Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

МІКРОПРОЦЕСОРНА МУЛЬТИСЕНСОРНА СИСТЕМА БЕЗПЕКИ

Виконав: студент 2 курсу, групи 2КІ-22м
спеціальності 123 — «Комп'ютерна інженерія»
_____ Ярошевський М. М.

Керівник: к.т.н., доц.каф. ОТ
_____ Тарновський М. Г.
«14» 12 2023 р.

Опонент: к.т.н., доц. каф. ПЗ
_____ Войтко В. В.
«15» 12 2023 р.

Допущено до захисту

Завідувач кафедри ОТ
_____ д.т.н., проф. Азаров О. Д.
«18» 12 2023 р

ВНТУ 2023

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Галузь знань — Інформаційні технології
Освітній рівень — магістр
Спеціальність — 123 Комп'ютерна інженерія
Освітня програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ, д.т.н., проф.
_____ Азаров О. Д.
"26" 09 2023року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Ярошевському М. М.

1 Тема роботи «Мікропроцесорна мультисенсорна система безпеки», керівник роботи Тарновський М. Г. к.т.н., доцент, затверджено наказом вищого навчального закладу від 18.09.23 року № 247.

2 Строк подання студентом роботи 18.12.2023.

3 Вихідні дані до роботи: призначення системи — виявлення ознак несанкціонованого проникнення; тип використовуваних датчиків — дротові та бездротові; організація — інтеграція з хмарними сервісами; архітектура — розподілена з можливістю легкого масштабування.

4 Зміст текстової частини (перелік питань, які потрібно розробити): вступ, аналіз сучасних технологій забезпечення безпеки, вибір архітектури системи безпеки, розробка апаратно-програмних засобів системи безпеки, розробка рекомендацій з введення в експлуатацію, економічна частина.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): архітектура системи безпеки, структурна схема приймально-контрольного пристрою, структурна схема контролера дротових датчиків,

функціональна схема приймально-контрольного пристрою, функціональна схема контролера дротових датчиків.

6 Консультанти розділів роботи наведені в таблиці 1.

Таблиця 1 — Консультанти роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-4	Тарновський М. Г. к.т.н., доцент	19.09.2023р	15.12.2023р
5	Небава М. І. проф., к.е.н	1.11.2023	15.12.2023

7 Дата видачі завдання «19» 09 2023 року.

8 Календарний план виконання приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів дипломного роботи	Термін виконання		Примітка
		початок	закінчення	
1	Постановка задачі роботи	19.09.2023		Виконано
2	Обгрунтування актуальності теми. Аналіз сучасних технологій забезпечення безпеки	19.09.2023	15.10.2023	Вик
3	Визначення архітектури системи безпеки	16.10.2023	29.10.2023	Вик
4	Розробка апаратно-програмних засобів системи.	30.10.2023	19.11.2023	Вик
5	Розробка рекомендацій з введення в експлуатацію.	20.11.2023	26.11.2023	Вик
6	Оцінка комерційного потенціалу розробки	27.11.2023	3.12.2023	Вик
7	Оформлення пояснювальної записки та ілюстративного матеріалу	4.12.2023	10.12.2023	Вик
8	Перевірка якості виконання магістерської кваліфікаційної роботи та усунення недоліків	11.02.2023	15.02.2023	Вик

Студент Ярошевський М.М.

Керівник роботи Тарновський М.Г.

АНОТАЦІЯ

УДК 004

Ярошевський М. М. Мікропроцесорна мультисенсорна система безпеки. Магістерська кваліфікаційна робота зі спеціальності 123 — Комп'ютерна Інженерія, Вінниця: ВНТУ, 2023, 102 с.

На укр. мові. Бібліогр.: 35 назв; рис.: 22; табл. 9.

У роботі розглянуто принципи побудови мікропроцесорної системи безпеки, що інтегрована в інтернет речей. В роботі проведений аналіз сучасних технологій забезпечення безпеки, розглянуті основні принципи побудови систем безпеки, вибрано та проаналізовано аналоги, визначено архітектуру системи безпеки, орієнтованої на використання дротових та бездротових датчиків. Розроблено структурні та функціональні схеми основних функціональних модулів системи, що надає можливість віддаленого контролю через хмарний сервер, надані рекомендації з введення її в експлуатацію.

Ключові слова: система безпеки, охоронна система, сповіщувач, датчик, хмарний сервер, інтернет речей, Z-Wave.

ABSTRACT

УДК 004

Yaroshevskyi M. M. Microprocessor multi-sensor security system. Master's thesis on specialty 123 — Computer Engineering, Vinnytsia: VNTU, 2023, 102 p.

In Ukrainian speech Bibliography: 35 titles; Fig.: 22; table 9.

The paper examines the principles of building a microprocessor security system integrated into the Internet of Things. The paper analyzes modern security technologies, considers the basic principles of building security systems, selects and analyzes analogues, defines the architecture of a security system focused on the use of wired and wireless sensors. The structural and functional diagrams of the main functional modules of the system, which provides the possibility of remote control via a cloud server, have been developed, and recommendations for its commissioning have been provided.

Keywords: security system, security system, detector, sensor, cloud server, Internet of Things, Z-Wave.

ЗМІСТ

					08-54.БДР.048.00.000 ПЗ		
Змн.	*Лист*	*№ докум.*	*Підпис*	*Дата*			
Розроб.		Ярошевський М.М			Мікропроцесорна мультисенсорна система безпеки Пояснювальна записка на тему	*Літ.*	*Арк.*	*Акрушів*
Перевір.		Тарновський М.Г..						
Реценз.		Войтко В.В..				*ВНТУ, гр. 2КІ–22м*		
Н. Контр.		Швець С.І.						
Затверд.		Азаров О.Д.						

ВСТУП

Безпека об’єктів нерухомого майна різних форм власності забезпечується комплексом різноманітних заходів, важливою ланкою серед яких є системи охоронної сигналізації. Залежно від рівня важливості об'єкта, що захищається, його категорії визначається структура і склад такої системи, головним завданням якої є інформування господарів або служб охорони про незаконне проникнення зловмисників для запобігання вчиненню противоправних дій. Це основне завдання вирішується шляхом своєчасного виявлення спроб несанкціонованого проникнення на об'єкт з визначенням місця та часу порушення охоронного рубежу.

Актуальність теми роботи обумовлена необхідністю постійного вдосконаленням методів і засобів забезпечення безпеки різних об'єктів, рівень якої визначається ймовірністю збереження захисту об’єкта при різному виді загроз. Провідна роль у цьому питанні належить сучасним технічним засобам безпеки, ринок яких у теперішній час є один з таких, що найбільш швидко та динамічно розвивається. Сучасним трендом у сфері безпеки є поступовий перехід до розширення спектру продуктів та послуг, які не лише захищають, а й дозволяють підвищувати ефективності бізнесу, створювати додаткові цінності як для окремих користувачів, так і для компаній та суспільства [1].

Сучасні охоронні системи є складним комплексом технічних засобів, ефективність функціонування яких залежить від безлічі взаємопов'язаних між собою факторів і, як правило, оцінюється сукупністю критеріїв, що перебувають у складних конфліктних взаєминах. Вони можуть містити різноманітні компоненти, такі як камери відеоспостереження, датчики, засоби контролю та управління доступом, пожежної сигналізації тощо.

Для конкретного об'єкта можливі загрози можуть відрізнятися. Поряд із цим, може існувати цілий комплекс різних загроз. У зв’язку з цим надійний захист можуть забезпечити тільки багатофункціональні засоби, що здатні

взаємодіяти з будь-якими датчиками, підтримують різні режими роботи, надають можливість легко змінювати алгоритм функціонування на об’єкті.

Об’єкт дослідження: процеси взаємодії між засобами виявлення загроз безпеки на об’єктах.

Предметом дослідження є методи та мікропроцесорні засоби контролю безпеки на об’єктах.

Метою роботи є вдосконалення системи безпеки за рахунок функціональної оптимізації основних її компонентів, що дозволяє скоротити їх кількість.

Для досягнення поставленої мети у роботі розв’язані такі **задачі**:

— проведено аналіз сучасних технологій забезпечення безпеки;

— вибрано архітектуру системи безпеки;

— розроблено апаратно-програмні засоби системи безпеки;

— запропоновані рекомендації з введення в експлуатацію.

Новизна роботи полягає в тому, що набув подальшого розвитку принцип використання хмарних технологій для отримання даних від засобів виявлення загроз безпеки, в якій за рахунок підтримки можливості використання бездротових та дротових датчиків, розширюються можливості контролю за станом об’єкту.

Практичне значення роботи полягає в тому, що запропоновані технічні рішення дозволяють зменшити номенклатуру основних компонентів системи безпеки, що полегшує її розгортання на об’єкті.

Апробація результатів роботи здійснена у доповіді на Міжнародній науково-практичній Інтернет-конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2024)».

1 АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

1.1 Основні принципи побудови сучасних систем безпеки

Система безпеки представляє комплекс різнорідних елементів, об'єднаних єдиним завданням із запобігання реалізації всіляких загроз нанесення шкоди об'єкту, що охороняється. Відповідно до цього завдання до складу системи входять засоби виявлення (датчики), засоби контролю (приймально-контрольні прилади, засоби централізованого спостереження, засоби передачі сповіщень), інше обладнання (звукові і світлові оповіщувачі, джерела живлення, засоби охоронного освітлення та т.і.).

Технічні засоби виявлення та лінії зв’язку, що прокладаються між ним і від них до засобів контролю, утворюють шлейф охоронної сигналізації. Частина об’єкта, що охороняється, яка контролюється одним або кількома шлейфами, називається зоною, що охороняється, а самий шлейф або їх сукупність утворює охоронний рубіж. У залежності від типу об’єкта, що охороняється, технічні засоби охоронної сигналізації поділяють на об’єктові, які розміщуються в середині приміщень, та периметральні, які розташовуються зовні вздовж зовнішнього огороджування [3].

Охоронні системи в залежності від принципу організації охорони поділяються на автономні та централізовані. Автономна система користується великою популярністю за рахунок своєї доступності та простого монтажу на об'єкті. Сьогодні широко пропонуються готові комплекти різноманітного обладнання. Такі системи комплектуються датчиками, що реагують на рух, відчинення дверей та замків, пошкодження вікон та скла.

При спрацьовуванні сигнал тривоги не передається ні на які пристрої, а працює навпаки локально, завдяки чому привертає увагу за рахунок звукових сирен і світлових оповіщувачів. Таким чином, основним завданням автономної системи є зупинка правопорушників шляхом привертання уваги. Такі системи підходять для об’єктів з цілодобовою роботою та штатом постійно присутнього чергового персоналу [4], [5].

Головними перевагами автономної системи є:

— порівняно низька вартість;

— можливість самостійного монтажу;

— відсутність абонентської плати за передачу сигналу охоронної компанії та екіпажу швидкого реагування.

Недоліками автономної системи є необхідність самостійного контролю за працездатністю обладнання, перш за все датчиків, з боку персоналу або власника та неможливість отримувати сигнал про несанкціоноване проникнення, не перебуваючи поряд з об’єктом.

Існують автономні системи, що обладнуються автономним міні пультом, що передбачають присутність чергового оператора. Такі системи як правило застосовуються на підприємствах, складах, базах та інших великих об’єктах з великою кількістю зон, що охороняються. Функцією чергового оператора є контроль за станом шлейфа сигналізації та сповіщення по телефону підрозділів поліції у разі спрацювання сигналізації.

Ще одним з видів автономних систем є системи з автоматичним додзвоном або GSM системи. Вони мають можливість передачі сигналу власнику на відстані за допомогою повідомлення або виклику на телефон. Дані охоронні системи часто використовуються невеликими компаніями, а також для забезпечення охорони приватного майна: квартири, дачі та гаража. Більшість таких систем обладнуються GSM-модулем та працюють з бездротовими пристроями. У разі спрацювання, пристрій з GSM-сигналізацією включає звукові та світлові індикатори та одночасно передає сповіщення на номер власника [5], [6].

Серед основних переваг GSM систем можна відзначити такі:

— можливість самостійної установки;

— можливість гнучкого налаштування системи;

— можливість віддалено отримувати сигнал оповіщення;

— персональний доступ до системи охорони.

Основними недоліками є:

— можливі збої та вихід з ладу сигналізації у приміщеннях з мінусовою температурою;

— порівняно велика імовірність хибних спрацювань;

— порівняно низька надійність захищеність, пов’язана з можливою нестабільністю мережі GSM зв’язку та можливістю блокування передачі сигналу оповіщення шляхом глушіння сигналу GSM.

В основі централізованої системи лежить підключення системи до пульта централізованого спостереження. Вони є більш ефективними ніж автономні. Сигнал тривоги в них передається на пульт централізованого спостереження, розташований у підрозділах спеціалізованої служби охорони. Тому такі системи зазвичай називають «пультова система охоронної сигналізації». У залежності від специфіки об’єкта, що охороняється, та типу використовуваних каналів зв’язку, існують два основних варіанти побудови централізованих систем: системи централізованого спостереження та системи передачі тривожних сповіщень.

Централізовані системи знаходять застосування при охороні об’єктів, які характеризуються значною кількістю цінного майна, а тому вимагають оперативного реагування у разі проникнення сторонніх осіб, наприклад банків, великих торгових об’єктів, бізнес-центрів, складів, приміщень організацій і підприємств, музеїв і т. і. Пульт централізованого спостереження надає можливість не лише приймати сигнал тривоги, а й контролювати працездатність системи [3], [6].

До головних переваг централізованих систем відносяться:

— висока надійність та ефективність;

— фаховий монтаж та обслуговування;

— оперативний виїзд служби охорони на об'єкт під час спрацьовування;

— можливість використання додаткових засобів контролю, таких як датчиків пожежної охорони, витоку газу, диму, протікання води.

Основними недоліками є висока вартість обладнання та наявність обов’язкової абонентської плати.

Останні тенденції у сфері технологій безпеки пов’язані з розвитком мережевих технологій та Інтернету речей (IoT). Відповідно сучасним трендом стає зростання кількості підключених до мережі засобів систем безпеки, які стають важливою частиною сегмента інтернету речей. Це виводить галузь безпеки на принципово новий рівень, що характеризується більш широким доступним функціоналом [1], [7].

За останні кілька років значно зросла кількість охоронних сигналізацій для дому, які використовують бездротові канали зв'язку, зокрема Wi-Fi. На сьогоднішній день Wi-Fi сигналізація є новим ступенем у розвитку охоронних технологій. Поєднання звичних технологій, таких як Ethernet та радіочастотних каналів передачі зв'язку, дозволяє значно покращити якість та безпеку при передачі конфіденційних даних на мобільні пристрої через Інтернет.

Бездротові системи охоронної сигналізації мають вбудовані радіочастотні передавачі, що дозволяє пристроям зв'язуватися з головною панеллю керування (хабом). Через канал Wi-Fi здійснюється контроль над усіма встановленими датчиками.

Зростання пропускної здатності мереж надає можливість збільшувати роздільну здатність та швидкість передачі зображень та відео, розширювати номенклатуру та кількість використовуваних датчиків. Стрімко зростає попит на засоби, здатні формувати повнокольорові високодеталізовані зображення. У результаті створюються умови для ефективної реалізації комплексного багатофункціонального контролю безпеки за значеннями величезної кількості показників.

На ринку безпеки спостерігається постійно зростаючий попит на системи відеоспостереження, хмарні сервіси та інтелектуальні рішення IoT. Підвищений попит на хмарні рішення обумовлюється надійністю та доступністю цих технологій. Поширення хмарних сервісів позбавляє необхідності використання

локальних сервісів та додаткового програмного забезпечення. Контроль за роботою системи, отримання тривожних сповіщень та реакція на події може бути реалізовано з будь-якої точки. Усе більше операцій, пов’язаних з вирішенням завдань із запобігання загрозам, переноситься в онлайн, керуються та контролюються дистанційно [7], [8].

З іншого боку, при зростанні кількості пристроїв, підключених до мережі, підвищує актуальність питання безпеки. Концепція «нульової довіри», в основі якої лежить постулат «ніколи не довіряй і завжди перевіряй» і яка спочатку була прийнята у сфері захисту даних, тепер знаходить застосування і в області систем безпеки відповідно до того, як охоронні засоби інтегруються в IoT.

1.2 Аналіз сучасних засобів виявлення загроз безпеки

Найважливішими компонентами охоронних систем є датчики або сповіщувачі, що дозволяють виявляти загрози, контролювати параметри, управляти пристроями та процесами. Для отримання інформації про тривожну ситуацію на об'єкті до виникає необхідність використання різних типів датчиків, що відрізняються типом контрольованого фізичного параметра, принципом дії, способом передачі інформації на центральний пульт управління.

У теперішній час на ринку представлена велика різноманітність різних типів датчиків, деякі з них є доволі вузькоспеціалізованими. За принципом формування інформаційного сигналу датчики поділяються на пасивні та активні. Пасивні датчики реагують на зміну певного фізичного параметру. Активні датчики охоронної системи генерують в зоні, що охороняється, сигнал та реагують на зміну його параметрів.

Магнітоконтактні датчики застосовуються для фіксації несанкціонованого відкриття дверей та вікон. Вони бувають двох видів: для зовнішнього і прихованого встановлення. Як правило, їх розміщують у верхній частині дверей або вікна. Магнітоконтактні датчики складаються з двох

елементів, один з яких встановлюється на рухому частину вікна чи дверей, другий — на нерухому дверну коробку чи раму [9].

Елементом, що встановлюється на рухому частину, є постійний магніт. Елементом, що розміщується на нерухомій частині, є геркон, який складається з двох контактів, розташованих в геометричному корпусі. Замикання/розмикання контактів відбувається при наближенні/віддалені постійного магніту.

Магнітоконтактні датчики відрізняються між собою матеріалом, з якого вони виготовлені, типом встановлення, а також значенням зазору між двома його елементами, при якому контакти геркона залишаються у замкненому стані, тобто датчик перебуває у режимі очікування. Контрольованим параметром є провідність електричного кола шлейфа, в який увімкнені контакти геркона [9], [10].

Основним перевагами магнітоконтактних датчиків є низька вартість, простота використання та мала імовірність помилкового спрацювання. Основний недолік — захист лише від несанкціонованого відкриття дверей або вікна, і не можливість контролю пролом двері або розбиття скла.

У чомусь подібними до магнітоконтактних датчиків є електроконтактні, які використовуються для виявлення пошкоджень або руйнування елементів, на яких вони закріплені, на сам перед скління вікон та дверей. Вони являють собою смугу тонкої алюмінієвої фольги малої ширини. Іноді замість фольги може використовуватися тонкий дріт. При руйнуванні конструкції, на яку наклеєна фольга або дріт, відбувається їх розривання, внаслідок чого розмикається електричне коло і, як наслідок, припиняється протікання електричного струму [11].

Основними перевагами електроконтактних датчиків є низька вартість та простота використання. Як основний недолік можна відзначити малу надійність, яка пов’язана з можливістю збереження цілісності електричного кола при певних умовах, наприклад при вирізанні частини скління та низькою стійкістю до випадкового руйнування.

Подібними датчиками є детектори розбиття скла. Основним елементом датчика є конденсаторний мікрофон, за допомогою якого фіксується звук розбиття скла. Мікрофон перетворює звукові шуми у приміщенні в електричний сигнал, який через смугові підсилювачі подається в електронний блок опрацювання сигналу, який аналізує його спектр. Якщо у спектрі шуму є складова, аналогічна до спектру звуку при пошкоджені або розбитті скла, відбувається спрацювання датчика [10], [11].

