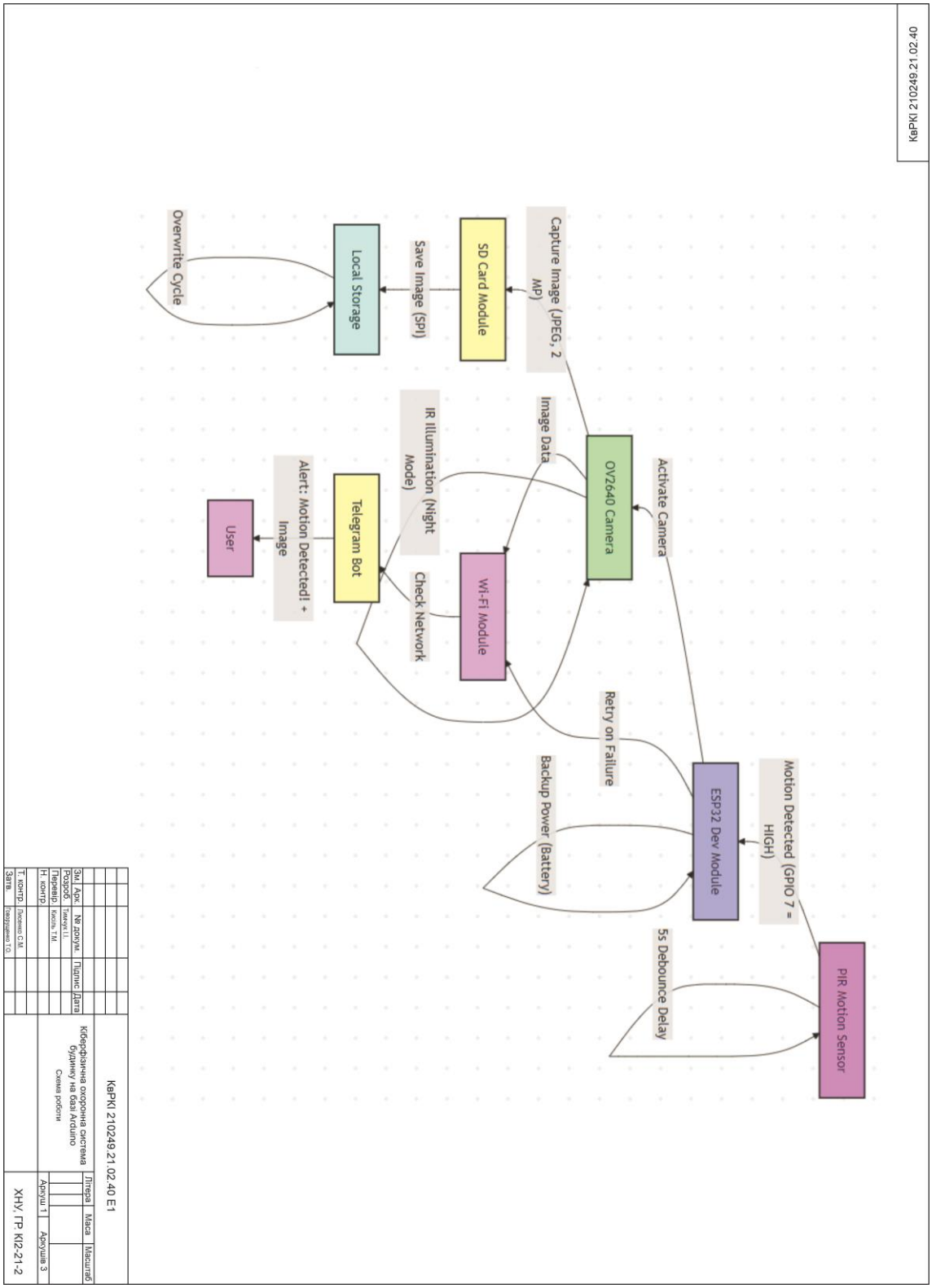
44. Espressif Systems. OV2640 Camera Integration with ESP32. 2023. URL: https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-reference/peripherals/camera.html (дата звернення: 16.05.2025)