Принцип роботи сучасних датчиків розбиття скла базується на схемі фазочастотного поділу, яка на порядок знижує кількість помилкових тривог. Така технологія ґрунтується на прослуховуванні двох певних діапазонів частот. Сповіщувач піднімає тривогу тільки в тому випадку, якщо спочатку фіксується інфранізкий звук від удару, а потім уже дзвін розбитого скла.

Чутливість обох частотних каналів регулюється окремо, що дозволяє дуже тонко налаштувати пристрій під параметри навколишнього середовища. Нові моделі датчиків розбиття скла забезпечують контроль по всьому об'єму в радіусі від 10 м до 15 м. Це дозволяє не встановлювати його безпосередньо на скло. Датчик можу бути встановлений на стелі або стіні, що дозволяє стежити за цілісністю відразу кількох скляних поверхонь або скління великої площі [11].

Основною перевагою датчиків розбиття скла є можливість одночасного контролю одним датчиком усього скління приміщення, основний недолік — висока вартість, обумовлений складністю конструкції.

Сейсмічні датчики або геофони дозволяють зареєструвати коливання звукового діапазону, що збуджуються на поверхні землі під час руху зловмисника, або коливання в елементах конструкцій при спробі їх руйнування. Датчики цього типу приховано встановлюються у ґрунт або під будівельні конструкцій, характеризуються надзвичайно високою чутливістю і широко використовуються для охорони будівель та периметрів територій [13], [14].

Нині існує кілька типів таких датчиків. Перший, рідинний, принцип дії якого заснований на виявленні різниці у тисках. Чутливим елементом є дві або

кілька паралельних еластичних труб, встановлених під землею. Труби заповнені рідиною, що не замерзає, і підключені до сенсора, який реєструє різницю тисків рідини в сусідніх трубах. Коли порушник перетинає периметр, ґрунт злегка стискається під його вагою. Це створює невелику різницю у тисках між двома паралельними підземними шлангами, заповненими рідиною. Різниця тисків вимірюється спеціальним гідростатичним сенсором, вмикання якого в електричне коло здійснюється за диференціальною схемою для зменшення імовірності хибних тривог, причиною яких є фонові сейсмічні шуми [14].

Інший тип сейсмічного датчика використовує п'єзоелектричний ефект, що виникає у п'єзоелектричному кристалі при його деформації. У відповідь на механічну дію на поверхні п'єзоелектричного кристала генерується електричний заряд через деформації його внутрішньої структури решітки. Цей заряд може бути виміряний як вихідна напруга або струм, який пропорційний прикладеному механічному тиску. Датчик складається з п'єзоелектричного кристалу, затиснутого між двома металевими пластинами. Чутливість датчика та час відгуку залежать від властивостей п'єзоелектричного кристала, таких як його товщина та склад матеріалу.

Ще один тип геофону є дискретним датчиком, що складається з магнітного осердя, яке може вільно коливатися всередині обмотки, що проводить. Будь-які вібрації геофонного датчика викликають рух магніту відносно котушки, в результаті чого у котушці генерується електрична напруга, пропорційна швидкості руху магніту. Висока чутливість геофону забезпечує реєстрацію надзвичайно малих коливань ґрунту, викликаних, наприклад, обережно повзучим порушником. Дискретні геофонні датчики порівняно рідко використовуються як автономні сенсори. Зазвичай геофони встановлюють на периметрі у вигляді ліній, що включають до 20-50 дискретних сенсорів [14].

Перевагою геофонних датчиків є висока чутливість та скритність установки. Основний недолік пов’язаний з тим, що вихідний сигнал є аналоговим. Це вимагає застосування додаткових засобів для його підсилення,

фільтрації завад, що створюються навколишнім середовищем, та аналого-цифрового перетворення.

Останнім типом широко використовуваних пасивних датчиків є пасивні інфрачервоні датчики. Це найбільш використовувані в охоронних системах датчики. Принцип дії таких датчиків заснований на контролі за інфрачервоним (тепловим) випромінюванням в приміщенні, що захищається. При зміні інфрачервоного фону у приміщенні, що відбувається у момент переміщення людини, датчик формує сигнал тривоги. Ще такі датчики називають датчиками руху. Існують інфрачервоні пасивні датчики з різними діаграмами виявлення: об'ємної, кругової типу «штора» або «коридор». Найбільшого поширення набули об'ємні датчики, які, як правило, встановлюються в кутку приміщення під стелею [15].

Основні переваги пасивних інфрачервоних датчиків руху є висока надійність, низька вартість та простота монтажу. Головним недоліком є можливість помилкових спрацювань при появі у контрольованій зоні великих тварин, при циркуляції теплих повітряних мас в приміщенні, що охороняється.

Серед активних датчиків охоронних систем перш за все треба відзначити ємнісні сенсори, інфрачервоні активні та ультразвукові датчики.

Принцип дії ємнісних датчиків заснований на зміні ємності електроду або антени щодо землі, викликаної наближенням до неї людини. Антеною може бути звичайний дріт, що може бути прокладений по верхній частині паркану, вздовж вікон, дверних отворів тощо, або металевий корпус предмета, що охороняється, наприклад, сейфа, шафи, і т.і. Такі датчики застосовують для охорони об'єктів по периметру, контролю безпеки певної зони, через яку можливе проникнення на об’єкт (дверні чи віконні отвори) або окремих предметів (сейфи, металеві шафи) [16], [17].

Перевагою ємнісних датчиків є можливість контролю безпеки великих зон, а також здатність виявляти зловмисника на відстані. Основний недолік — висока імовірність хибних спрацювань.

Активні інфрачервоні датчики складаються з інфрачервоного випромінювача та приймача. Їх принцип заснований на формуванні випромінювачем імпульсного інфрачервоного випромінювання, яке сприймається приймачем. При перериванні світлового променю випромінювання не потрапляє на фотоприймач, що викликає спрацювання датчика. Можуть передбачати використання кількох світлових пучків.

Активні інфрачервоні датчики можуть встановлюватися як зовні, так і всередині, але при використанні в приміщеннях штучне освітлення створює їм перешкоди, особливо світло люмінесцентних ламп. Виходячи з цього, необхідно застосовувати пасивні та активні фільтри. При використанні зовні слід виключити можливість появи роси та інею на оптиці датчиків [18].

Перевагами активних інфрачервоних датчиків є високий ступінь захисту від несанкціонованого проникнення та простоту використання, основний недолік — чутливість до зовнішнього освітлення, пилу та випаданню роси.

Ультразвукові датчики забезпечують виявлення проникнення та пересування всередині охоронюваного периметру. Датчик складається з передавача та приймача акустичного випромінювання, блоку обробки сигналів тощо. Їх принцип дії заснований на реєстрації змін ультразвукового поля, що має місце при появі у приміщенні людини. Передавач будується на п’єзоелектричному ультразвуковому перетворювачі, що надсилає імпульси ультразвукових коливань в охоронюваний периметр. Приймач забезпечує зворотне перетворення ультразвукових коливань в електричний сигнал, і містить п'єзоелектричний ультразвуковий перетворювач. Блок обробки сигналів, у залежності від алгоритмів, що покладений у нього, формує сигнал тривоги [19].

Ультразвукові датчики можуть бути засновані на двох принципах дії: з використанням інтерференції ультразвукових коливань та ефекту Доплера. Принцип дії датчика з використанням інтерференції звукових хвиль заснований на тому що закритому приміщенні простір є обмеженим, а тому у будь-якій його

точці формується стійка інтерференційна картина. Приймач, що розташований у цій точці, реєструє амплітуду результату інтерференції у ній. При будь-яких змінах у приміщенні інтерференційна картина порушується, що відбивається на вихідному сигналі приймача.

На роботу датчиків такого типу впливають нерівномірність потоків повітря. Крім того, стабільність інтерференційної картини в реальному приміщенні залежить від різного роду вібрації, теплових деформацій елементів інтер'єру.

Усунити ці недоліки дозволяє інший метод, що полягає у реєстрації частоти сигналу, а не його амплітуди. При переміщенні об'єкта уздовж напряму розповсюдження хвилі відповідно ефекту Доплера спостерігається деякий зсув за частотою відбитої від нього хвилі відносно тієї, що формується передавачем. У замкненому приміщенні відбивання хвиль є рівнозначним за усіма напрямами, а тому ефект Доплера має місце і при перпендикулярному переміщенні об'єкту відносно напряму розповсюдження хвилі, але дещо слабкіше. Це надає можливість виявляти об'єкт, що рухається у будь-якому напрямі [19].

Ультразвукові датчики характеризуються високою чутливістю. Поряд із цим, вони не дозволяють зафіксувати повільні переміщення. Їх застосування ускладнено на об'єктах з широким використанням матеріалів, що поглинають звук. Крім того, на роботу ультразвукових датчиків впливають повітряні потоки, створювані кондиціонерами і опалювальними приладами.

За подібним принципом працюють мікрохвильові датчики, які замість ультразвукового випромінювання використовують електромагнітне випромінювання надвисокочастотного діапазону. Такі датчики складаються з: НВЧ генератора, антенної системи, що створює електромагнітне поле в навколишньому просторі та приймає сигнали, що відбиваються, формує діаграму спрямованості датчика та визначає форму просторової зони

чутливості, НВЧ приймача, що реєструє зміну характеристик прийнятого сигналу, та блоку обробки, що аналізує сигнали [20].

Поряд з розглянутими типами датчиками, які забезпечують контроль безпеки за одним з фізичних показників, знаходять застосування комбіновані, які дозволяють контролювати зону, що охороняється, одночасно за двома параметрами, що взаємно доповнюють один одного. Комбіновані датчики контролюють один і той самий параметр, використовуючи різні фізичні принципи. Сигнал тривоги в них при формується при одночасному спрацюванні обох каналів. Перевагою комбінованих датчиків, є підвищена надійність виявлення ознак порушення безпеки, основний недолік — підвищена вартість.

Ще одним видом датчиків є суміщені сповіщувачі, що є пристроями, що в одному корпусі об’єднують два датчики з різними фізичними принципами дії, кожний з яких є автономним приладом та у своєму функціонуванні не перетинаються. Кожен має свої окремі виходи на шлейф для подачі сигналів тривоги і сканує свою зону відповідальності. Зараз у системах охорони найбільш поширені суміщені датчики на основі інфрачервоного пасивного датчика та датчика розбиття скла, які розташовані в єдиному корпусі.

Оскільки два канали детекції в суміщених сповіщувачах не дублюють один одного, а працюють незалежно, то і перешкоди, і фактори, що впливають на помилкові тривоги, відповідно залишаються для кожного каналу. Головною перевагою суміщених датчиків є те, що при їх використанні зменшується загальна кількість елементів охоронної системи.

1.3 Вибір та аналіз аналогів

Одним з аналогів розглядуваної системи є система сигналізації для корпоративного сектору від компанії Tipac [21]. Дана система з центральним пультом охорони використовує сертифіковані протоколи передачі повідомлень і є повноцінних варіантом для охорони підприємств. Керування та програмування системи здійснюється за допомогою чотирьох кнопок

управління та вбудованої клавіатури (рис. 1.1). Центральний пульт допускає живлення від батареї та підтримує підключення керованого модуля релейних виходів та модуля цифрового автодозвону по аналоговій телефонній лінії. Крім того, допускається підключення на один шлейф кількох пожежних сповіщувачів з релейними виходами, що працюють у режимі замикання/розмикання, а також двожильних сповіщувачів з суміщеними сигнальними лініями та лініями живлення.

Рисунок 1.1 — Центральний пульт керування ADT Orion 8K

Головними недоліками охоронних систем Tipac є висока вартість обладнання та його несумісність з пристроями інших виробників.

Рисунок 1.2 — Бездротова сигналізація GSM Kerui G18

Ще одним з аналогів є бездротова сигналізація GSM Kerui G18 (рис 1.2) з оповіщенням через засоби мобільного зв’язку [22]. Система може працювати в

чотирьох режимах: Away Arm, Home Arm, Delay Arm, Emergency Arm. Кожен з цих режимів використовує унікальний алгоритм увімкнення/вимкнення охорони та формування реакції на спрацювання датчиків. Система підтримує можливість віддаленого керування через Android застосування, ведення журналу подій, вмикання та вимикання за розкладом.

Система передбачає можливість підключення до 100 бездротових датчиків. При виявленні спроби вторгнення система G18 формує звуковий сигнал потужністю 110 дБ та дозволяє здійснити голосовий дзвінок або відправити СМС повідомлення на 6 телефонних номерів.

Основні характеристики охоронної системи G18 [22]:

— 100 охоронних зон;

— 8 типів зон (повна варта, часткова варта, 24-годинні зони, тривожна кнопка, охороною периметром, інтелектуальний режим на подвійне спрацьовування);

— 6 номерів для дзвінків про тривогу;

— 3 номери для сповіщення за СМС про стан сигналізації;

— автоматичне зняття з охорони за розкладом;

— можливість віддаленого керування через застосунки Android;

— вбудована та зовнішня сирена для формування звукового сигналу «Тривога»;

— споживаний струм у режимі охорони — 30 мА;

— споживаний струм у режимі тривога — 300 мА;

— резервне живлення: Li-ion Акумулятор 7.2 В, до 10 год автономної роботи.

Комплект поставки:

— центральний модуль — 1 шт.;

— бездротовий датчик руху — 1шт;

— бездротовий датчик відчинення — 1 шт.;

— брелок дистанційного керування — 2 шт.;

— блок живлення — 1 шт.;

— п'єзоелектрична дротова сирена — 1 шт.

Основним недоліком системи GSM Kerui G18 є залежність від мережі мобільного зв’язку.

Найбільш близькою до розглядуваної системи є система бездротової автономної Wi-Fi сигналізації ATIS Kit 200T для офісу, будинку, квартири призначений для передачі сигналів тривоги та повідомлень на мобільні пристрої за допомогою WiFi (рис 1.3) [23].

Рисунок 1.3 — Комплект сигналізації ATIS Kit 200T

Комплект сигналізації ATIS Kit 200T сумісний із елементами розумного будинку на базі системи Tuya Smart. Система дозволяє додати до 24 охоронних або пожежних датчиків та 8 брелків дистанційного керування. Управління сигналізацією з мобільного телефону здійснюється за допомогою програми Tuya Smart. Яку можна завантажити її з Apple Store чи Play Market.

Система підтримує кілька режимів реагування сирени-сигналізації на вторгнення в зону, що охороняється:

— режим "Господар будинку" — включається тільки світлова індикація;

— режим "Охорона" — сирена включає звуковий та світловий сигнал;

— режим "Знято з охорони" — режим тривоги увімкнеться лише при натисканні на тривожну кнопку SOS на брелку.

При виявленні тривожної ситуації система подає сигнал сирени та здійснює відправлення через WI-FI push-up повідомлень абонентам, підключеним до неї. Наявність резервного живлення та підтримка стандарту WiFi забезпечує гарантовану стабільність та швидкість роботи охоронної системи безпеки. Спрацювання сигналізації, що знаходиться в режимі охорони, відбувається в таких ситуаціях: відчинення дверей та/або вікна всього на 1 см; фіксування руху людини у приміщенні на відстані до 12 м від датчика руху; при натисканні кнопки тривоги; при підключенні відповідних датчиків у систему у разі виникнення позаштатної ситуації — задимлення чи затоплення приміщення.

У базовий комплект охоронної сигналізації ATIS Kit 200T входять:

— системний блок сигналізації з вбудованою сиреною — 1 шт;

— бездротовий датчик руху — 1 шт;

— бездротовий датчик відкриття дверей/вікна — 1 шт;

— брелок дистанційного керування —1 шт.

Основні характеристики системи ATIS Kit 200T:

— потужна звукова сирена, світлове сповіщення;

— оповіщення про спрацювання у додаток на телефон у реальному часі;

— дистанційна постановка на охорону та зняття з охорони;

— легке керування з мобільного телефону підключеними пристроями;

— сумісність з усім обладнанням, що працює на платформі розумного будинку TUYA;

— розширення системи до 24 датчиків та 8 пультів дистанційного управління;

— відстань передачі сигналу від датчиків — до 100 метрів;

— підтримка роботи при зникненні живлення 220 В;

— оповіщення у додаток про зникнення живлення 220 В;

— оповіщення про розряд акумуляторної батареї;

— оповіщення у додаток про пошкодження корпусу центрального пульта контролю/управління;

— підтримка роботи WIFI у діапазоні 2,4 ГГц;

— підтримка Amazon Alexa та Google Assistant.

Основними недоліками системи ATIS Kit 200T є неможливість налаштування без мобільного застосування або пульта дистанційного управління, несумісність з обладнанням інших виробників, підтримка лише бездротових датчиків.

Підводячи підсумки можна зазначити таке:

— високий ступінь забезпечення безпеки може бути досягнутий лише за умови контролю усіх можливих видів загроз, що вимагає застосування в одній системі різних типів датчиків;

— для отримання конкурентоспроможної системи, яка відповідала би сучасним тенденціям у сфері безпеки, необхідно передбачити в ній можливість інтеграції з хмарними рішеннями.

2 ВИБІР АРХІТЕКТУРИ СИСТЕМИ БЕЗПЕКИ

2.1 Аналіз можливих архітектурних рішень у побудові системи безпеки

Як було зазначено за результатами аналізу, проведеному у першому розділі, сучасним трендом побудови охоронних систем безпеки є інтеграція технічних засобів охорони з Інтернетом речей. Це дозволяє створювати розумні системи безпеки, які можуть взаємодіяти з усіма пристроями на об'єкті, від дверних замків до систем опалення. Наприклад, система охоронної сигналізації може автоматично вимкнути всі електричні прилади при виникненні небезпеки або надіслати повідомлення на мобільний телефон у разі несанкціонованого доступу.

Спочатку бездротові системи охоронної сигналізації розроблялися виключно для житлових приміщень. За останні три роки бездротові рішення в галузі систем безпеки міцно закріпили свої позиції поряд з класичними рішеннями. При цьому сфера застосування таких систем вийшла за межі невеликих офісів.

Найпростіший варіант системи безпеки з підтримкою IoT може бути реалізований з використанням бездротових WiFi датчиків та пристроїв звукового й світлового оповіщення (рис. 2.1).

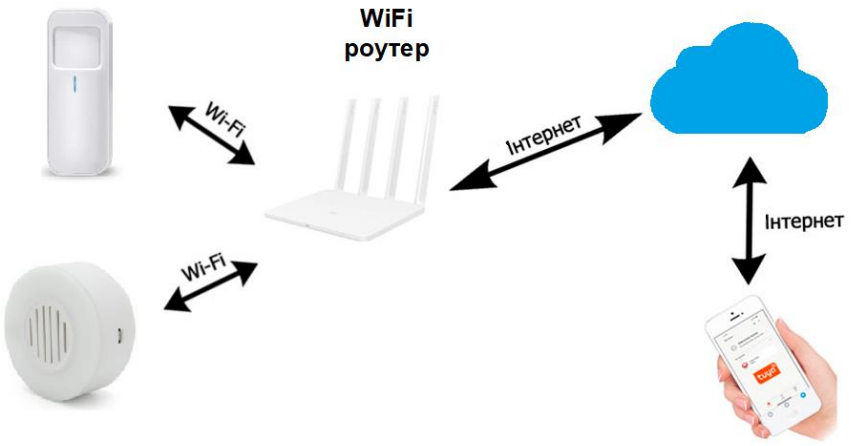

Рисунок 2.1 — Система безпеки з підтримкою IoT на основі WiFi пристроїв

Така система може бути реалізована на основі готових рішень, наприклад, платформи Tuya Smart [24]. Tuya Smart — це глобальна платформа Інтернету речей, яка об'єднує десятки виробників та тисячи різних пристроїв. Технологічно платформа охоплює біля 500 видів різноманітної продукції, включає хмару та мобільний додаток, і надає можливість партнерам використовувати програмні модулі API та мобільний додаток при розробці власного обладнання Така концепція дозволяє використовувати IoT пристрої незалежно від продукту, протоколу, регіону або постачальника.

Головна перевага рішення, що ілюструє рис. 2.1, полягає у простоті інсталяції, гарній масштабованості, можна використовувати пристрої різних виробників, користувач самостійно визначає склад системи. Проте така архітектура має зіркоподібну толпологію. Її головним елементом, що забезпечує зв’язок зі всіма пристроями, є WiFi роутер. Це накладає обмеження на радіус покриття та не забезпечує високої надійності функціонування.

Інший недолік полягає у тому, що така архітектура системи заснована на використанні WiFi пристроїв. Хоча WiFi є найпоширенішою бездротовою мережною технологією, яка є найбільш популярною для підключення комп'ютерів, смартфонів та планшетів до Інтернет, вона не є «ідеальною» для застосування в системах IoT.

Технологія Wi-Fi заснована на сімействі стандартів бездротової мережі IEEE 802.11x. Вони визначають лише перші два рівні моделі OSI: фізичний та канальний. На фізичному рівні використовується радіоканал. Основними частотними діапазонами Wi-Fi вважаються 2,4 ГГц (від 2412 до 2472 МГц), 5 ГГц (від 5160 до 5825 МГц) та 6 ГГц (від 5955 до 7115 МГц). На мережному та транспортному рівнях Wi-Fi зазвичай використовує інші стандартні протоколи: IPv4 чи IPv6 для мережного рівня та UDP або TCP для транспортного. Прикладний рівень, який відповідає за сумісність пристроїв, не визначений зовсім і повинен підтримуватися самими виробниками програмних та апаратних рішень [25].

Не зважаючи на те, що через Wi-Fi можна передавати дані на швидкостях у кілька десятків Мбіт/с, для домашньої автоматизації висока швидкість доступу до Інтернет та можливість швидко передавати величезні обсяги інформації не є основними перевагами. Типові пристрої IoT при обміні використовують мінімальні об’єми даних.

Сама собою надмірна пропускна спроможність не є проблемою, але її підтримка пов'язана зі значним енергоспоживанням. Як високошвидкісний стандарт бездротового зв'язку, Wi-Fi надмірно енерговитратний для «Інтернету речей». Це стає проблемою для тих рішень, які працюють від автономних джерел живлення, а саме такими і є більшість серед бездротових датчиків для систем безпеки.

Ще одне серйозне обмеження, яке було зазначено вище, виникає через топологію Wi-Fi-мережі. Усі пристроїв такої мережі взаємодіють центральний маршрутизатор. При виході його ладу, відбувається збій усієї мережі.

Альтернативним варіантом Wi-Fi є технології Zigbee и Z-Wave. Технологія Zigbee заснована на стандарті IEEE 802.15.4 і є економічно ефективним варіантом бездротового зв'язку для невеликих локальних мереж. Набір протоколів ZigBee визначає лише верхні рівні моделі OSI: мережевий, транспортний та прикладний. Він побудований поверх стандарту IEEE 802.15.4, який визначає нижні рівні бездротової мережі, а тому ZigBee може використовувати Wi-Fi або Bluetooth канали. Як робочий діапазон стандарт визначає частоти, що не ліцензуються: 2,4 ГГц (по всьому світу), 915 МГц (для Америки та Австралії) і 868 МГц (для Європи). Максимальна швидкість передачі даних становить 250 Кбіт/с у діапазоні 2,4 ГГц, 40 Кбіт/с у діапазоні 915 МГц та всього 20 Кбіт/с у діапазоні 868 МГц. Тому практично всі пристрої ZigBee працюють лише на частоті 2,4 ГГц.

На відміну від Wi-Fi Zigbee дозволяє використовувати розподілену (комірчасту) топологію мережі, що дозволяє пристроям з'єднуватися один з одним на великих відстанях. У реалізації комірчастої мережі ZigBee беруть

участь три класи пристроїв: координатор, який формує мережу та координує її роботу, маршрутизатор, що забезпечує підключення та обслуговування до 32 кінцевих пристроїв, та кінцеві пристрої, які задля економії заряду батареї велику частину часу знаходяться в режимі сну, можуть приймати та відправляти пакети, але не беруть участь у їх ретрансляції. Таким чином, при відсутності прямого зв′язку з роутером кінцевий пристрій зберігає зв′язок з іншими пристроями мережі.

Отже, головними перевагами технології Zigbee є мале енергоспоживання кінцевих пристроїв, гарна масштабованість та висока надійність мережі. Основний недолік ZigBee пов’язаний з використанням надзавантаженого діапазону 2,4 ГГц та тим, що він є одноканальним рішенням, а тому на роботу мережі сильно впливають перешкоди, що створюються іншими Wi-Fi або Bluetooth пристроями.

Менш чутливим до перешкод, викликаних побутовими приладами та мережами Wi-Fi, є протокол Z-Wave, що працює на частоті 869 МГц. Пристрої мережі Z-Wave є як передавачами або приймачами, так і ретрансляторами, тобто здатні брати участь у пересиланні сигналу від одного пристрою до іншого, що дозволяє обходити перешкоди на прямому шляху між пристроями. Такий підхід дозволяє значно розширити радіус дії бездротової мережі та підвищує її надійність. Радіус дії пристроїв досягає 30 метрів, а мережа загалом може мати розміри від120 до 150 метрів.

Стандарт Z-Wave охоплює всі рівні моделі OSI, від фізичного до прикладного. Це гарантує високий рівень сумісності обладнання від різних постачальників. Z-Wave є добре налагодженим протоколом, орієнтованим на обмін короткими командами та повідомленнями між пристроями, що зводить до мінімуму завантаженість радіоканалу і знижує ймовірність втрати даних.

Кожна логічна мережа Z-Wave може підтримувати до 232 пристроїв. За необхідності підключення більшої кількості пристроїв є можливість об'єднання мереж. Декілька мереж Z-Wave можуть спокійно співіснувати на одній і тій

самій території, не впливаючи одна на одну. Це досягається мінімізацією розміру пакета, що передається, і обов'язковою вимогою до мінімального навантаження на радіоканал, яке зобов'язує пристрій перебувати в стані передачі не більше 1 % часу. Проте вузли різних мереж неспроможні “бачити” однин одного і, відповідно, якось зв’язуватися між собою. Зв'язок між мережами здійснюється через пристрої, що виконують роль мережевих мостів [25].

Як і мережа Zigbee , кожна мережа Z-Wave має основний контролер, який забезпечує додавання нових пристроїв до мережі та видалення старих, складання карт маршрутизації, забезпечення безпечного підключення, забезпечення можливості створювати сценарії автоматизації та інших функцій з організації та контролю роботи мережі. У мережі також може бути один або кілька вторинних контролерів, які для нормальної роботи запитують інформацію про топологію мережі у основного контролера. Зазвичай основним контролером є той, з якого почалося побудова мережі. Але згодом цю функцію можна передати одному з вторинних контролерів.

Особливістю мережі Z-Wave є асоціації між пристроями. Завдяки цій функції один пристрій може відправляти команду, що знаходиться поблизу іншого пристрою, минаючи центральний контролер. Це не тільки прискорює спрацювання виконавчих пристроїв, а й підвищує надійність відповідальних вузлів мережі. Наприклад, зв'язка «датчик-виконавчий пристрій» буде працювати, навіть якщо контролер вийшов з ладу.

Крім високої надійності та можливості самовідновлення мережа Z-Wave характеризується високим рівнем захисту. Для шифрування даних, що передаються, використовуються ті самі технології шифрування, як і в системі онлайн-банкінгу.

Z-Wave працює в частотному діапазоні від 800 МГц до 900 МГц, що виділена для пристроїв малого радіусу дії. Особливістю цих частот є здатність впевнено долати різні перепони, у тому числі перекриттів та стін. Для цього частотного діапазону також характерна мала кількість перешкод, створюваних

іншими пристроями, що працюють на цих частотах, оскільки конкуруючі технології використовують діапазон 2,4 ГГц [26].

Для отримання можливості використовувати Z-Wave пристрої до системи безпеки, що наведена рис. 2.1, треба додати Z-Wave шлюз, який забезпечить пересилку даних між мережами Z-Wave та WiFi (рис. 2.2).

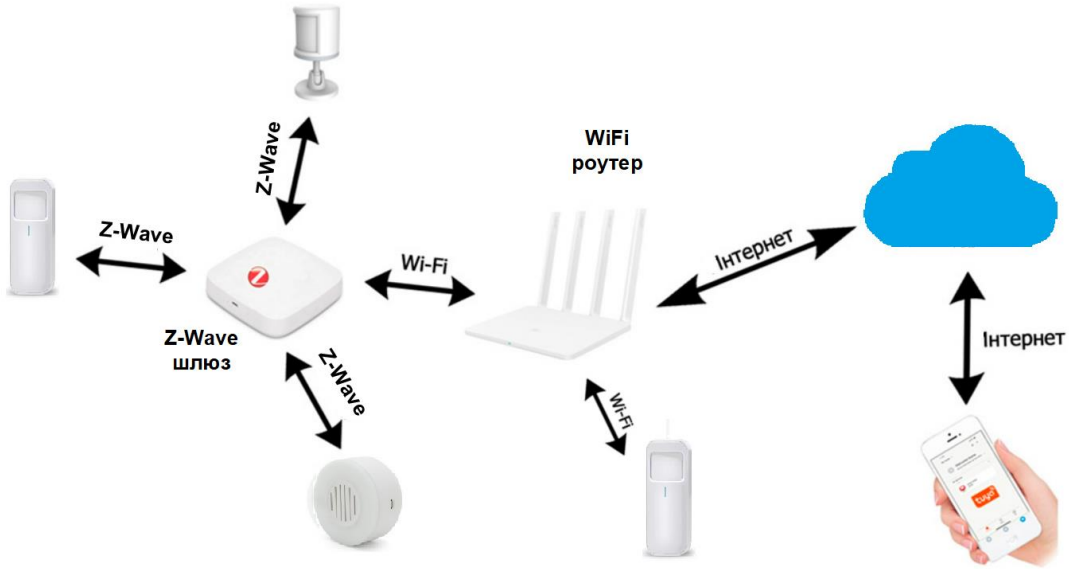

Рисунок 2.2 — Система безпеки з підтримкою IoT на основі мережі Z-Wave

У мережі WiFi шлюз Z-Wave є одним з кінцевих пристроїв, що підключений до WiFi роутера. В мережі Z-Wave він є центральним контролером (координатором), який організовує роботу мережі і підключення до неї Z-Wave датчиків та виконавчих елементів.

Однією з переваг архітектур системи безпеки, що зображені на рис. 2.1 та рис. 2.2, є те що вони можуть бути реалізовані з використанням готових рішень та характеризуються легкістю масштабування. При цьому варіант архітектури, що наведений на рис. 2.2, має такі переваги як знижене енергоспоживання використовуваних датчиків, а значить більш тривалий час їх автономної роботи, та високу надійність. Вихід з ладу Z-Wave шлюза або WiFi роутера призведе лише до втрати зв’язку з хмарним сервером та мобільним додатком. При цьому

працездатність тієї частини системи, що охоплена мережею Z-Wave, не порушиться.

З іншого боку обидві архітектури орієнтовані на використання бездротових датчиків. Не зважаючи на те, що бездротові датчики можуть бути встановленні у важкодоступних місцях та не вимагають прокладання додаткових проводів, що дозволяє проводити монтаж без необхідності проведення подальшого ремонту, таке рішення має ряд недоліків. По-перше, вартість бездротового датчика набагато перевищує вартість його дротового аналога. По-друге, бездротові датчики поступають дротовим за різноманіттям типів, що звужує можливості виявлення усіх загроз, що можуть мати місце на об’єкті.

Отримати можливість використання в одній системі як бездротових, так і дротових датчиків можна за рахунок введення до її складу додаткового модуля, що забезпечить підключення шлейфів сигналізації з дротовими датчиками. Оскільки дротові датчики використовують живлення від шлейфу, даний модуль повинен живитися від мережі, а тому його підключення до системи можна здійснити через WiFi. Таким чином приходимо до варіанту системи безпеки, що зображений на рис. 2.3.

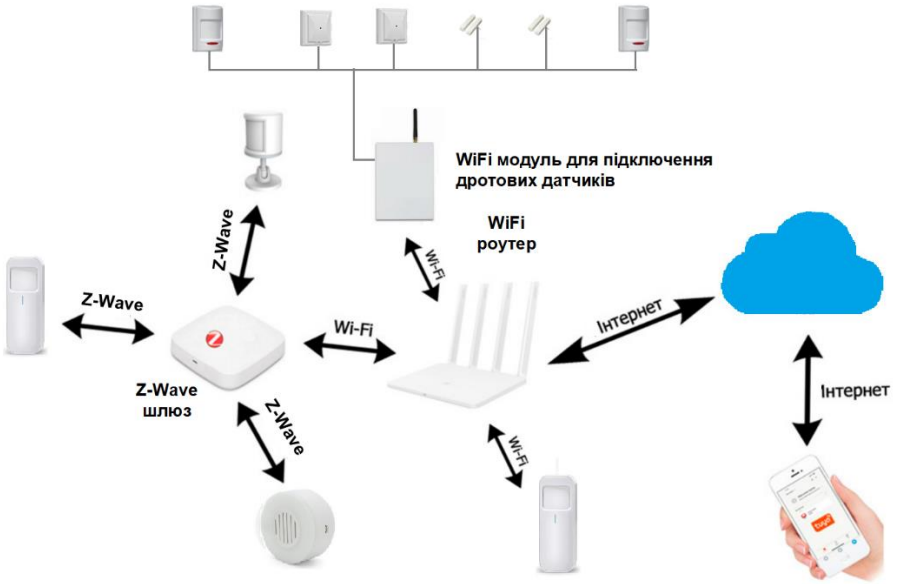

Рисунок 2.3 — Система безпеки з підтримкою IoT та можливістю підключення бездротових та дротових датчиків

Саме цей варіант візьмемо за основу для розглядуваної системи безпеки.

2.2 Визначення архітектури мікропроцесорної мультисенсорної системи безпеки

Розглядувану систему будемо реалізовувати за архітектурою, що наведена на рис. 2.3. Така система може бути побудована з використанням готового обладнання сторонніх виробників. Не зважаючи на те, що вона за рахунок зміни переліку використовуваних компонентів може бути легко адаптована під конкретного замовника, така архітектура підходить до забезпечення безпеки не великих об’єктів. Перш за все це пов’язано з тим, що вона будується навколо WiFi роутера, що обмежує область охоплення радіусом забезпечення надійного зв’язку WiFi, який для приміщень складає до 60 м. Цю проблему можна вирішити за рахунок поділу об’єкту на зони, в кожній з яких контроль безпеки буде забезпечуватися системою з архітектурою, що зображена на рис. 2.3. Однак у цьому випадку ускладняється здійснення централізованого контролю за безпекою об’єкта у цілому.

З іншого боку через те, що архітектура, зображена на рис. 2.3, орієнтована на використання готових рішень, вона є надмірною. В системі, що зображена на рис. 2.1, WiFi роутер є ключовим елементом системи, що забезпечує зв’язок з WiFi датчиками та хмарним сервером. В системі, що зображена на рис. 2.3, ці завдання можуть виконувати як Z-Wave шлюз, так і WiFi модуль, що забезпечує зв’язок з бездротовими датчиками, за умови підтримки ними можливості підключення до Інтернет через Ethernet з’єднання.

З врахуванням усього викладеного вище приходимо до архітектури мультисенсорної системи безпеки, що представлена у додатку Б. Головним елементом запропонованої архітектури є приймально-контрольний пристрій, який поєднує у собі функції WiFi роутера та Z-Wave шлюза. Завдяки цьому він

надає можливість використання бездротових WiFi та Z-Wave датчиків. Пристрій також підтримує Ethernet підключення до Інтернет для зв’язку з віддаленим хмарним сервером.

Підключення дротових датчиків здійснюється через відповідні контролери. Дротові датчики можуть бути неадресними або адресними [3]. Неадресні датчики є пороговими пристроями, що мають фіксований поріг чутливості. Такі датчики об′єднуються у групи, кожна з яких включається в один шлейф охоронної сигналізації. Порогові датчики реагують на зміну контрольованого параметра зміною свого вихідного опору, тому у разі спрацювання одного з тих, що підключені до одного шлейфа, формується сигнал тривоги у всьому шлейфі. Особливістю використання неадресних датчиків є те, що рішення про небезпеку приймається самим датчиком. Оскільки на роботу датчика можуть впливати різні зовнішні фактори, наприклад, стрибки напруги, це обумовлює доволі значну імовірність хибних спрацювань.

Адресні датчики відрізняються наявністю у них адресу, що дозволяє визначити місце порушення параметру безпеки. Кожен датчик має свій унікальний адрес, а тому приймально-контрольний пристрій може точно визначити який саме датчик спрацював.

Одним з типів адресних датчиків є інтелектуальні датчики, в які дозволяють надавати інформацію про поточне значення контрольованого параметра шляхом їх опитування. Опитування датчиків у шлейфі відбувається за рахунок надсилання запиту про стан до кожного датчика у шлейфі по черзі за зростанням їх адресів. Під час кожного періоду опитування від кожного датчика отримується нове значення контрольованого ним параметру. У результаті рішення про небезпеку приймається самим датчиком приймально-контрольним пристроєм.

Використання контролерів дротових датчиків дозволяє розширити контрольовану зону та зменшити навантаження на приймально-контрольний

пристрій. Кожен з контролерів може контролювати стан безпеки у певній зоні, наприклад в одній або кількох поруч розташованих кімнат, аналізуючи стан бездротових датчиків відкриття вікон та дверей, датчиків руху тощо.

Для підключення контролерів бездротових датчиків до приймально-контрольного пристрою передбачимо можливість використання або бездротового, або дротового каналів зв’язку. Для організації бездротового зв’язку між приймально-контрольним пристроєм та контролерами дротових датчиків передбачаємо використання технології Z-Wave.

Зазвичай дротовий зв’язок між пристроями в охоронних системах організовується через інтерфейс RS-485, який є одним з найбільш поширених стандартів фізичного рівня. Каналом зв′язку є вита пара, утворена двома дротами, які позначаються як лінії A і B. Передача даних відбувається за допомогою диференціальних сигналів, які формуються різницею потенціалів між лініями A та B витої пари. Різниця потенціалів виникає за рахунок передачі прямого сигналу по лінії A та інверсного по лінії Завдяки цьому між лініями A та B завжди присутня різниця потенціалів: позитивна при передаванні "1" та негативна при передаванні "0".