45. • Arduino Project Hub. IoT Security Projects with ESP32. 2023. URL: https://create.arduino.cc/projecthub (дата звернення: 16.05.2025)

Додаток А

(обов’язковий)

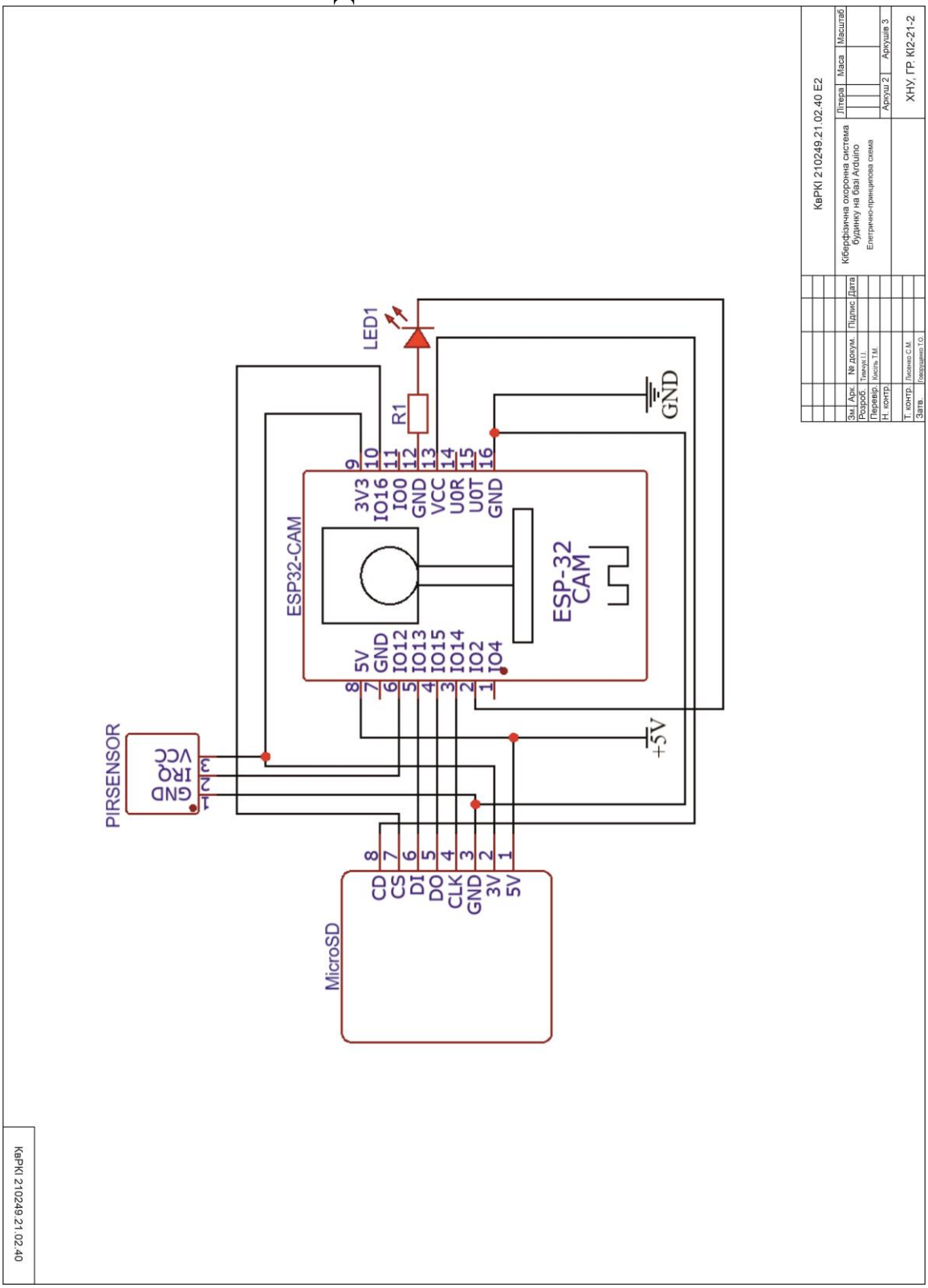
БЛОК-СХЕМА РОБОТИ ПЗ



Додаток Б

(обов’язковий)