3 РОЗРОБКА АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ СИСТЕМИ БЕЗПЕКИ

3.1 Розробка структурної схеми приймально-контрольного пристрою

Відповідно до запропонованої архітектури системи безпеки приймально-контрольний пристрій повинен забезпечувати контроль за станом різноманітних датчиків, передачу даних про їх стан до хмарного серверу, формувати сигнал тривоги у разі спрацювання будь-якого з датчиків. Формування сигналу тривоги забезпечується за допомогою пристроїв звукової та світлової сигналізації. Поряд із цим, інформація про порушення стану безпеки може передаватися на пульт служби охорони. На об’єкті місце порушення безпеки визначається через підключення до хмарного сервера.

Відповідно до з цих завдань приймально-контрольний пристрій повинен підтримувати підключення бездротових WiFi та Z-Wave датчиків, взаємодію з контролерами бездротових датчиків через бездротове Z-Wave з’єднання або з’єднання через інтерфейс RS-485, Ethernet підключення до Інтернет, можливе вмикання пристрою звукової або світлової сигналізації, відправлення повідомлень через канали мобільного зв’язку тощо. У результаті приходимо до структурної схеми приймально-контрольного пристрою, яка наведена у додатку В.

Головним блоком приймально-контрольного пристрою є мікроконтролер, який забезпечує виконання усіх перерахованих вище функцій. Прийом сигналів від бездротових датчиків здійснюється за рахунок підтримання мікроконтролером функцій координатора мережі Z-Wave. Також виконання функцій координатора дозволяє отримувати сигнали від контролерів дротових датчиків у разі використання бездротового з’язку з ними.

Підключення мікроконтролера до мережі Z-Wave та його робота у режимі координатора цієї мережі забезпечується модулем Z-Wave. Отримання мікроконтролером даних від бездротових WiFi датчиків забезпечується за допомогою модуля WiFi.

У разі підключення контролерів дротових датчиків через дротовий канал RS-485, усі контролери підключають до витої пари паралельно. У результаті обмін даними між приймально-контрольним пристроєм та кожним з контролерів здійснюється по одних і тих самих лініях. Тому для коректної роботи передача та прийом даних відбуватися у різні часові інтервали так, що у кожний момент часу у режимі передачі працює лише один пристрій: або приймально-контрольний, або контролер. Решта пристроїв працюють в режимі прийому та одночасно отримують ці дані. Таким чином взаємодія мікроконтролера з контролерами дротових датчиків відбувається у режимі master-slave, що передбачає обмін даними у форматі «запит-відповідь».

Підключення мікроконтролера до витої пари здійснюється за допомогою модуля RS-485, що забезпечує перетворення диференціальних сигналів у лініях у напруги, що відповідають логічним значенням сигналів мікроконтролера.

Передача повідомлень про стан датчиків до хмарного сервера здійснюється мікроконтролером через модуль Ethernet, основним завданням якого є підтримання канального та фізичного рівнів моделі OSI відповідно до стандарту IEEE 802.3. Особливістю мережі Ethernet є використання механізму множинного доступу з контролем несучої та виявлення колізій (CSMA/CD, Carrier Sense Multiple Access / Collision Detection) для доступу до каналу зв’язку. Це дозволяє комп’ютерам у мережі спільно використовувати єдиний канал зв’язку без втрати даних.

Передача сигналу тривоги на пульт служби охорони може відбуватися через Інтернет, з використанням телефонної лінії або GSM каналу. У розглядувані системі передбачається використання мобільного зв′язку, що забезпечується модулем GSM.

Мережа GSM є глобальним цифровим стандартом для стільникового зв'язку, з поділом каналу за принципом TDMA та забезпеченням високого ступеня безпеки завдяки шифруванню з відкритим ключем. Для передачі

інформації використовуються 4 діапазони частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц.

Останнім структурним блоком приймально-контрольного пристрою є блок комутації, основним призначенням якого є вмикання будь-якого зовнішнього пристрою для формування звукового або світлового сигналу тривоги. Фактично блок комутації забезпечує замикання/розмикання електричного кола.

3.2 Розробка функціональної схеми приймально-контрольного пристрою

Розробку функціональної схеми приймально-контрольного пристрою розпочнемо з вибору елементної бази. Головним елементом пристрою є мікроконтролер. У даний час на ринку широко представлені мікроконтролери різної архітектури та різних виробників. Поряд із цим пропонуються і готові рішення у вигляді одноплатних мікроконтролерних модулів, які на одній платі крім мікроконтролера містять додаткові компоненти, що дозволяє швидко реалізовувати різноманітні проекти. Тому для реалізації приймально-контрольного пристрою доцільно орієнтуватися на використання саме таких модулів.

Основними критеріями при виборі модуля для побудови приймально-контрольного пристрою є наявність у ньому апаратної підтримки інтерфейсів Z-Wave, WiFi та Ethernet. Крім того, необхідна підтримка кількох послідовних асинхронних інтерфейсів UART для забезпечення підключення додаткових модулів та до мережі RS-485. Найбільш повно цим критеріям задовольняє одноплатний комп’ютер Raspberry Pi4 Model B.

Raspberry Pi4 Model B (рис. 3.1) є одноплатним комп'ютером, що побудований на однокристальній системі Broadcom BCM2711. Кристал включає 4-ядерний 64-бітний процесор CPU Cortex-A72 (ARM v8) з частотою 1,5 ГГц і графічний процесор GPU VideoCore VI з частотою 500 МГц. На платі є чотири порти USB, два HDMI-виходи під монітори, бездротовий модуль Wi-

Fi/Bluetooth та повноцінний гігабітний Ethernet.

Можливість бездротових підключень забезпечується чипом BCM43143 WiFi, що підтримує стандарти Wi-Fi 802.11 b/g/n/ac та протокол Bluetooth 4.2 с BLE. Це робить Raspberry Pi4 Model B готовим рішенням для використання у мережі WiFi. Модель обладнана 1 ГБ оперативної пам'яті SDRAM, яка ділиться між CPU та GPU.

Рисунок 3.1 — Одноплатний комп’ютер Raspberry Pi4 Model B

Основні характеристики Raspberry Pi4 Model B:

— процесор: 64-ох бітний Broadcom BCM2837B0, 1.4ГГц, 4-ядра ARM Cortex-A72;

— графічний процесор: двоядерний VideoCore IV;

— оперативна пам’ять: 1ГБ LPDDR4-2400;

— бездротовий зв’язок: Wi-Fi 2.4ГГц/5ГГц IEEE 802.11 b/g/n/ac, Bluetooth Low Energy v5.0 (BLE);

— 10/100 BaseT Ethernet (максимальна пропускна здатність 300 Мбит / с);

— 2 порти USB 2.0, 2 порти USB 3.0;

— 40-контактний роз'єм GPIO;

— повнорозмірний HDMI;

— порт камери CSI для підключення камери;

— порт дисплея DSI для підключення сенсорного екрану Raspberry Pi;

— 4-полюсний стереовихід та композитний відео порт;

— порт micro SD для завантаження операційної системи та збереження даних;

— максимальне споживання 5 В/3,0 А постійного струму;

— підтримка Power-over-Ethernet (PoE) (потрібен окремий PoE HAT).

На рис. 3.2 представлена схема сигналів роз'єму на платі Raspberry Pi4 Model B, призначеного для підключення зовнішніх компонентів.

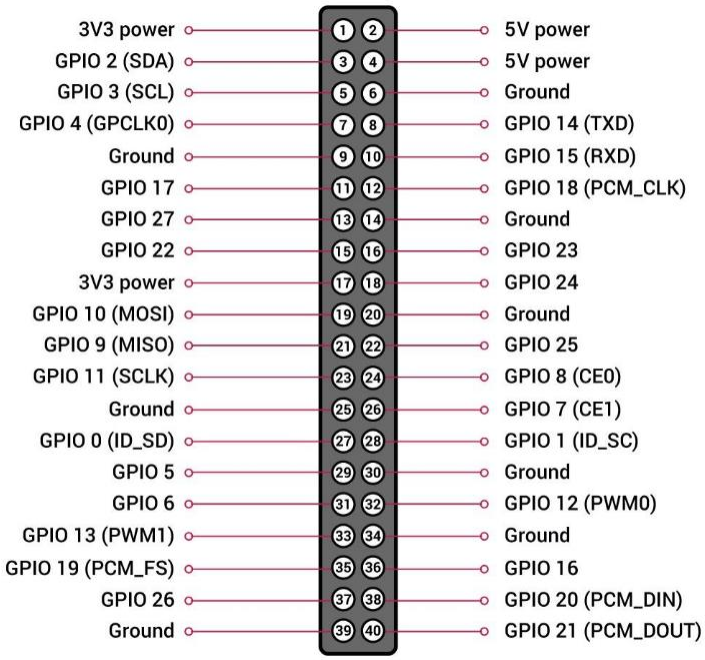

Рисунок 3.2 — Схема сигналів контактів роз'єму Raspberry Pi4 Model B для підключення зовнішніх елементів

Як витікає з характеристик модуля Raspberry Pi4 Model B він обладнаний засобами для підтримання бездротових підключень. Тому він може бути використаний як WiFi роутер без застосування додаткових зовнішніх компонентів. Поряд із цим, модуль Raspberry Pi4 Model B не має засобів для підтримання Z-Wave підключень. Це вимагає необхідність використання додаткових компонентів.

Для забезпечення підтримання підключень до мережі Z-Wave було

вибрано плату розширення Z-Wave.Me RaZberry7 Pro для Raspberry Pi (рис. 3.3). Плата розширення Z-Wave.Me RaZberry7 Pro дозволяє забезпечити можливість керування обладнанням Z-Wave з боку Raspberry Pi, перетворюючи Raspberry Pi на контролер Z-Wave [28].

Плата сумісна з Raspberry Pi 1/2/3A/3B/3A+/3B+/4B та Z-Wave пристроями різних виробників (понад 2000 сумісних пристроїв). У комплекті додається програмне забезпечення Z-Way, що має відкрите API для реалізації взаємодії з нею та дозволяє створювати різноманітні сценарії управління. Модуль RaZberry також підтримує стандартний Zensys API (SerialAPI) та сумісний з такими програмами як Home Assistant, Z-Cloud, OpenHAB, OpenZ-Wave та OpenRemote.

Рисунок 3.3 — Плата розширення Z-Wave.Me RaZberry7 Pro

Завдяки сумісності з моделями Raspberry Pi та проектами з відкритим вихідним кодом, такими як Home Assistant, OpenZWave, OpenHAB, FHEM та Domoticz, Z-Wave.Me RaZberry7 Pro легко інтегрується у мережу Z-Wave [28].

Програмне забезпечення Z-Way має такі характеристики:

— сертифіковане програмне забезпечення, написане на C/C++/JavaScript;

— підтримка функцій контролера мережі: увімкнення/виключення та налаштування мережі;

— надає API рівнів C та/або JSON по HTTP;

— сервер домашньої автоматизації на базі модулів JavaScript;

— підтримувані класи команд: AlarmSensor, Association, Basic, Battery, Configuration, Clock, Door Lock, DoorLockLogging, Indicator, Manufacturer Specific, Meter, Multichannel, Multichannel Association, MultiCommand, NodeNaming, Protection, SceneActivation, SceneActuator inary , SensorConfiguration, SensorMultilevel, SwitchAll, SwitchBinary, SwitchMultilevel, ThermostatFanMode, ThermostatFanState, ThermostatMode, ThermostatOperatingState, Time, TimeParameters, ThermostatSetpoint, UserCode, Version, Wake-up [28].

Основні характеристики Z-Wave.Me RaZberry7 Pro:

— робоча частота: 868.42 МГц / 869.0 МГц (перемикається з ПЗ);

— збільшена дальність радіозв'язку завдяки новому чіпу Z-Wave 7-го покоління;

— інтерфейс UART.

Для забезпечення зв’язку з контролерами дротових датчиків через мережу RS-485 необхідно забезпечити підтримку фізичного рівня інтерфейсу RS-485. Для цього використаємо модуль RS485 TTL (рис. 3.4) від торгової марки Arduino. Модуль реалізований на мікросхемі MAX485 та призначений для здійснення прямого та зворотного перетворення між сигналами ТТЛ та сигналами стандарту RS485 [29].

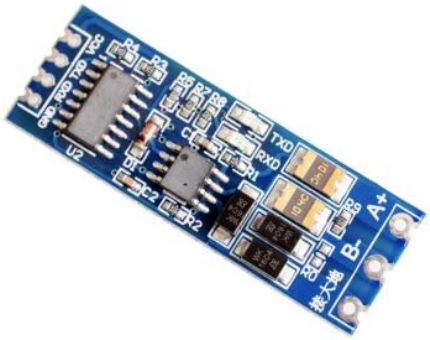

Рисунок 3.4 — Модуль RS485 TTL

Призначення контактів роз'єму з боку UART TTL:

— DI - вхід передавача;

— DE (driver enable) — дозвіл роботи передавача;

— RE (receiver enable) — дозвіл роботи приймача;

— RO - вихід приймача.

Призначення контактів роз'єму з боку RS-485:

— «+» живлення;

— A — прямий диференційний вхід / вихід лінії RS-485;

— B — інверсний диференціальний вхід / вихід лінії RS-485;

— GND —загальний.

Підтримання можливості передачі сигналу тривоги на пульт служби охорони вимагає використання засобу GSM з'язку. Сьогодні у різних проектах для реалізації GSM з'язку найбільш широко використовується GSM/GPRS модуль SIM800L (рис. 3.5) на однойменному чіпі SIM800L. Модуль SIM800L є GSM-модемом, який за функціональними можливостями аналогічний звичайному мобільному телефону. Він дозволяє відправляти SMS повідомлення, передавати або приймати телефонні дзвінки, підключатися до Інтернету через GPRS, TCP/IP та т.і. [30].

Рисунок 3.5 — GSM/GPRS модуль SIM800L

Модуль підтримує чотирьохдіапазонну мережу GSM/GPRS 850/900/1800/1900 МГц і може використовуватися з SIM картою будь-якого оператора мобільного зв'язку. Взаємодія з модулем відбувається через послідовний асинхронний інтерфейс UART з використанням AT команд, які є командами текстового протоколу. В табл. 3.1 представлені основні

характеристики модуля SIM800L [31].

Останнім структурним блоком приймально-контрольного пристрою є блок комутації. Основним електронним компонентами, які використовуються для комутації силових електричних кіл, є симистор та електромагнітне реле. Симистор є напівпровідниковим приладом, що в залежності від значення сигналу управління може перемикатися з низькоомного стану до високоомного та навпаки. Електромагнітне реле є електромеханічним приладом, в основі якого лежить електромагнітне реле є котушкою. При протіканні струму через котушку відбувається замикання чи розмикання контактів реле.

Таблиця 3.1 — Основні технічні характеристики GSM модуля SIM800L

Параметр	Значення
Робочі діапазони	EGSM900, DCS1800, GSM850, PCS1900
Потужність передачі DCS1800, PCS1900	1 Вт
Потужність передачі GSM850, EGSM900	2 Вт
Робочі частоти	850, 900, 1800, 1900 МГц
Режим мережі	2G
Зовнішній інтерфейс	UART TTL
Максимальна швидкість передачі даних	85,6 Кбод
Управління	AT команди
Кодування	CS-1, CS-2, CS-3, CS-4
Підтримувані протоколи	PBCCH, CSD, USSD, PAP, RTC
Струм споживання в режимі очікуваання	0,7 мА
Струм споживання в піковому режимі	2 А
Робочий діапазон напруг	від 3.7 В до 4.2 В

Оскільки електромагнітне реле є більш простим у керуванні для реалізації блоку комутації будемо використовувати реле. Для керування реле зазвичай використовується ключовий каскад на транзисторі. Оскільки усі інші структурні блоки приймально-контрольного пристрою будуть будуватися з використанням готових модулів, для побудови блоку комутації доцільно також скористатися готовим релейним модулем. Відповідно до цього вибираємо одноканальний

релейний модуль Arduino Relay Module 1 relay 5V (рис. 3.6).

Рисунок 3.6 — Релейний модуль Arduino Relay Module 1 relay 5V

Основні характеристики модуля Arduino Relay Module 1 relay 5V представлені в табл. 3.2 [31].

Таблиця 3.2 — Основні характеристики релейного модуля Arduino Relay Module 1 relay 5V

Параметр	Значення
Напруга живлення	5 В
Напруга вмикання	від 3,3 В до 5 В
Максимальний комутований струм	10 А
Максимальна комутована напруга	250 В змінного струму

	30 В постійного струму
Кількість перемикань	20 млн

З використання вибраних компонентів була розроблена функціональна схема приймально-контрольного пристрою, яка наведена у додатку Г. Приймально-контрольний пристрій побудований на одноплатному мікрокомп'ютері Raspberry Pi 4 Model B, головним елементом якого є потужний 64-ох бітний 4-ох ядерний ARM мікроконтролер BCM2837B0.

Підключення пристрою до Інтернет здійснюється через з'єднання з Ethernet мережею та забезпечується мікросхемою BCM54213PE. Мікросхема BCM54213PE є тришвидкісним трансівером Gigabit Ethernet, що підтримує усі функції фізичного рівня стандарту Ethernet. Підключення до мережу Wi-Fi забезпечується мікросхемою BCM43013, яка є комбінованим контролером Wi-Fi/Bluetooth 5.0, що об′єднує на одному кристалі мікроконтролер та радіомодуль.

Інші компоненти схеми є зовнішніми відносно Raspberry Pi4 Model B елементами, що підключені до нього через контакти роз'єму на платі Raspberry, що спеціально передбачений для організації взаємодії між Raspberry Pi4 Model B та зовнішніми компонентами.

Підключення модулів Z-Wave.Me RaZberry7 Pro, RS485 TTL та SIM800L повинно відбуватися через послідовний асинхронний інтерфейс. UART0, UART1. В Raspberry Pi 4 доступні шість універсальних асинхронних приймачів/передавачів UART, що можуть бути використані для цього: UART0, UART1, UART2, UART3, UART4 та UART5. Відповідно до документації лінії послідовних даних для них є альтернативними функціями таких ліній введення/виведення загального призначення GPIO мікроконтролера BCM2837B0:

UART0: TxD0 — GPIO14, RxD0 — GPIO15;

UART1 (mini UART): TxD1 — GPIO14, RxD1 — GPIO15;

UART2: TxD2 — GPIO0, RxD2 — GPIO1;

UART3: TxD3 — GPIO4, RxD3 — GPIO5;

UART4: TxD4 — GPIO8, RxD4 — GPIO9;

UART5: TxD5 — GPIO12, RxD5 — GPIO15.

Взаємодія з модулем Z-Wave.Me RaZberry7 Pro, що забезпечує підключення Raspberry Pi4 Model B до бездротової мережі Z-Wave, відбувається через послідовний асинхронний канал зв'язку, обмін даними по якому забезпечується універсальним асинхронним приймачем/передавачем UART0 (лінії GPIO14 та GPIO15).

Обмін даними всередині системи між приймально-контрольним пристроєм та контролерами дротових датчиків може відбуватися або через бездротовий канал мережі Z-Wave, або дротове підключення до мережі RS-485. Для Підключення приймально-контрольного пристрою до мережі RS-485 здійснюється через перетворювач RS-485TTL. Обмін повідомленнями буде забезпечуватися асинхронним приймачем/передавачем UART4 (лінії GPIO8 та GPIO9).

Оскільки прийом та передача даних відповідно до стандарту RS-485 здійснюється з використанням одних і тих самих лінії A та B, в трансиверах RS-485 передбачений цифровий вхід RE/DE для керування напрямом передачі. Цей вхід підключений до лінії GPIO7. Сигнал низького логічного рівня на вході RE/DE переводить трансивер в режим прийому, сигнал високого логічного рівня — в режим передачі. Підключення приймально-контрольного пристрою до каналу зв'язку RS-485 здійснюється через роз'єм X1.

Підключення GSM/GPRS модуля SIM800L до Raspberry Pi4 Model B здійснюється через лінії GPIO4 та GPIO5. Відповідно для обміну даними з модулем SIM800L буде використовуватися UART2.

Керування релейним модулем Arduino Relay Module 1 relay 5V здійснюється через лінію GPIO16. Вмикання реле забезпечується сигналом високого логічного рівня, вимикання — низького.

3.3 Розробка структурної схеми контролера дротових датчиків

У запропонованій архітектурі системи безпеки контролер дротових датчиків забезпечує контроль за станом датчиків неадресного та адресного типу, які передбачають підключення через дротове з'єднання. У випадку спрацювання будь-якого з датчиків інформація про це повинна бути надіслана у приймально-контрольний пристрій через бездротовий канал зв'язку Z-Wave. Як альтернативний канал зв'язку може бути використане з'єднання через диференційний дротовий канал передачі даних RS-485.

Відповідно до цих завдань була розроблена структурна схема контролера дротових датчиків, яка наведена у додатку Д. Основним елементом контролера є мікроконтролер. Він забезпечує безперервний контроль за станом шлейфів охоронної сигналізації. У результаті виявлення спрацювання будь-якого з датчиків, що підключені до цих шлейфів, мікроконтролер формує та надсилає відповідне повідомлення у приймально-контрольний пристрій.

Сигнали від неадресних датчиків отримуються мікроконтролером через модуль контролю неадресного шлейфу. Неадресні датчики мають релейні виходи і можуть перебувати лише у двох станах: «норма» та «тривога». За принципом функціонування вони є пороговими пристроями. При виході значення контрольованого параметра за задані межі відбувається перемикання контактів реле у протилежний стан, що обумовлює зміну вихідного опору датчика.

Порогові датчики поділяються на датчики з нормально розімкнутими та нормально замкненими контактами. Датчики з нормально розімкнутими контактами вмикаються у шлейф паралельно, а датчики з нормально замкненими контактами — послідовно (рис. 3.7). Шлейф перебуває під напругою і по ньому протікає певний струм. Спрацьовування хоча б одного із датчиків відбувається зміна струму у шлейфі.

Для запобігання короткому замиканню шлейфу при спрацюванні датчика з нормально розімкненим виходом, послідовно з кожним датчиком

підключається резистор $R_{Пар}$. Цілісність шлейфу контролюється за допомогою кінцевого резистора $R_{Терм}$, опір якого визначає значення струму у шлейфі у черговому режимі. При спрацьовуванні датчика, його контакти замикаються, що призводить до збільшенню струму у шлейфі. При обриві шлейфу струм падає до нуля.

Датчики з нормально замкненими контактами включаються у шлейф послідовно. При спрацьовуванні датчика струм у шлейфі стрибкоподібно зменшується. Для отримання можливості фіксувати обрив шлейфу (обрив сприймається як спрацювання датчика), паралельно контактам датчика вмикається резистор $R_{Посл}$. При такому варіанті при спрацьовуванні датчика струм буде протікати через шунтувальний резистор $R_{Посл}$. Як і попередньому випадку при обриві шлейфу струм падає до нуля.

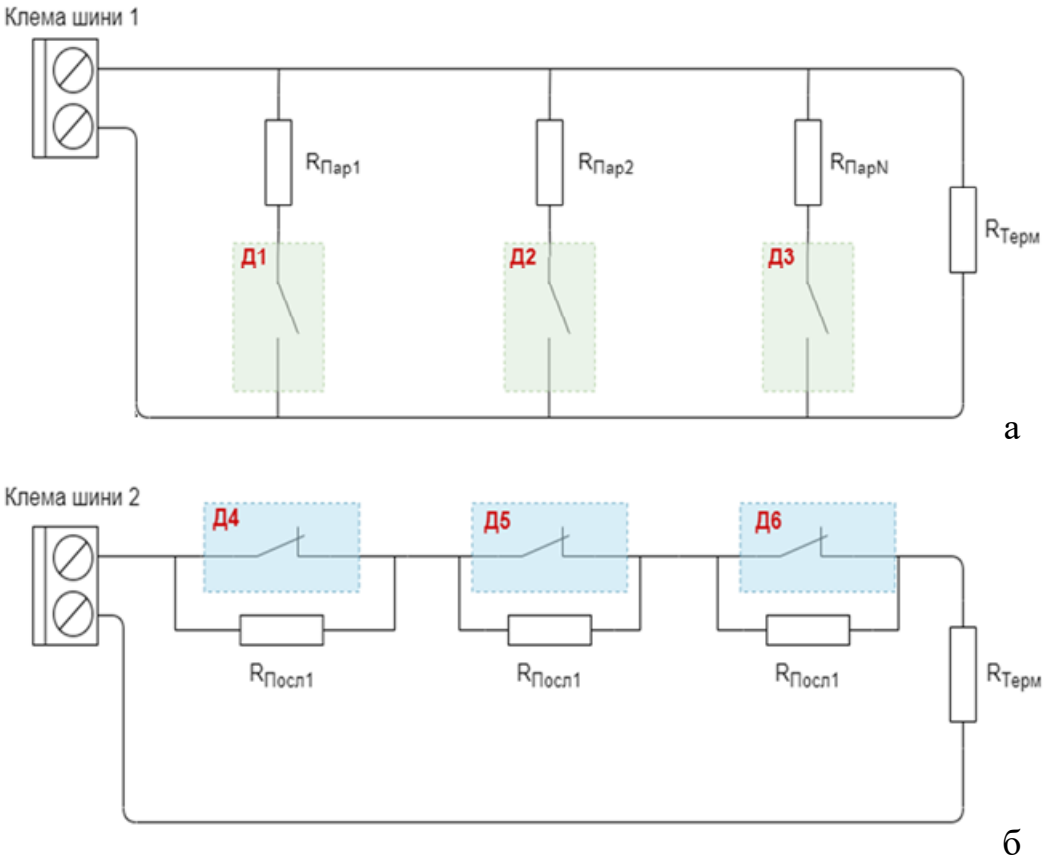

Рисунок 3.7 — Паралельне (а)та послідовне (б) підключення датчиків до шлейфу

Часто використовуються так звані комбіновані шлейфи, в яких одночасно

використовуються датчики з нормально розімкненими та нормально замкненими контактами.

Зміна струму у шлейфі фіксується модулем контролю неадресного шлейфу і перетворюється у зміну логічного значення сигналу на виході контролера. За цією зміною мікроконтролер визначає спрацювання датчика у шлейфі.

Контроль за станом адресних датчиків здійснюється мікроконтролером через модуль контролю адресного шлейфу. Взаємодія з адресними датчиками відбувається через обмін даними з ними у режимі «master-slave». Ведучим є мікроконтролер. Датчики є веденими. Кожен з адресних датчиків має свій унікальний адрес, що дозволяє мікроконтролеру ідентифікувати кожний датчик.

Каналом зв’язку з адресним датчиками є адресний шлейф, який є двопровідною лінією, одна з ліній якого є лінією даних, а інша — лінією «земля». Адресний шлейф будується за топологією загальної шини, відповідно до якої кожен з пристроїв підключається до єдиної магістралі паралельно до інших. Для підвищення надійності зв′язку шину замикають у кільце, що дозволяє підтримувати зв′язок з датчиками навіть при обриві шлейфу.

Як було зазначено взаємодія з адресними датчиками відбувається в режимі «master-slave», що передбачає циклічне послідовне опитування датчиків одного за одним. Під час опитування мікроконтролер надсилає у шлейф команду із запитом стану датчика, в який задається адрес чергового датчика. Усі датчики приймають цю команду, але відповідь на неї надсилає лише той, адрес якого відповідає адресу зазначеному у команді.

Отримувані з адресних датчиків дані аналізуються мікроконтролером і у випадку виявлення змін у них, надсилаються у приймально-контрольний пристрій або канал зв’язку мережі Z-Wave, або мережі RS-485.

Зв’язок з приймально-контрольним пристроєм через бездротовий канал Z-Wave забезпечується однойменим модулем, що реалізує підтримує функції фізичного та канального рівнів. Зокрема, блок Z-Wave забезпечує доступ до

радіоканалу та обмін пакетами даних через нього.

Підключення мікроконтролера до двопровідної лінії зв′язку каналу RS-485 відбувається за допомогою інтерфейсного модуля RS-485. Модуль забезпечує обмін даними згідно принципу диференціальної передачі сигналів.

3.4 Розробка функціональної схеми контролера дротових датчиків

Розробку функціональної схеми контролера дротових датчиків розпочнемо з вибору елементної бази. Як і у випадку приймально-контрольного пристрою, контролер дротових датчиків будемо будувати на одноплатному мікроконтролерному модулі. Оскільки функціонально контролер дротових датчиків є більш простим пристроєм побудови, ніж приймально-контрольний пристрій, використовувати для його побудови одноплатний комп'ютер Raspberry Pi4 Model B не доцільно.

Основними критеріями при виборі мікроконтролерного модуля є апаратна підтримка підключення до мережі Z-Wave, наявність кількох каналів асинхронної послідовної передачі даних. Відповідно до цих критеріїв було вибрано модуль Модуль Z-Uno 2 (рис. 3.8), що виконаний у парадигмі популярного модуля Arduino. Основу модуля складає 32-ох бітний мікроконтролер 7 покоління ZGM130S з ядром CortexM4F, 39 МГц та підтримкою Z-Wave. Для підключення зовнішніх компонентів доступні 26 цифрові входи/виходи (рис. 3.9). Як середовище розробки програмного забезпечення та для програмування модуля може використовуватися Arduino IDE [32].

Рисунок 3.8 — Зовнішній вигляд модуля Z-Uno 2

Модуль Z-Uno 2 не може бути використаний як координатор мережі Z-Wave, але для контролера дротових датчиків це і не потрібно. Координатором мережі Z-Wave у розглядуваній системі безпеки є приймально-контрольний пристрій.

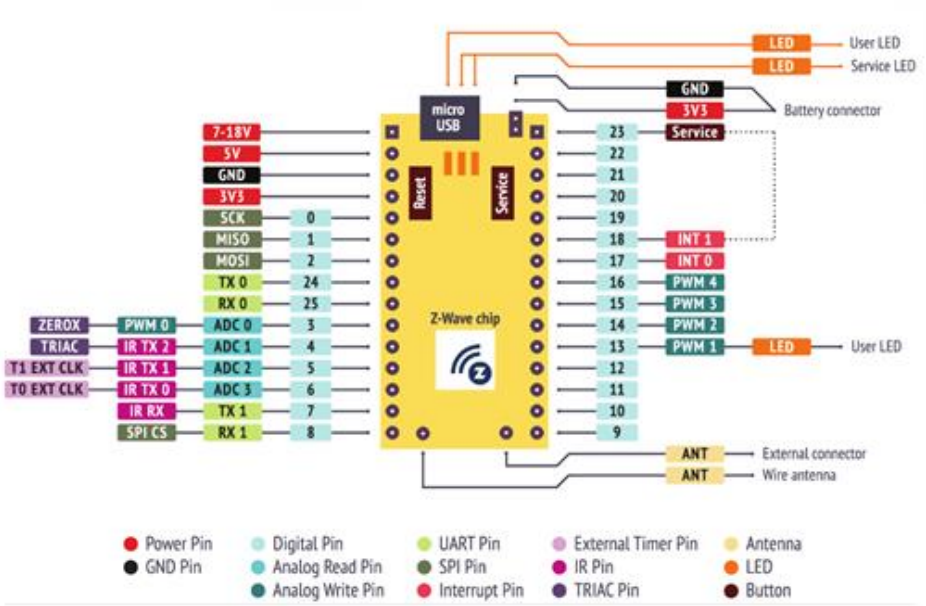

Рисунок 3.9 — Схема контактів для підключення модуля Z-Uno 2

Основні технічні параметри модуля Z-Uno 2 [32]:

— 39 МГц тактова частота;

— 32-х бітний мікропроцесор архітектури CortexM4F;

— 40 кБ флеш пам'ять для вашого коду;

— 8 кБ оперативної пам’яті;

— 2 кБ енергонезалежної пам’яті EEPROM;

— Z-Wave радіопередавач на швидкостях 9.6/40/100 кБіт/с;

— 26 ліній введення/виведення загального призначення (на будь-якому висновку можлива обробка зовнішніх переривань, до 16 одночасно);

— 4 АЦП;

— 4 ШИМ;

— 3 SPI/UART (роздільне використання);

— 1 USB з окремим контролером CP2102 (використовує 1 із UART);

— 1 апаратний I2C;

— 1-wire (програмний);

— 2 16-ти бітних багатоканальних таймерів;

— 1 32-бітний багатоканальний таймер;

— сервісні LED, 1 сервісна кнопка;

— 1 користувальницький LED;

— живлення: USB 5 В, зовнішнє 3,3 В, зовнішнє 4-15 В.

Для забезпечення підключення до мережі RS-485, так само як і в приймально-контрольному пристрої, використаємо модуль RS485 TTL (рис.3.4).

Як було зазначено при розробці структурної схеми основним контрольованим параметром в неадресному шлейфі є струм. Найпростішим варіантом здійснити контроль за струмом у шлейфі є використання резистора. При вмиканні резистора зі шлейфом, падіння напруги на резисторі буде пропорційне струму у шлейфі.

Вмикання резистора вносить додатковий опір у шлейф, що впливає на його роботу та збільшує потужність, що розсіюється. Для зменшення цього негативного впливу опір резистора повинен бути малим. Проте зменшення опору резистора робить його опір сумірним з опором самого шлейфу. У результаті падіння напруги на низькоомному резисторі також буде малим, що вимагає підсилення напруги.

Існують два основних методи вимірювання струму — на боці «землі» та на боці джерела. Кожен з них має свої переваги та недоліки, але на практиці перевагу надають другому з них, який дозволяє виявляти коротке замикання. Типова схема будується з використанням операційного резистора (рис. 3.10).

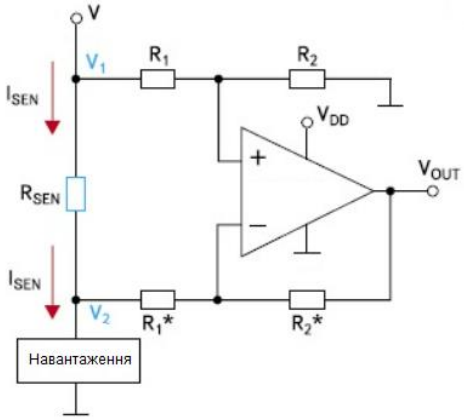

Рисунок 3.10 — Схема контролю значення струму

Як операційний підсилювач вибираємо мікросхему LM741, яка є типовим операційним підсилювачем з високим коефіцієнтом підсилення, що не вимагає частотної корекції, має захист від короткого замикання та підтримує широкий діапазон напруг. Відмінні робочі характеристики мікросхеми забезпечують її широке використання [34].

Основні характеристики операційного підсилювача LM741 наведені у табл. 3.3.

Таблиця 3.3 — Основні характеристики операційного підсилювача LM741

Параметр	Значення
Напруга живлення	від -22 В до +22 В
Діапазон вхідних напруг	від -15 В до +15 В
Напруга зміщення	1мВ
Вхідний струм зміщення	20 нА
Вхідний струм утікання	80 нА
Вхідний опір	2 МОм
Коефіцієнт підсилення	$2 \cdot 10^5$

Взаємодія з адресними датчика через адресний шлейф відбувається за

рахунок обміну двійковими даними по однопровідній лінії зв′язку. Таким чином ця лінія зв’язку бути підключена безпосередньо до мікроконтролера. Проте у цьому випадку цифрові входи мікроконтролера не будуть захищеними від можливих стрибків напруги у шлейфі. Для захисту лінії введення/виведення мікроконтролера, яка буде підключатися до лінії зв’язку, скористаємося двонаправленим формувачем послідовної шини. Типовим прикладом такого формувача є мікросхема PCA9515, на якій буде побудований модуля контролю адресного шлейфу.

Мікросхема PCA9515 призначена для застосування як шинний формувач I2C-bus і SMBus. За рахунок буферизації підвищується навантажувальна спроможність шини, що дозволяє підключати до неї більше пристроїв. Крім того, використання PCA9515 дозволяє системи ізолювати дві половини шини, збільшуючи або довжину шини, або кількість підключених до неї пристроїв. Даний формувач також можна використати для підтримки двох ріхних шин, наприклад, однієї на 3,3 В, та іншої на 5 В [35].

З використанням вибраної елементної бази була розроблена функціональна схема контролера дротових датчиків системи безпеки, яка наведена у додатку Е. Основним функціональним блоком пристрою є модуль DD3 Z-Uno 2 на базі мікроконтролера 32-ох бітний мікроконтролер ZGM130S. Основними завданнями модуля є контроль за станом дротових датчиків різного типу та передача цієї інформації до приймально-контрольного пристрою системи безпеки.

Модуль підтримує взаємодію з неадресними та адресно-аналоговими датчиками. Підключення неадресних датчиків здійснюється через роз’єм X3. Стан неадресних датчиків контролюється за значенням струму, що протікає через неадресний шлейф, до якого вони підключені. Живлення шлейфу здійснюється від напруги +24 В.

Значення струму у неадресному шлейфі контролюється за значенням напруги на резисторі R6, що послідовно включений в його електричне коло.

Падіння напруги на резисторі R6 підсилюється операційним підсилювачем DA1 та подається на вхід ADC0 мікроконтролера, який функціонально є входом вбудованого у мікроконтролер аналого-цифрового перетворювача. Операційний підсилювач DA1 працює в режимі диференційного підсилювача. .Значення напруги на виході підсилювача за допомогою аналого-цифрового перетворювача перетворюється у цифровий код, який аналізується мікроконтролером.

Підключення шлейфу адресних датчиків до здійснюється через роз′єм X2. Контроль за станом адресних датчиків відбувається за рахунок отримання значення вихідного параметра кожного з датчиків через цифрову однопровідну лінію зв′язку, шляхом їх послідовного опитування. Передача мікроконтролером запитів до датчиків та отримання відповіді від них здійснюється у послідовному асинхронному напівдуплексному режимі. Дані можуть інтерпретуватися як команди (відповідно до заздалегідь.

Для підтримання працездатності системи при обриві шлейфу, використовується його замикання у кільце. У нормальному режимі обмін даними з датчиками здійснюється через буферний пристрій DD2 та лінію введення/виведення мікроконтролера, що з’єднана з контактом 9 на платі модуля DD3. Цілісність шлейфу контролюється за сигналом на лінії, з’єднана з контактом 10. При цілісному шлейфі сигнали на обох лініях будуть ідентичні.

При обриві шлейфу, обмін повідомленнями з датчиками відбуватиметься з використанням обох лінії, що забезпечить зв′язок з датчиками в обох частинах шлейфу, розділених місцем розриву. Буферний пристрій DD2 захищає входи мікроконтролера від стрибків напруги, які можуть виникати у шлейфі.