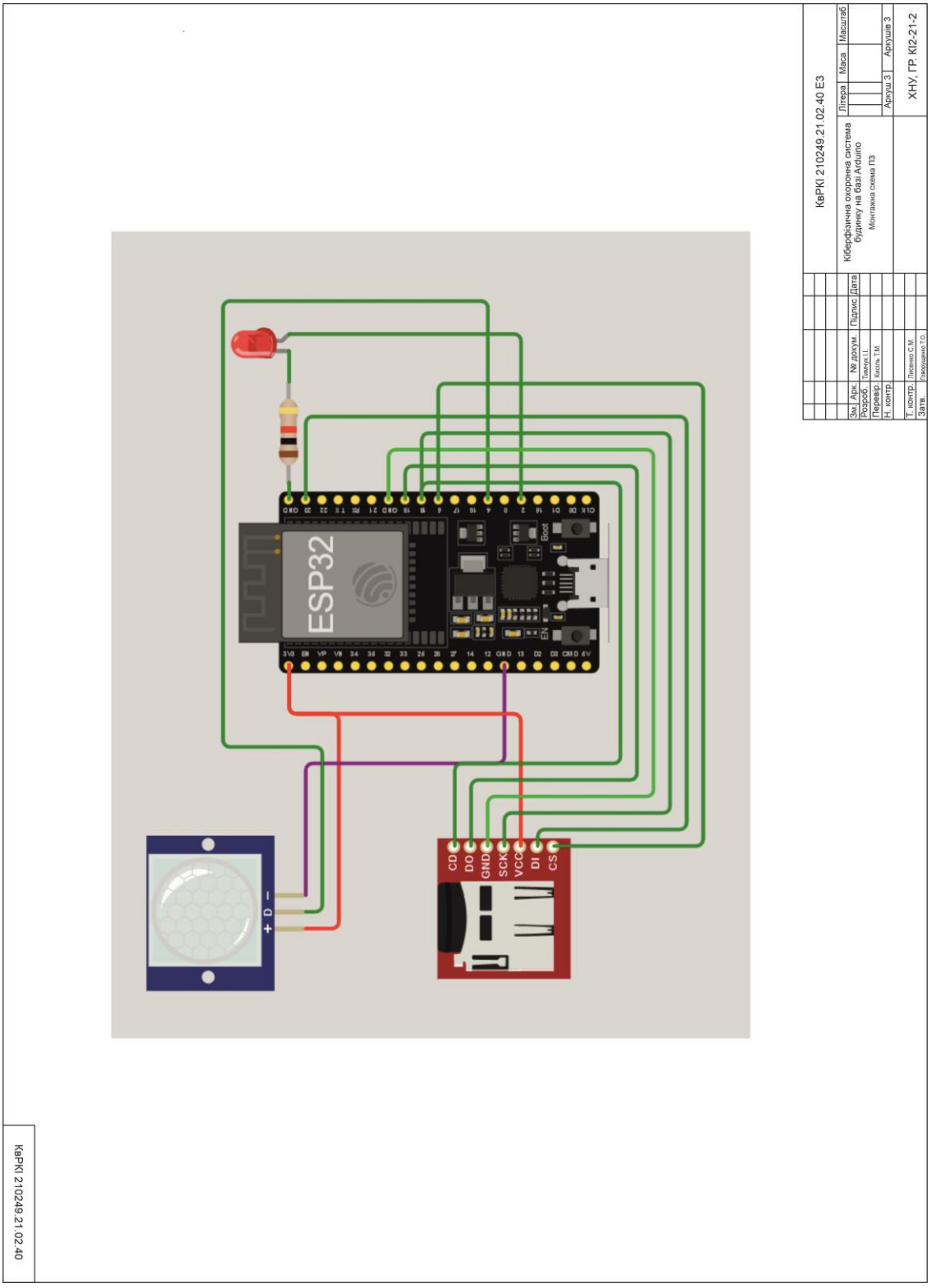
СХЕМА З’ЄДНАННЯ КОМПОНЕНТІВ ПЗ



Додаток В

(обов’язковий)