При спрацювання неадресного датчика, або при зміні у значеннях, отримуваних від адресних датчиків, мікроконтролер надсилає повідомлення у приймально-контрольний пристрій або через радіоканал Z-Wave, або через виту пару дротового інтерфейсу RS-485. Підключення мікроконтролера до бездротової мережі Z-Wave забезпечується апаратними засобами модуля DD3.

Можливість мікроконтролера обмінюватися даними через виту пару надається елементом DD1, який забезпечує підтримку фізичного рівня інтерфейсу RS-485. Оскільки для прийому та передачі даних у мережі RS-485 використовуються одна і та сама вита пара, обмін повідомленнями відбувається у напівдуплексному режимі. При цьому напрям передачі визначається логічним значенням сигналу на вході RE/DE елемента DD1. Керування напрямом здійснюється через цифрову лінію введення/виведення загального призначення мікроконтролера, що з'єднана з контактом 6 на платі модуля DD3.

Низький логічний рівень на цій лінії формується у момент прийому даних мікроконтролером, високий — під час їх передачі. Прийом та передача асинхронних даних по каналу RS-485 забезпечується універсальним асинхронним приймачем/передавачем UART1 мікроконтролера. Контакт 7 на платі модуля є лінією вихідних даних Tx1 UART1, а контакт 8 — лінією вхідних даних Rx1. Фізичне підключення до витої пари здійснюється через роз'єм X1.

Стабілізатор напруги DA2 забезпечує перетворення напруги +24 В, яка подається в контролер дротових датчиків і використовується для живлення шлейфів охорони, в напругу +5В, яка потрібна для живлення елементів DD1, DD2 та DD3.

3.5 Розробка програмного забезпечення для взаємодії з приймально-контрольним пристроєм

Одним з основних завдань, що вирішуються приймально-контрольним пристроєм, є взаємодія з хмарним сервером для надання можливості віддалено отримувати дані про стан системи безпеки. Обмін інформацією буде відбуватися за рахунок підтримання двох базових режимів: "getphone" для отримання інформації з хмари та "setobjstat" для новлення інформації про об'єкт у базі даних хмари.

На хмарі буде розміщений серверний компонент, що є набором скриптів та web сторінок, створених за допомогою технологій HTML, PHP та MYSQL.

Перелік основних скриптів представлений у табл. 3.4. Ядром серверного компоненту є база даних, що містить усю інформацію про користувачів, пристрої та їх стани.

Таблиця 3.4 — Окремі скрипти та їх призначення

Назва скрипта	Опис
INDEX.HTML	Показує навігацію по серверній компоненті. Є головним файлом

Продовження таблиці 3.4

LOGIN.PHP	Наступна сторінка, на якій можна ввійти в систему під певним користувачем
STATUS.PHP	Показує перелік всіх пристроїв та стан кожного з них
OPTIONS.PHP	Дозволяє змінювати налаштування кожного пристрою та його об’єктів.
USER.PHP	Налаштування користувача, де можна змінити номер та налаштувати бот для телеграм
API.PHP	Опрацювання запитів від Arduino контролера

Взаємодію між приймально-контрольним пристроєм та серверними компонентами забезпечено за допомогою засобів HTTP REST.

Обмін даними з серверною компонентами у хмарі здійснюється за допомогою скрипта api.php, лістинг якого наведений у додатку К. Скрипт API.PHP працює на базі бібліотеки Restbox і її класу RestUtil. Скрипт API.PHP

може працювати у двох режимах: безпосередньо приймально-контрольним пристроєм, за що клас device, та з клієнтськими мобільними пристроями, що забезпечується класом Mobale.

Створення сесії для роботи з приймально-контрольним пристроєм забезпечується за допомогою метода device_auth, лістинг якого наведений на рис. 3.11. Метод використовує метод outs, що забезпечує підключення пристрою до серверної компоненти. Під час підключення пристрій заносить свій ідентифікатор та токен доступу. Після цього він отримує ідентифікатор сесії.

Оновлення стану пристрої системи забезпечує метод device_update_status, лістинг якого наведений на рис. 3.12. Метод працює в режимі запит-відповідь. У запиті вказується ідентифікатор пристрою та його токен доступу.

```
// Device methods
case 'device_auth':
      if($context->method == "POST") {
      $sess_data = Device::CreateSession(
            $context->post['device_id'],
            $context->post['token']
      )
      return RestUtil::ReturnJson( $sess_data );
      } else {
      return RestUtil::ReturnError(400, 'Bad request');
      }
      break;
```

Рисунок 3.11 — Лістинг методу device_auth

```
case 'device_update_status':
      if( $context->method == "POST" &&
      Device::IsSessionValid(
            $context->post['token']
      )
      ) {
      $result = Device::SetStatus(
            $context->post['device_id'],
            $context->post['token']
      )
      return RestUtil::ReturnJson( $result );
      } else {
      return RestUtil::ReturnError(400, 'Bad session');
      }
      break;
```

Рисунок 3.12 — Лістинг методу device_update_status

Передачу критичних повідомлень, наприклад таких як про спрацювання датчика, забезпечує метод device_alarm, лістинг якого представлений на рис. 3.12.

```
case 'device_alarm':
      if( $context->method == "POST" &&
      Device::IsSessionValid(
            $context->post['token']
      )
      ) {
      $result = Device::Alarm(
            $context->post['device_id'],
            $context->post['object'],
            $context->post['status']
      )
      return RestUtil::ReturnJson( $result );
      } else {
      return RestUtil::ReturnError(400, 'Bad session');
      }
      break;
```

Рисунок 3.13 — Лістинг методу device_alarm

Метод mobile_auth, що належить класу Mobale, опрацьовує запити від додатків. Так передається ідентифікатор пристрою та його токен. Єдиною відмінністю від ідентифікації приймально-контрольного пристрою полягає в тому, пристрій надсилає сповіщення на сервер, а мобільний пристрій вже безпосередньо отримує до них доступ. Лістинг методу mobile_auth представлений на рис. 3.14.

```
// Mobile methods
case 'mobile_auth':
      if($context->method == "POST") {
      $sess_data = Mobile::CreateSession(
            $context->post['device_id'],
            $context->post['token']
      )
      return RestUtil::ReturnJson( $sess_data );
      } else {
      return RestUtil::ReturnError(400, 'Bad request');
      }
      break;
```

Рисунок 3.14 — Лістинг методу mobile_auth

Доступ мобільних пристроїв до серверної компоненти надає метод mobile_list_device, лістинг якого наведений на рис. 3.15. За допомогою цього методу отримується перелік пристроїв, що підключені до акаунту користувача. У результаті отримується можливість переглядати інформацію про їх стан.

```
case 'mobile_list_devices':
      if( Mobile::IsSessionValid(
      $context->post['token']
      ) ) {
      $result = Device::List(
            Mobile::GetUserID(),
      )
      return RestUtil::ReturnJson( $result );
      } else {
      return RestUtil::ReturnError(400, 'Bad session');
      }
      break;
```

Рисунок 3.15 — Лістинг методу mobile_list_device

Перевірити стан пристроїв у мобільному додатку дозволяють два методи. Перший з них є метод mobile_list_alarms, що надає можливість отримати інформацію про спрацювання датчиків. Лістинг цього методу наведений на рис. 3.16. Метод надає дані про усі останні події, які відбулися та на які потрібно реагувати. У результаті за ідентифікатором користувача з класу device створюється перелік усіх тривог, які призначені для конкретного користувача.

```
case 'mobile_list_alarms':
      if( Mobile::IsSessionValid(
      $context->post['token']
      ) ) {
      $result = Device::ListAlarms(
            Mobile::GetUserID(),
      )
      return RestUtil::ReturnJson( $result );
      } else {
      return RestUtil::ReturnError(400, 'Bad session');
      }
      break;
```

Рисунок 3.16 — Лістинг методу mobile_list_alarms

Другим методом є метод mobile_mute_alarms, лістинг якого представлений на рис. 3.17. Метод верифікує сесію і у результаті цього отримується ідентифікатор користувача та надається інформація про пристрій, що знаходиться в режимі тривога.

```
case 'mobile_mute_alarms':
      if( Mobile::IsSessionValid(
      $context->post['token']
      ) ) {
      $result = Device::MuteAlarm(
            Mobile::GetUserID(),
            $context->post['device_id'],
      )
      return RestUtil::ReturnJson( $result );
      } else {
      return RestUtil::ReturnError(400, 'Bad session');
      }
      break;
```

Рисунок 3.17 — Лістинг методу mobile_mute_alarms

4. РЕКОМЕНДАЦІЇ З ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ

4.1 Підготовка до роботи

Встановлення приймально-контрольного пристрою

Першим кроком розгортання запропонованої мікропроцесорної мультисенсорної системи безпеки є встановлення та налаштування мережевого підключення приймально-контрольного пристрою. У розглядуваній системі приймально-контрольний пристрій є головним елементом, що на сам перед забезпечує бездротовий зв’язок з охоронними датчиками. Фактично він виконує функції роутера, а тому при виборі місця його розташування потрібно дотримуватися таких правил. По-перше, краще розміщувати приймально-контрольний пристрій на однаковій відстані від усіх інших бездротових засобів системи, які будуть підключатися до нього. По-друге, слід вибирати найбільш високу точку для його розміщення. З одного боку це забезпечить менше фізичних перешкод на шляху у сигналу від підключених до нього пристроїв, а з іншого — захистить його від ненавмисного чи навмисного пошкодження, фізичного відключення від мережі живлення або комп’ютерної мережі.

Налаштування підключення до мережі Ethernet.

Далі необхідно підключити приймально-контрольний пристрій до мережі Ethernet, використовуючи багатожильний кабель з роз’ємом RJ45 на кінці. Також потрібно підключити пристрій, з якого задаватимуться налаштування приймально-контрольного пристрою, наприклад ноутбук. Це можна зробити і через бездротове WiFi з'єднанням, проте для первинного налаштування зручніше і надійніше використовувати кабель.

Після цього треба увімкнути приймально-контрольний пристрій. Для увімкнення потрібно вставити у відповідний порт на боковій панелі шнур блока живлення та підключити його розетки ~220 В. Блоком живлення є джерело постійної напруги +5 В з допустим вихідним струмом не менше 3 А, що надається у комплекті з приймально-контрольним пристроєм або аналогічний за

характеристиками. Після засвічування відповідної індикації здійснюється налаштування мережі.

Якщо налаштування здійснюється через бездротове з'єднання, у пристрої, з якого воно виконується, потрібно вибрати «Налаштування Wi-Fi-з’єднання». Якщо використовується ноутбук або персональний комп’ютер, на панелі завдань треба скористатися іконкою «Підключення». Натискання лівої клавіші миші на ній викликає спливаюче вікно, в якому будуть вказані всі доступні для підключення бездротові мережі. Серед них треба знайти те найменування, яке відповідає приймально-контрольному пристрою. Потім слід ввести пароль цієї мережі.

Налаштування доступу до Інтернет

Наступним кроком є налаштування приймально-контрольного пристрою для доступу до Інтернет. Налаштування підключення до Інтернет полягає у введенні значень параметрів, що відповідають інтернет-провайдеру. З використанням звичайного інтернет-браузеру потрібно увійти у панель управління пристроєм. Для цього в адресному рядку браузеру треба ввести IP-адрес приймально-контрольного пристрою: 192.168.0.1. На першій сторінці потрібно буде ввести логін та пароль, які зазначені у документації на пристрій. Далі потрібно вибрати тип підключення, що використовує інтернет-провайдер: динамічний IP (DHCP), статичний IP, PPPoE, L2TP, PPTP.

Налаштування Wi-Fi-мережі.

У панелі управління можна задати для Wi-Fi мережі нове ім'я і бажано змінити логін та пароль для доступу до мережі, встановлені за промовчанням. Це захистить від несанкціонованого підключення приймально-контрольного пристрою сторонніх осіб. Після введення нових даних треба натиснути кнопку «Зберегти». Також серед налаштувань можна задати параметри автентифікації. Рекомендується вибирати значення WPA/WPA2-Personal, шифрування – AES.

Підключення до хмарного середовища

Після налаштувань доступу до Інтернет та Wi-Fi-мережі необхідно

завантажити та встановити додатку на комп’ютер відділу охорони підприємства або установи, мобільний пристрій користувача у разі використання системи для контролю безпеки житла. Під час встановлення додатку треба слідувати рекомендаціям та підказкам. Після завершення установки необхідно запустити встановлений додаток. Під час першого запуску додатку потрібно створити обліковий запис, задати логін та пароль для входу.

Додавання обладнання системи безпеки до облікового запису.

Після створення облікового запису, що відповідатиме системі безпеки, що розгортається, можна приступити до додавання до нього обладнання, що буде використовуватися. Перш за все додається приймально-контрольний пристрій. Це наддасть можливість відділено контролювати стан дротових адресних та неадресних датчиків. У властивостях пристрою до нього треба додати контролери дротових датчиків, задаючи для кожного з них ім’я. Бажано вибирати такі імена, що однозначно визначатимуть контрольовані ними зони.

Якщо взаємодія приймально-контрольного пристрою з контролерами дротових датчиків буде відбуватися через мережу RS-485, крім імені контролера дротових датчиків треба задати ще їх адрес в цій мережі. Запис адресів у контролери відбувається натисканням кнопки «Застосувати». При цьому увімкненим має бути лише той контролер, для якого встановлюється адрес. По завершенню процедури додавання контролерів, яка виконується окремо для кожного з них, усі контролери вмикаються. При успішній операції додавання вони мають стати активними у додатку.

На наступному кроці до системи додаються використовувані датчики. При додаванні бездротових Wi-Fi та Z-Wave датчиків слід дотримуватися інструкції до них. При успішному завершенні процедури додавання бездротового датчика він має з’явитися у додатку.

Додавання дротових датчиків відбувається на закладці властивостей відповідного контролера. Для кожного адресного бездротового датчика, що

додається, задається його ім’я та адрес. Для неадресних датчиків вказується лише ім’я та номер шлейфа, до якого вони підключені.

По завершенню необхідно перевірити працездатність кожного елемента системи. На сам перед це стосується взаємодії з дротовими датчиками, оскільки усі компоненти системи, що підключаються через бездротове з’єднання, у випадку несправності не будуть видимими у додатку.

4.2 Рекомендації з монтажу

Розгортання системи безпеки розпочинається з встановлення приймально-контрольного пристрою. Як було зазначено у підрозділі 4.1 приймально контрольний пристрій повинен розміщуватися на однаковій відстані до 50 м від усіх інших бездротових засобі, які будуть підключатися до нього, та у найбільш високій точці. До одного приймально-контрольного пристрою може бути підключено до 64 Wi-Fi та до 232 Z-Wave пристроїв.

При більших відстанях або при використанні дротових датчиків замість бездротових як доповнення до приймально-контрольного пристрою використовуються контролери дротових датчиків. При використанні дротового каналу зв’язку RS-485 до одного приймально-контрольного пристрою може бути підключено до 32-ох контролерів.

Контролери дротових датчиків дозволяють організувати контроль безпеки по окремим зонам, що охоплюють кілька кімнат, та знизити вартість системи за рахунок використання дротових датчиків. Для надійного захисту приміщень від несанкціонованого проникнення, кожна зона можливого проникнення (двері та вікна) повинна контролюватися датчиком відкриття. Крім того, цілісність віконного скління повинна контролюватися датчиками розбиття скла. Нарешті, додатковий захист приміщень може забезпечуватися датчиками руху.

Кількість використовуваних датчиків розбиття скла та датчиків руху, їх розташування визначаються з врахуванням геометричних та конструктивних

особливостей приміщення, рекомендацій до встановлення датчиків, що наведених в інструкція до них.

Найчастіше подібні датчики встановлюються так, щоб сенсор охоплював район вхідних дверей та віконного отвору за мінімальної кількості «сліпих зон». Місце встановлення залежить від конструкції. Розрізняють такі типи датчиків:

— настінні (робоча зона — 180 °);

— кутові (90 °);

— стельові (360 °).

Настінні моделі монтують по центру бокової стіни, між дверима та віконним отвором при висоті розміщення не вище 2,5 м. Кутові монтуються в кутку, з протилежного боку від вікна. Висота розміщення зазвичай 2,5 м. Стельові модифікації розміщуються ближче до дверей, щоб звести до мінімуму випадки хибних спрацьовувань внаслідок руху об'єктів за вікном.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Комерційний та технологічний аудит науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному випадку мікрпроцесорної мультисенсорної системи безпеки. Метою дослідження є вдосконалення системи безпеки.

Особливістю програмної частини розробки є зменшення кількості використовуваних для її побудови блоків.

Аналогом розробки може бути комплект сигналізації ATIS Kit 200T за ціною 1650 грн.

Для проведення комерційного та технологічного аудиту залучають не менше 3-х незалежних експертів. Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням п’ятибальної системи оцінювання за 12-ма критеріями, у відповідності із табл. 5.1.

Таблиця 5.1 — Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздат-ність продукту в реальних умовах
2	Багато аналогів на малому ринку	Ринкові п Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку

Продовження табл. 5.1

Ринкові переваги					
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною .	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так із комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві

Продовження табл. 5.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в таблиці 5.2

Таблиця 5.2 — Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	4	4	4
Наявність аналогів на ринку	3	4	4
Цінова політика	4	4	4
Технічні та споживчі властивості виробу	4	4	4
Експлуатаційні витрати	4	4	3
Ринок збуту	3	4	4
Конкурентоспроможність	4	4	3
Фахівці з технічної і комерційної реалізації	4	4	4
Фінансування	4	3	4
Матеріально-технічна база	3	3	4
Термін реалізації ідеї	4	4	4
Супровідна документація	3	3	4
Сума	44	45	46
Середньоарифметична сума балів	(44+45+46) / 3 = 45		

За даними таблиці 5.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці 4.3.

Таблиця 5.3 — Рівні комерційного потенціалу розробки

Середньоарифметична сума балів СБ , розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового програмного продукту є високим, що досягається за рахунок зменшення кількості використовуваних для її побудови блоків. Необхідність розробки обумовлена необхідністю постійного вдосконаленням методів і засобів забезпечення безпеки різних об'єктів, рівень якої визначається ймовірністю збереження захисту об’єкта при різному виді загроз.

5.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи

Розраховуємо витрати на заробітну плату.

Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t, \qquad (5.1)$$

де М — місячний посадовий оклад конкретного розробника (дослідника), грн.;

$T_р$ — число робочих днів за місяць, 20 днів;

t — число днів роботи розробника (дослідника).

Результати розрахунків зведемо до таблиці 5.4.

Таблиця 5.4 — Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	28000	1217,39	30	36521,739
Інженер	25000	1086,96	30	32608,696
Всього				69130,43

Так як в даному випадку розробляється програмний продукт, то розробник виступає одночасно і основним робітником, і тестувальником розроблюваного програмного продукту.

Додаткова заробітна плата розробників, які приймали участь в розробці обладнання, прийнято розраховувати як 10 % від основної заробітної плати розробників та робітників:

$$З_д = З_о \cdot 10\ \% / 100\ \% \quad (5.2)$$

$$З_д = (69130,43 \cdot 10\ \% / 100\ \%) = 6913,04 \ \text{(грн.)}$$

Визначаємо нарахування на заробітну плату розробників. Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_о + З_д) \cdot 22\ \% / 100\% \quad (5.3)$$

$$Н_з = (69130,43 + 6913,04) \cdot 22\ \% / 100\ \% = 16729,57 \ \text{(грн.)}$$

Визначаємо витрати на комплектуючі. Оскільки для апаратної частини розроблювального пристрою було потрібно комплектуючі:

—модуль Raspberry Pi 3 Model B+ - 2150 грн, 1 шт;

—модуль Razberry 2 Z-Wave – 2100 грн, 1 шт;

—мікросхема PCA9515 – 54 грн, 2 шт;

—перетворювачі UART TTL в RS-485 – 38 грн, 1 шт;

—релейний модуль Arduino Relay Module 1 relay 5V – 27 грн, 1 шт.

Витрати на них занесемо в повному обсязі в вартість розробки, включаючи транспортні витрати в розмірі 10%:

$$В = (2150 + 2100 + 108 + 38 + 27)*1,1 = 4865,30 \text{ грн.}$$

Розраховуємо амортизаційні витрати на обладнання, яке використовувалось для проведення розробки. Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді амортизація обладнання, що використовувалась для розробки розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \quad (5.4)$$

де Ц — балансова вартість обладнання, грн.;

Т — термін корисного використання обладнання згідно податкового законодавства, років;

$t_{вик}$ — термін використання під час розробки, місяців.

Розрахуємо, для прикладу, амортизаційні витрати на комп’ютер балансова вартість якого становить 20000 грн., термін його корисного використання згідно податкового законодавства – 2 роки, а термін його фактичного використання – 1,30 міс.

$$A_{обл} = \frac{20000}{2} \times \frac{1,3}{12} = 1086,957 \text{ грн.}$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до таблиці 5.5.

Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників (енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1-й або 2-й клас).

Таблиця 5.5 — Амортизаційні відрахування матеріальних і нематеріальних ресурсів для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна переферія	20000	2	1,30	1086,957
Офісне обладнення	25000	4	2,00	1041,667
Приміщення	800000	20	1,30	4347,826
Ліцензійна ОС, та спеціалізовані ліцензійні нематеріальні ресурси (вартість менше 20000 грн - сума включається повністю))	надано безкоштовно	-	-	0,000
Всього				5978,26

Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \quad (5.6)$$

де В — вартість 1 кВт-години електроенергії для 1 класу підприємства, В = 6,2 грн./кВт;

П — встановлена потужність обладнання, кВт. П = 0,4 кВт;

Ф — фактична кількість годин роботи обладнання, годин.

$К_п$ — коефіцієнт використання потужності, $К_п$ = 0,9.

$$В_е = 0,9 \cdot 0,35 \cdot 8 \cdot 30 \cdot 2,01 = 151,956 \text{ (грн.)}$$

Визначаємо інші витрати та загальновиробничі витрати. До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як

50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.7)$$

де $Н_{ів}$ — норма нарахування за статтею «Інші витрати».

$$I_в = 69130,43 * 50\% / 100\% = 34565,22 \text{ (грн.)}$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.8)$$

де $Н_{нзв}$ — норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$Н_{нзв} = 69130,43 * 100\ \% / 100\ \% = 69130 \text{ (грн.)}$$

Розраховуємо витрати на проведення науково-дослідної роботи як суму всіх попередніх статей витрат:

$$В_{заг} = 69130,43+6913,04+16729,57+4865,30+5978,26+151,96+34565,22+$$

$$+69130 = 207464,21 \text{ грн.}$$

Розраховуємо загальні витрати на науково-дослідну (науково-технічну) роботу та оформлення її результатів. Загальні витрати на завершення науково-

дослідної (науково-технічної) роботи та оформлення її результатів розраховуються *ЗВ*, визначається за формулою:

$$ЗВ = \frac{B_{заг}}{\eta} \text{ (грн)}, \quad (5.9)$$

де η — коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Так, якщо науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

$$ЗВ = 207464,21 / 0,5 = 414928 \text{ грн.}$$

5.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

В ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розробки необхідно:

— вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

— зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3-х років після її впровадження);

— кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основних суб'єктів (зацікавлених осіб) цього попиту;

— визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов'язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

— абсолютного економічного ефекту (чистого дисконтованого доходу);

— внутрішньої економічної дохідності (внутрішньої норми дохідності);

— терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором можна об'єднати, враховуючи визначені ситуації з відповідними умовами.

Економічний ефект від вдосконалення програмного засобу для використання масовим споживачем буде формуватися на основі таких даних:

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \qquad (5.10)$$

де $\pm\Delta Ц_o$ — зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

N — кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки;

$Ц_о$ — основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_о = Ц_б \pm \Delta Ц_о$;

Цб — вартість програмного продукту у році до впровадження результатів розробки;

ΔN — збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ — коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$.

p — коефіцієнт, який враховує рентабельність продукту;

ϑ — ставка податку на прибуток, у 2023 році ϑ =18%.

Припустимо, що при прогнозованій ціні 950 грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти її ціну на *50* грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року – на 9000 шт., протягом другого року – на 10000 шт., протягом третього року на 11000 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

$$\Delta П_1 = (0*50 + (950 + 50)*9000)* 0{,}8333* 0{,}35) * (1 - 0{,}18) = 2044874{,}918 \text{ грн.}$$

$$\Delta П_2 = (0*50 + (950 + 50)*(9000+10000)* 0{,}8333* 0{,}35) * (1 - 0{,}18) = 4544166{,}485 \text{ грн.}$$

$$\Delta П_3 = (0*50 + (950 + 50)*(9000+10000+11000)* 0{,}8333* 0{,}35) * (1 - 0{,}18) = 7174999{,}713 \text{ грн.}$$

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 13764041,12 грн.

Розраховуємо приведену вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (5.11)$$

де $\Delta П_i$ — збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т — період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ — ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ = 0,05…0,15;

t — період часу (в роках).

Збільшення прибутку ми отримаємо починаючи з першого року:

$$ПП= (2044874,918/(1+0,1)^1)+(4544166,485/(1+0,1)^2)+(7174999,713/$$
$$/(1+0,1)^3) = 1858977,20 + 3755509,49 + 5390683,48 = 11005170,17 \text{ грн.}$$

Далі розраховують величину початкових інвестицій *PV*, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (5.12)$$

де $k_{інв}$ — коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;

ЗВ — загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 2 * 414928 = 829856{,}85 \text{ грн.}$$

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід *(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \tag{5.13}$$

$$E_{абс} = 11005170{,}17 - 829856{,}85 = 10175313{,}32 \text{ грн.}$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність або показник внутрішньої но-рми дохідності *(IRR, Internal Rate of Return)* вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{5.14}$$

де $Т_ж$ — життєвий цикл наукової розробки, роки.

$$E_в = \sqrt{\text{з}\ (1 + 10175313{,}32/829856{,}85\ - 1 = 1{,}367}$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{5.15}$$

де d — середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d = (0,09…0,14);

f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{\min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{5.16}$$

$$T_{ок} = 1 / 1{,}367 = 0{,}73 \text{ р.}$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 0,73 роки, то фінансування даної наукової розробки є доцільним.

У даному розділі проведено розрахунок витрат на розробку нового програмного продукту, сума яких складає 414928 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення, розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений програмний продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,73 роки.

ВИСНОВКИ

Аналіз сучасних технологій забезпечення безпеки показав, що надійний захист вимагає застосування в одній системі різних типів датчиків. При цьому для отримання системи, яка відповідала би сучасним тенденціям у сфері безпеки, необхідно передбачити в ній можливість інтеграції з хмарними рішеннями.

Серед бездротових технологій передачі даних найменш чутливою до завад та найбільш надійною з точки зору забезпечення зв’язку між окремими вузлами мережі є технологія Z-Wave. Поряд із цим значний сегмент бездротових датчиків підтримує технологію Wi-Fi.

Не зважаючи на популяризацію бездротових технологій, більш дешевими та більш різноманітними залишаються дротові датчики. З врахуванням цього запропоновано архітектуру системи, що може бути реалізована на основі лише двох типів модулів, підтримує можливість підключення як дротових, так і бездротових датчиків та дозволяє використовувати хмарні середовища для віддаленого контролю.

В роботі розроблено структурні та функціональні схеми приймально-контрольного пристрою, що є головним модулем системи, забезпечуючи зв’язок усіх її компонентів з хмарним сервером, та контролера дротових датчиків, що надає можливість збільшити зону контролю та виявляти більшу кількість загроз. Дані пристрої будуються на основі готових модулів, що мінімізує перелік потрібної елементної бази та спрощує їх реалізацію.

Оцінка комерційного потенціалу розробки показала економічну доцільність її впровадження, термін окупності витрат складатиме 0,73 роки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Тренди у сфері безпеки у воєнних реаліях 2022 року [Електронний ресурс]. Режим доступу: https://www.bezpeka-shop.com/ua/blog/obzor/trendy-v-sfere-bezopasnosti-v-voennykh-realiyakh-2022-goda/

2. Стайкуца С. В. Щодо використання систем охоронної сигналізації / С. В. Стайкуца, В. Й. Кільдішев, Є. В. Карнаухий. // Молодий вчений. – 2022. – С. 46–50.

3. Груба І.І. Система охоронної сигналізації технічні засоби виявлення. Харків: Солон прес. Україна, 2011. 220с.

4. Системи пожежної та охоронної сигналізації : навч. посіб. / Кушнір А.П., Чалий Д.О. Львів : СПОЛОМ, 2022. 298 с.

5. Види охоронної сигналізації [Електронний ресурс]. Режим доступу: https://sg-ukraine.com.ua/news/vidy-ohrannoj-signalizacii/

6. Види охоронної сигналізації та принцип їх роботи [Електронний ресурс]. Режим доступу: https://klaster.ua/ua/stati-i-obzory/vidy-okhrannoi-signalizacii-i-princip-ikh-raboty/

7. Передумови застосування технологій IoT в сфері охоронних систем та відеоспостереження / Коренівська О.Л., Коротун О.В., Нікітчук Т.М., Андреєв О.В. / Тези V ВНТК «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 01–02 грудня 2022 р. – Житомир: Житомирська політехніка, 2022, С. 285-286.

8. Інтернет речей та сектор охоронної сигналізації [Електронний ресурс]. Режим доступу: https://worldvision.com.ua/internet-veshchey-i-sektor-okhrannoy-signalizatsii/

9. Як працює датчик відкриття дверей: що таке геркон та який принцип його роботи. [Електронний ресурс]. Режим доступу: https://ohrana.ua/uk/stati-i-obzory/kak-rabotaet-datcik-otkrytiya-dveri-cto-takoe-gerkon-i-princip-ego-raboty.html

10. Герконові датчики відкриття дверей. [Електронний ресурс]. Режим

доступу: https://www.bezpeka-shop.com/ua/catalog/datchiki_otkrytiya_gerkony/

11. Датчики розбиття скла. [Електронний ресурс]. Режим доступу: https://ukrbezpeka.com/shop/datchiki_razbitija/

12. Wireless glass break sensor. Ajax GlassProtect [Електронний ресурс]. Режим доступу: https://svn.kiev.ua/besprovodnoy-datchik-razbitiya-stekla-ajax-glassprotect-belyy/

13. Трембач Р.Б. Сейсмічний сенсор охоронної сигналізаці / Р.Б. Трембач, Р.М. Хльовпик // Матеріали VII Міжнародної науково-технічної конференції молодих учених та студентів. Актуальні задачі сучасних технологій, Тернопіль, 28-29 листопада 2018, С. 177-178.

14. Геофонні системи. [Електронний ресурс]. Режим доступу: https://kazedu.com/referat/159767/6

15. Принцип дії датчику руху. [Електронний ресурс]. Режим доступу: https://watt-shop.com/ua/blog/173-printsip-diji-datchiku-rukhu.html.

16. Христич В. В. та ін. Системи пожежної та охоронної сигналізації. – Харків: Академія пожежної безпеки України, 2008, 87 с.

17. Ємнісні датчики. . [Електронний ресурс]. Режим доступу: http://vozom.org.ua/index.php/elementna-baza-a-i-t/datchyky?showall=&start=1

18. Пасивні і активні датчики руху: що це і як працює? [Електронний ресурс]. Режим доступу: https://klaster.ua/ua/stati-i-obzory/ohrana-perimetra/passivnye-i-aktivnye-datchiki-dvizheniya-chto-eto-i-kak-rabotaet/

19. Погребенник В . Д. Ультразвукові сенсори системи охоронної сигналізації / В . Д. Погребенник, Р . В. Політило // Вісник НТУУ “КПІ”. Серія ПРИЛАДОБУДУВАННЯ, 2008, Вип. 3, С. 68 – 76.

20. Мікрохвильовий датчик руху: принцип дії, переваги та особливості. [Електронний ресурс]. Режим доступу: https://epicentrk.ua/ua/articles/mikrovolnovyy-datchik-dvizheniya-printsip-deystviya-preimushchestva-i-osobennosti.html

21. Професійна охоронна система. [Електронний ресурс]. Режим доступу:

https://tiras.technology/orion_nova/

22. GSM Сигналізація KERUI G18. [Електронний ресурс]. Режим доступу: https://kerui.com.ua/gsm-signalizaciya-kerui-kr-g18-belaya

23. Комплект беспроводной Wi-Fi сигнализации ATIS Kit 200T. [Електронний ресурс]. Режим доступу: https://www.bezpeka-shop.com/product/komplekt-besprovodnoy-wi-fi-signalizatsii-atis-kit-200t/

24. Розумний будинок Tuya Smart. [Електронний ресурс]. Режим доступу: https://www.bezpeka-shop.com/ua/blog/poleznye-sovety/umnyy-dom-tuya-smart/

25. Z-Wave vs ZigBee, WiFi, Thread, Bluetooth BLE: выбираем протокол управления умным домом. [Електронний ресурс]. Режим доступу: https://superhome.pro/z-wave-vs-zigbee-wifi-thread-bluetooth-ble-vybiraem-protokol-upravleniya-umnym-domom/.

26. Основи побудови мережі Z-Wave. [Електронний ресурс]. Режим доступу: https://superhome.pro/osnovy-postroeniia-seti-z-wave/.

27. Raspberry Pi в Києві [Електронний ресурс]. Режим доступу: https://raspberry.com.ua/p/adafruit-itsybitsy-m0-express-for-circuitpython-arduino-ide-2/

28. Z-Wave.Me RaZberry 7 Pro - Z-Wave Plug-On Module for Raspberry Pi. [Електронний ресурс]. Режим доступу: https://www.amazon.com/Z-Wave-Me-RaZberry-Pro-Plug-Compatible/dp/B09DCR4RSX.

29. Модуль RS485 TTL, MAX485, , Arduino. [Електронний ресурс]. Режим доступу: https://uawest.com/modul-rs485-ttl-max485-preobrazovatel-arduino.html.

30. GSM GPRS модуль бездротового зв'язку, дистанційного управління SIM800L. [Електронний ресурс]. Режим доступу: https://sxema.com.ua/p801665400-gsm-gprs-modul.html.

31. Arduino Relay Module 1 relay 5V. [Електронний ресурс]. Режим доступу: http://www.kosmodrom.com.ua/el.php?name=RelayModule1relay5V.

32. Плата Z-Uno 2 Z-Wave для Arduino - ZMEEZUNO2. [Електронний ресурс]. Режим доступу: https://z-wave.com.ua/ua/p332641492-plata-uno-

wave.html.

33. Аналогові та аналого-цифрові пристрої : електронний конспект лекцій комбінованого (локального та мережного) використання. [Електронний ресурс] / М. Г. Тарновський, Л. В. Крупельницький. – Вінниця : ВНТУ, 2022. – 88 с.

34. LM741 Operational Amplifier. [Електронний ресурс]. Режим доступу: https://www.ti.com/lit/ds/symlink/lm741.pdf.

35. PCA9515 I 2C-bus repeater. [Електронний ресурс]. Режим доступу: https://www.nxp.com/docs/en/data-sheet/PCA9515.pdf.

ДОДАТОК А

Технічне завдання

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

проф., д.т.н.. Азаров О.Д.

_____

" ____ " _____ 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

"Мікропроцесорна мультисенсорна система безпеки"

08-54.МКР.048.00.000 ПЗ

Керівник роботи к.т.н. доц. каф. ОТ

_____ Тарновський М. Г

Студент групи 2КІ–22м

_____ Ярошевський М.М.

ВНТУ 2023

1 Підстава для виконання магістерської кваліфікаційної роботи (МКР)

1.1 Актуальність роботи обумовлена необхідністю постійного вдосконаленням методів і засобів забезпечення безпеки різних об'єктів, рівень якої визначається ймовірністю збереження захисту об’єкта при різному виді загроз.

1.2 Наказ про затвердження теми МКР.

2 Мета МКР і призначення розробки

2.1 Мета роботи — вдосконалення системи безпеки за рахунок функціональної оптимізації основних її компонентів, що дозволяє скоротити їх кількість.

2.2 Призначення розробки — створення мікропроцесорних засобів для контролю стану дротових та бездротових датчиків виявлення несанкціонованого проникнення.

3 Вихідні дані для виконання МКР

3.1 Призначення системи — виявлення ознак несанкціонованого проникнення.

3.2 Використовувані датчики — дротові та бездротові різного типу.

3.3 Організація — інтеграція з хмарними сервісами.

3.4 Архітектура — розподілена з можливістю легкого масштабування.

4 Вимоги до виконання МКР

4.1 Провести сучасних технологій забезпечення безпеки;

4.2 Визначити архітектуру мікропроцесорної мультисенсорної системи безпеки;

4.3 Розробити апаратно-програмні засоби системи безпеки;

4.4 Оцінити комерційний потенціал розробки.

5 Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз існуючих технологій, огляд аналогів системи.	19.09.2023	15.10.2023	Вступ, Розділ 1
2	Визначення архітектури розподіленої системи	16.10.2023	29.10.2023	Розділ 2
3	Розробка структурної та функціональної схем приймально-контрольного пристрою	30.10.2023	7.11.2023	Розділ 3
4	Розробка структурної та функціональної схем контролера дротових датчиків	8.11.2023	19.11.2023	Розділ 3
5	Розробка рекомендацій з введення в експлуатацію	20.11.2023	26.11.2023	Розділ 4
6	Підготовка економічної частини	27.11.2023	3.12.2023	Розділ 5
7	Оформлення пояснювальної записки, графічного матеріалу і презентації	4.12.2023	10.12.2023	ПЗ, графічний матеріал і презентація
8	Підготовка і підпис супроводжуючих документів, нормоконтроль та тест на плагіат	11.02.2023	15.02.2023	Оформленні документи

6 Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами.