МОНТАЖНА СХЕМА



Wed Jun 11 09:58:08 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 10%**

	Document		Sum coincidence on the DB	
ID: 244908 Title: БКР Кіберфізична охоронна система будинку на базі Arduino Added in a DB: 2025-06-11 Authors: Іван ТИМЧУК Heads: Тетяна КИСІЛЬ Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	100353	626	1351 (1%)	20 (3%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Іван ТИМЧУК

Співавтор:

Назва: имчук_Кіберфізична охоронна система будинку на базі Arduino

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:2.2%

Коефіцієнт подібності 2:0%

Мікропробіли: 6

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-11 03:20:14.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-06-11 Доцент Андрій Нічепорук

Дата експерт

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Тимчук Іван Ігорович

Тема: Кіберфізична охоронна система будинку на базі Arduino

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 67

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є розробка програмно-апаратного засобу охорони приватного будинку на базі Arduino

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. У першому розділі кваліфікаційної роботи проведено ґрунтовний огляд предметної сфери: проаналізовано сучасні способи захисту об'єктів, основні принципи створення кіберфізичних систем та особливості використання платформ, таких як Arduino. Досліджено технічні можливості мікроконтролера ESP32, зокрема його здатність обробляти сигнали в реальному часі, передавати дані бездротово та інтегруватися з IoT-рішеннями. Висвітлено досвід передових компаній, як-от Ajax Systems, Paradox і Eldes, що відображає використання новітніх розробок у сфері безпеки.

У другому розділі обґрунтовано підбір ключових апаратних елементів системи. Беручи до уваги вимоги до компактності, економії енергії та гнучкості, обрано мікроконтролер ESP32 Dev Module, камеру OV2640, датчик руху PIR і модуль SD-карти. Вивчено актуальні технології IoT, зокрема інтеграцію з Telegram-ботом для сповіщень і симуляцію в Wokwi для тестування. На основі аналізу визначено технічні специфікації системи захисту та розроблено схему її функціонування, спираючись на передові методи моделювання.

У третьому розділі здійснено перевірку розробленої системи в симуляторі Wokwi. Створено структурну та електричну схему з'єднання компонентів,

включаючи датчик PIR, імітацію камери OV2640 за допомогою LED і модуль SD-карти. Розроблено програмне забезпечення для ESP32 із застосуванням сучасних бібліотек, яке забезпечує аналіз сигналів від датчика, фіксацію зображень, зберігання даних на SD-карту та відправку повідомлень через Telegram. Перевірялась точність роботи коду, обробки сигналів і стабільність передачі інформації в симульованому середовищі. Оцінено ефективність алгоритмів розпізнавання руху, надійність збереження даних і працездатність сповіщень. Відсутність фізичного зразка компенсовано детальним моделюванням поведінки системи в Wokwi, що відповідає інноваційним методам розробки кіберфізичних рішень.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: недостатньо глибокий аналіз фільтрації та обробки біосигналів.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: добре

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

доцент кафедри ЗІЗ Лишко О.М.

_____

"10" 06 2025 р. _____(підпис)

Завідувачу кафедри КІІС
д-р. філософії, доц. Ользі ПАВЛОВІЙ

Івана ТИМЧУКА
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-21-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Strike-Plagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

12.06 2025 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи кіберфізична охоронна система будинку на базі Arduino
Автор Іван ТИМЧУК
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський) рівень
Спеціальність 123– Комп'ютерна інженерія
Науковий керівник: к.ф-м.н.,доцент Тетяна Кисіль

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	Відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	Не виявлено

Підтвердження:
Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:
1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) запозичення, знайдені системою Anti-Plagiarism, складають звіт з передипломної практики Мазура Богдана.
Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості StrikePlagiarism, складає 2.2%, та системою Anti-Plagiarism складає 1%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи Тетяна КИСІЛЬ
Гарант ОП Андрій НІЧЕПОРУК
Завідувач кафедри КІІС Ольга ПАВЛОВА