7 Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання МКР

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104–2006 «Єдина система конструкторської документації. Основні написи»;

— методичні вказівки до виконання магістерських кваліфікаційних робіт зі спеціальності 123 — «Комп’ютерна інженерія»;

— документи на які посилаються у вище вказаних.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ–03.02.02 П.001.01:21

ДОДАТОК Б

Архітектура мікропроцесорної системи безпеки

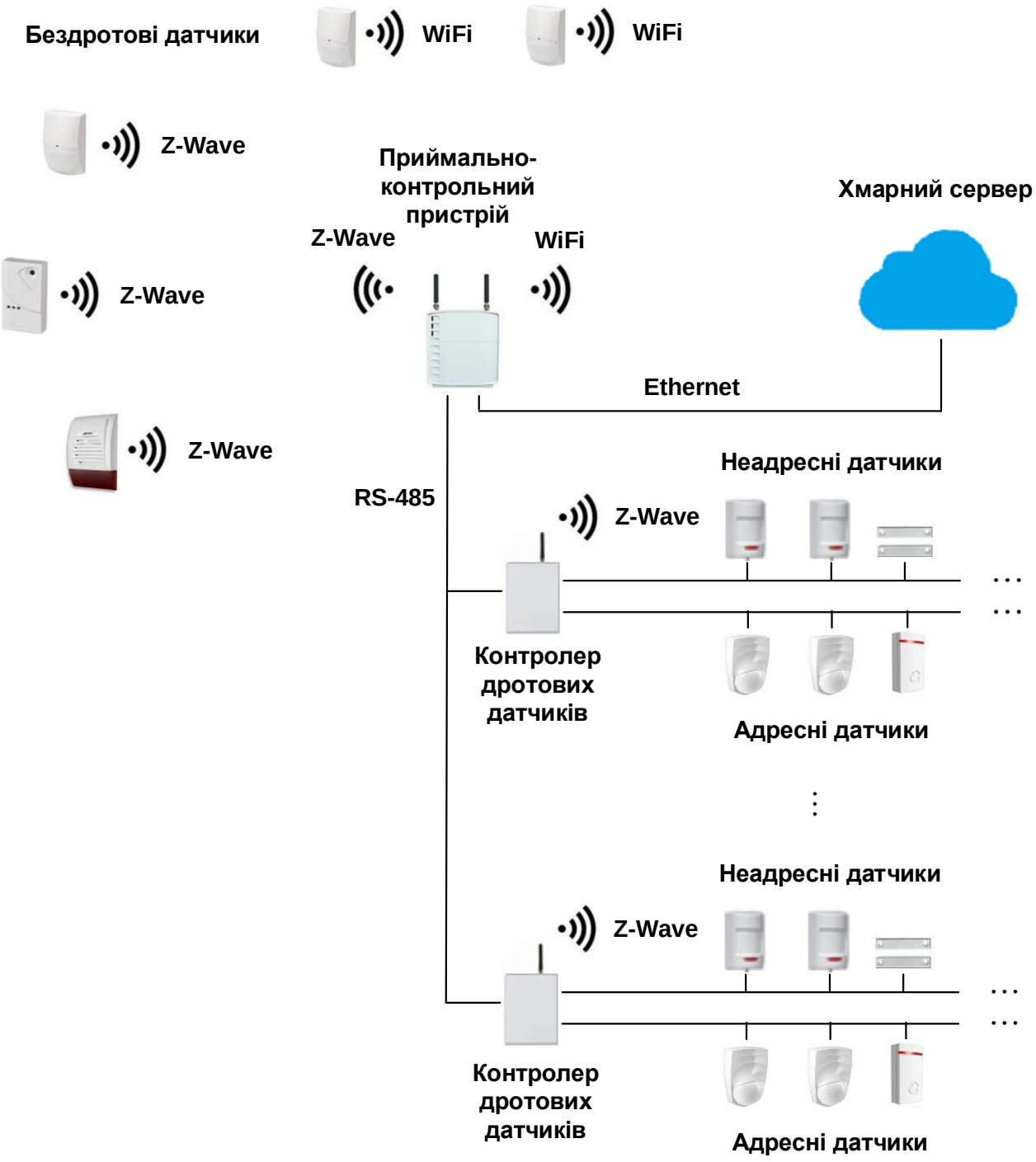

Рисунок Б.1 — Архітектура мікропроцесорної системи безпеки

ДОДАТОК В

Структурна схема приймально-контрольного пристрою

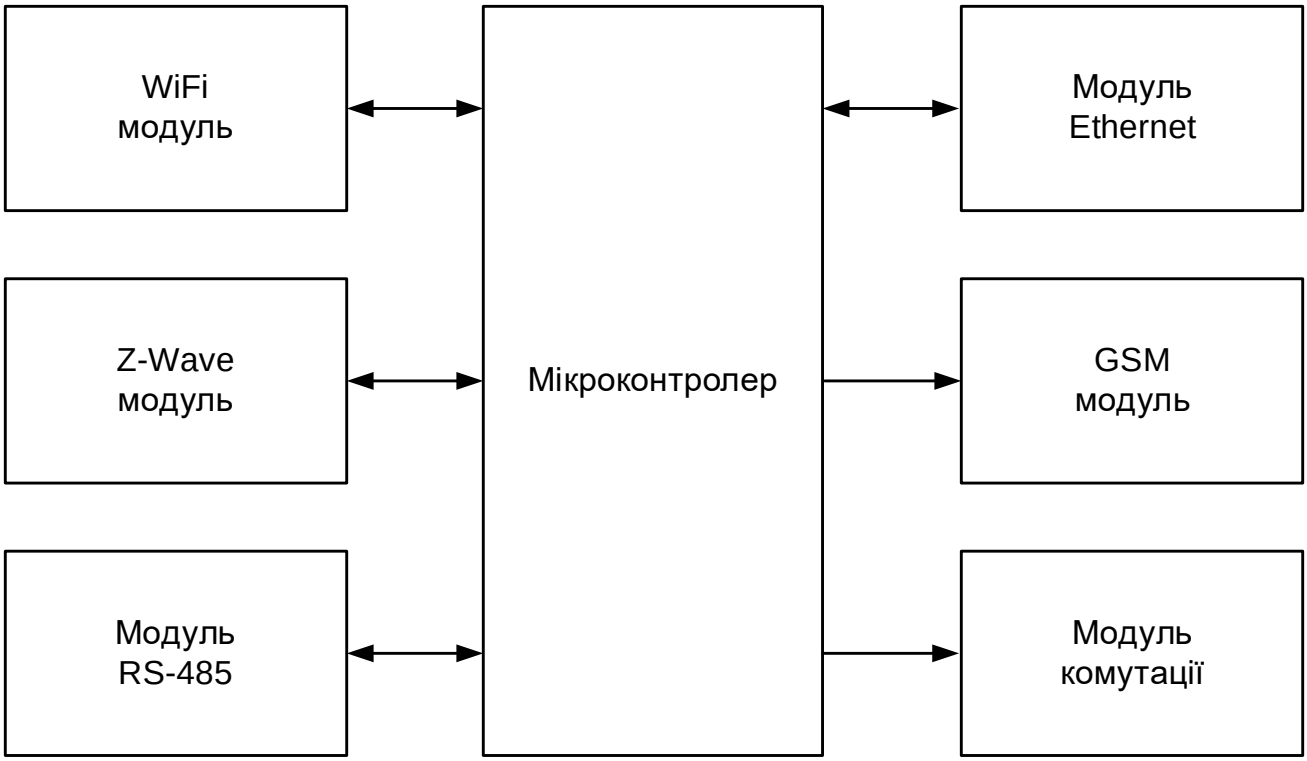

Рисунок В.1 — Структурна схема приймально-контрольного пристрою

ДОДАТОК Г

Функціональна схема приймально-контрольного пристрою

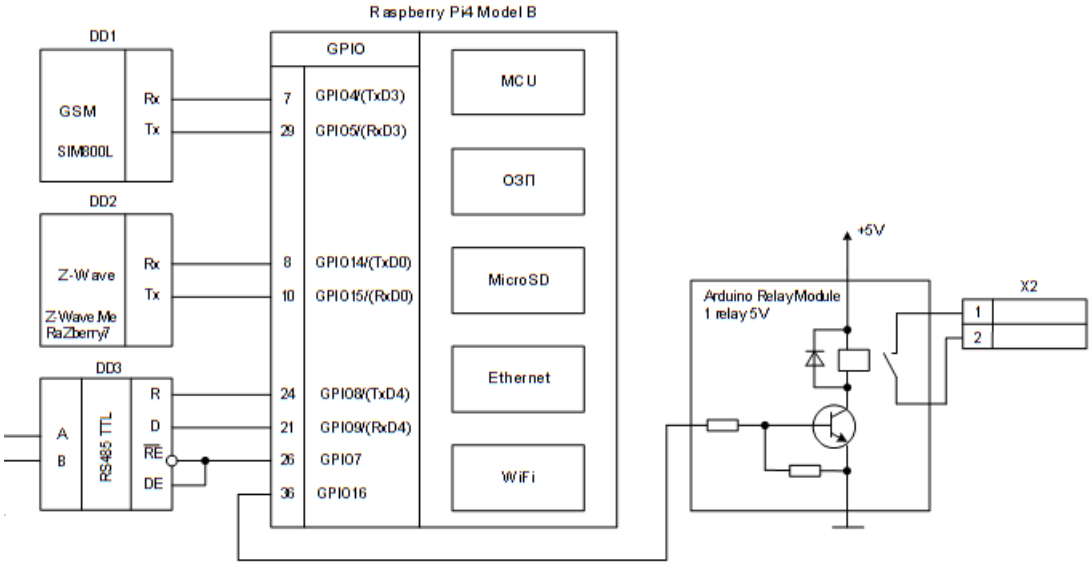

Рисунок Г.1 — Функціональна схема приймально-контрольного пристрою

ДОДАТОК Д

Структурна схема контролера дротових датчиків

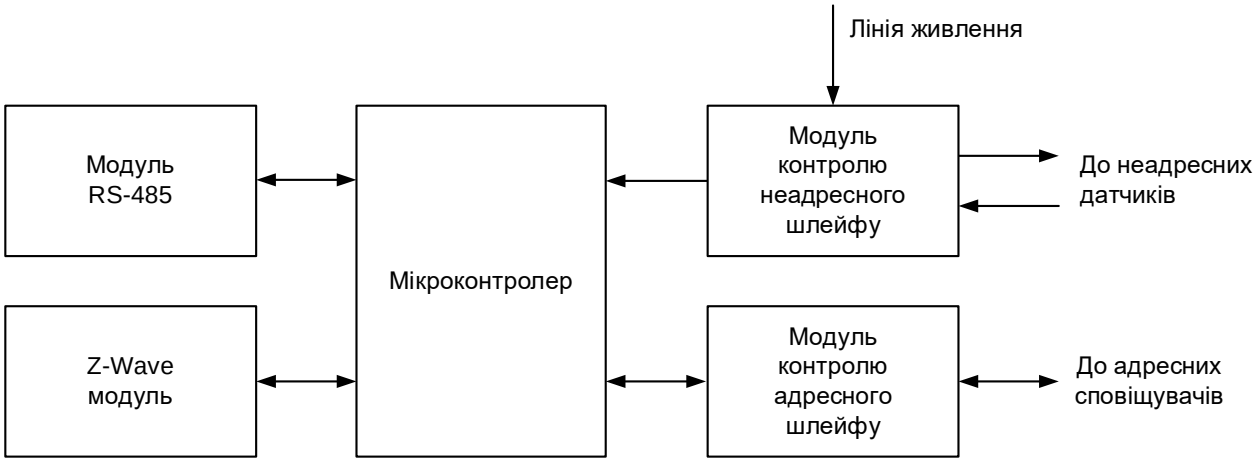

Рисунок Д.1 — Структурна схема контролера дротових датчиків

ДОДАТОК Е

Функціональна схема контролера дротових датчиків

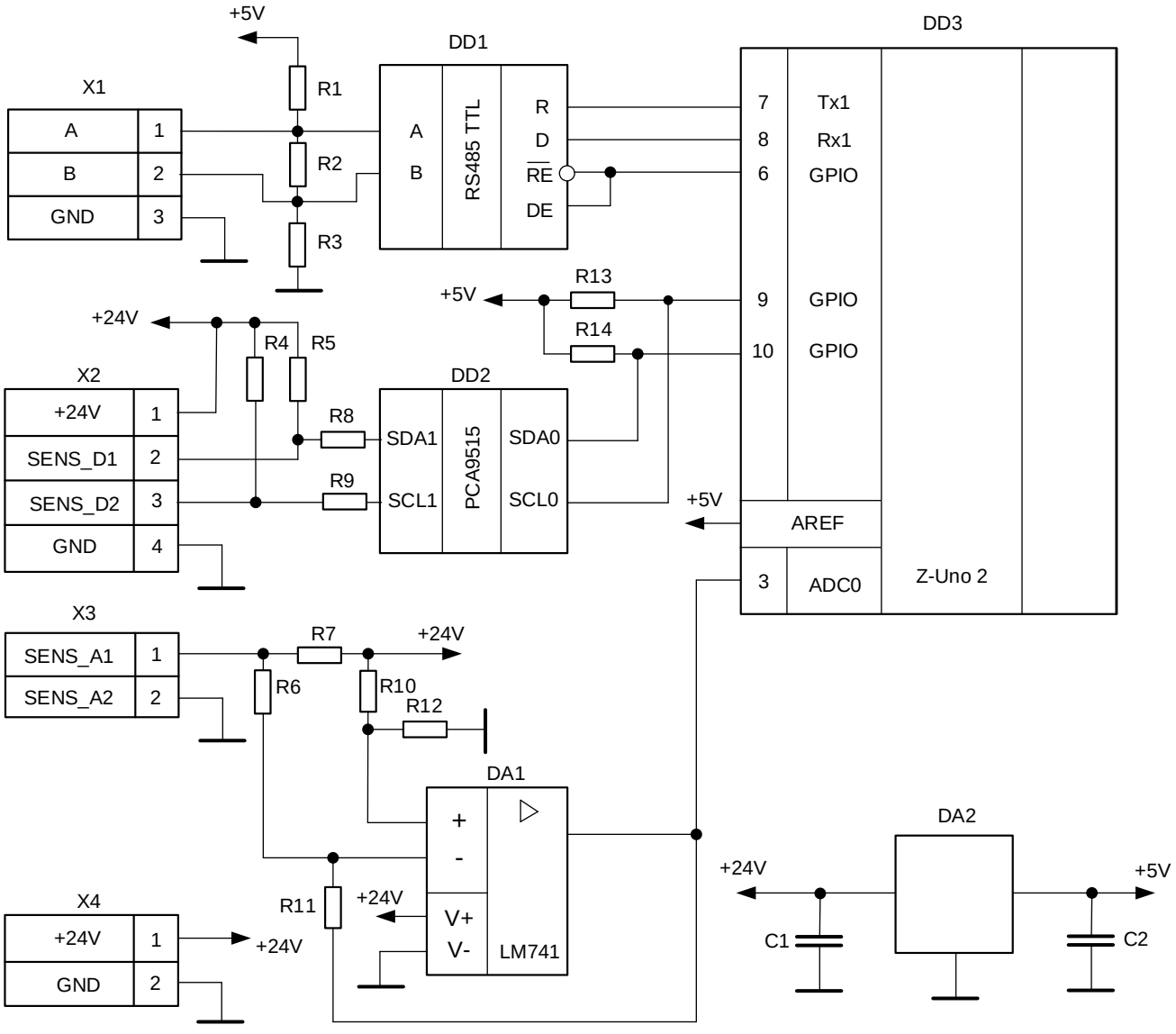

Рисунок Е.1 — Функціональна схема контролера дротових датчиків

ДОДАТОК Ж

Лістинг файл API.PHP

```
use RestBox\RestUtil;
require __DIR__ . '/vendor/autoload.php';
require __DIR__ . '/api/device.php';
require __DIR__ . '/api/mobile.php';
require __DIR__ . '/api/telegram.php';
function API_Router($context) {
switch ($context->get['metod']) {
    // Device methods
    case 'device_auth':
        if($context->method == "POST") {
            $sess_data = Device::CreateSession(
                $context->post['device_id'],
                $context->post['token']
            return RestUtil::ReturnJson( $sess_data );
        } else {
            return RestUtil::ReturnError(400, 'Bad request');
        }
        break;
    case 'device_update_status':
        if( $context->method == "POST" &&
            Device::IsSessionValid(
                $context->post['token']
         {
            $result = Device::SetStatus(
                $context->post['device_id'],
                $context->post['token']
            return RestUtil::ReturnJson( $result );
        } else {
            return RestUtil::ReturnError(400, 'Bad session');
        }
        break;
    case 'device_alarm':
        if( $context->method == "POST" &&
            Device::IsSessionValid(
                $context->post['token']
            )
        ) {
            $result = Device::Alarm(
                $context->post['device_id'],
                $context->post['object'],
                $context->post['status']
            )
            return RestUtil::ReturnJson( $result );
        } else {
            return RestUtil::ReturnError(400, 'Bad session');
        }
```

```
    break;
// Mobile methods
case 'mobile_auth':
    if($context->method == "POST") {
        $sess_data = Mobile::CreateSession(
            $context->post['device_id'],
            $context->post['token']
        )
        return RestUtil::ReturnJson( $sess_data );
    } else {
        return RestUtil::ReturnError(400, 'Bad request');
    }
    break;
case 'mobile_list_devices':
    if( Mobile::IsSessionValid(
        $context->post['token']
    ) ) {
        $result = Device::List(
            Mobile::GetUserID(),
        )
        return RestUtil::ReturnJson( $result );
    } else {
        return RestUtil::ReturnError(400, 'Bad session');
    }
    break;
case 'mobile_list_alarms':
    if( Mobile::IsSessionValid(
        $context->post['token']
    ) ) {
        $result = Device::ListAlarms(
            Mobile::GetUserID(),
        )
        return RestUtil::ReturnJson( $result );
    } else {
        return RestUtil::ReturnError(400, 'Bad session');
    }
    break;
case 'mobile_mute_alarms':
    if( Mobile::IsSessionValid(
        $context->post['token']
    ) ) {
        $result = Device::MuteAlarm(
            Mobile::GetUserID(),
            $context->post['device_id'],
        )
        return RestUtil::ReturnJson( $result );
    } else {
        return RestUtil::ReturnError(400, 'Bad session');
    }
    break;
// Telegram bot
```

```
    case 'mess_auth':
        if($context->method == "POST") {
            $sess_data = Telegram::CreateSession(
                $context->post['device_id'],
                $context->post['token']
            )
            return RestUtil::ReturnJson( $sess_data );
        } else {
            return RestUtil::ReturnError(400, 'Bad request');
        }
        break;
    case 'mess_list_devices':
        if( Telegram::IsSessionValid(
            $context->post['token']
        ) ) {
            $result = Device::List(
                Telegram::GetUserID(),
            )
            return RestUtil::ReturnJson( $result );
        } else {
                return RestUtil::ReturnError(400, 'Bad session');
        }
        break;
    case 'mess_list_alarms':
        if( Telegram::IsSessionValid(
            $context->post['token']
        ) ) {
            $result = Device::ListAlarms(
                Telegram::GetUserID(),
                true
            )
            return RestUtil::ReturnJson( $result );
        } else {
            return RestUtil::ReturnError(400, 'Bad session');
        }
        break;
    // Default mode
    default:
        http_response_code(404);
        RestUtil::ReturnError(404, 'Not found');
        die();
}
}
$application = new RestUtil('API_Router');
$application->Render();
```

ДОДАТОК К

ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: «Мікропроцесорна мультисенсорна система безпеки»

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра обчислювальної техніки

Показники звіту подібності Unicheck

Оригінальність 90.7 % Схожість 9.3 %

Аналіз звіту подібності (відмітити потрібне):

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- □ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
- □ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Ярошевський М. М.

Керівник роботи _____ Тарновський М.Г.