МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

«До захисту допущено»
Завідувач кафедри ЕКТ

_____ Анатолій ОПАНАСЮК
(підпис) (Ім'я та ПРІЗВИЩЕ)
____ _____ 2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня «магістр»

зі спеціальності 171 «Електроніка»

освітньо-професійної програми «Електронні системи та компоненти»

на тему:

ЕЛЕКТРОННА ОХОРОННА СИСТЕМА РОЗУМНИЙ ДІМ

Здобувача групи ЕС.мз-21 Шкирдань Владислав Сергійович

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ _____
(підпис) (Ім'я та ПРІЗВИЩЕ)

Керівник, Гриненко Віталій Вікторович _____
(підпис)

Консультант з техніко-економічної частини,
доцент, к.е.н., доцент Олександр МАЦЕНКО _____
(підпис)

Суми – 2023

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Факультет Електроніки та інформаційних технологій

Кафедра Електроніки і комп'ютерної техніки

Спеціальність 171 Електроніка

Освітня програма Електронні системи та компоненти

ЗАТВЕРДЖУЮ

Зав. кафедрою Опанасюк А.С.

"___"_____ 2023 р.

З А В Д А Н Н Я

на кваліфікаційну роботу магістра студентові

_____ Шкирданю Владиславу Сергійович_____

1 Тема проекту (роботи) «Електронна охоронна система розумний дім» затверджена наказом по університету "15" грудня 2023 р.№1466-VI

2 Термін здачі студентом закінченої проекту (роботи) _____

3 Вихідні дані до проекту (роботи). Система повинна забезпечувати моніторинг стану системи по протоколу Wi-Fi; керування виконавчими механізмами та режимом роботи системи по радіоканалу; оповіщення спрацювання системи по GSM каналу; світлозвукова сигналізація спрацювання системи; оступ до системи за допомогою RFID-ключа; можливість підключення 3х датчиків інфрачервоного та 3 датчиків магнітного випромінювання для моніторингу території.

4 Зміст розрахунково-пояснювальної записки (перелік питань, що належить розробити) 1. Огляд літератури та поставлення задачі проектування. 2. Наукова-дослідна частина. 3. Вибір та обґрунтування алгоритму функціонування та структурної схеми системи. 4. Розробка функціональної схеми блоків системи. 5. Вибір елементної бази та розробка принципових електричних схем блоків. 6. Техніко-економічна частина; Висновок; Список літератури.

5 Перелік графічного матеріалу: 1. Схема алгоритму функціонування. 2. Схема електрична структурна. 3. Схема електрична функціональна. 4. Схема електрична принципова

6 Консультанти по проекту (роботі), із зазначенням розділів проекту, що стосуються їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Економічна частина	МАЦЕНКО О.М.		

7 Дата видачі завдання

Керівник роботи Гриненко В.В.

Завдання прийняв до виконання Шкирдань В.С.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Огляд літератури та поставлення задачі проектування		
2	Вибір та обґрунтування алгоритму функціонування та структурної схеми системи		
3	Науково-дослідна частина		
4	Розробка функціональної схеми блоків системи		
5	Вибір елементної бази та розробка принципових електричних схем блоків		
6	Економічна частина		

Студент-дипломник _____ Шкирдань В.С.

Керівник проекту (роботи) _____ Гриненко В.В.

"___"_____2023 р.

Реферат

Випускна кваліфікаційна робота магістра сформована з 86 сторінок, 21 рисунків, 19 таблиць, 22 літературних джерела.

Об’єктом дослідження є інтерфейси зв’язку мікроконтролерів. Предмет дослідження охоронна система.

В ході роботи були розглянуті вразливості і факторів, що впливають на систему зв'язку охоронної системи розумного будинку. В ході досліджень було визначено, що технологія бездротового зв'язку LoRa найкраще підходять для виконання поставленої задачі.

За основу було взято мікроконтролер ATmega2560AU16, для дистанційного управління трансівер RFM95W-868S2, для моніторингу стану системи трансівер ESP8266 ESP-01S, для оповіщення по GSM мережі модуль SIM900D, узгоджувач логічних рівнів TXB0104 для нормальної роботи модулів з живленням 3.3В, для локального оповіщення дисплей LCD 1602 та сирена світлозвукова Дует (С-06С-220), матрична клавіатура для локальної взаємодії з системою

Зміст

Список скорочень

РБ – Розумний буднок

ТЗ – Технічні засоби

ОІ – Обробка інформації

ПЗ – Програмне забезпечення

ІЧ – Інфрачервоний

Вступ

В сучасному світі, де технологічний прогрес стрімко розвивається, поняття "розумний будинок" стає не просто технічним виробом, але й необхідною частиною нашого повсякденного життя. Розумні будинки втілюють у собі концепцію забезпечення житлових просторів високотехнологічними рішеннями для комфорту, безпеки та ефективного використання енергії.

Однак із зростанням рівня автоматизації та взаємодії між різними системами в розумному будинку зростають і виклики стосовно безпеки цих систем. Охоронна система розумного будинку стає ключовою складовою для захисту від потенційних загроз, які можуть виникнути в цифровому середовищі.

Ця кваліфікаційна робота магістра присвячена розробці та аналізу охоронної системи для розумного будинку. У процесі роботи буде проведений детальний аналіз вимог до системи безпеки, розглянуті сучасні технології, такі як KeeLoq та LoRa, для забезпечення ефективного та безпечного зв'язку в системі.

Основні цілі даної роботи полягають у визначенні вимог до охоронної системи розумного будинку, розробці оптимального зв'язку для забезпечення стійкості та конфіденційності даних, а також у створенні практичної реалізації системи та проведенні експериментальних досліджень.

Результати даної роботи можуть стати важливим внеском у розвиток безпеки розумних будинків та визначити перспективи використання конкретних технологій для забезпечення ефективності та надійності охоронних систем.

1. Огляд літератури та постановка задачі

Огляд та характеристика найбільш широко-розповсюджених протоколів передавання даних, які використовуються для зв’язку пристроїв системи розумний будинок.

1.1 Бездротові протоколи зв’язку

Бездротові протоколи зв’язку це найпопулярніший вид протоколів в основному через більш простий метод установки устаткування, проте важливу роль має відсутність необхідності втручання в кабельну мережу будинку. Серед бездротових алгоритмів передачі даних виділимо вісім найбільш відомих:

1) ZigBee. Один з найпопулярніших протоколів ZigBee. Використовується повсюдно через свою низьку ціну на модулі і високого енергозбереження. Стандарт підтримує Mesh мережі, шифрування та інші. Був створений як заміна протоколів Bluetooth і Wi-Fi, в силу підвищеної швидкості «опитування» датчиків і більш довгого життя від акумулятора. До недоліків також можна віднести «Vendor lock-in», який не дозволяє, наприклад, датчик від Xiaomi підключити до шлюзу від Ikea.

2) Z-wave. Так само, як і попередній, працює по радіочастотах і так само вміє будувати Mesh-мережі. Пристрої з цим протоколом виходять дорожчі, ніж ZigBee, через високу вартість ліцензування мікросхем зв’язку. Треба розуміти також, що можливо зіткнутися з непоєднаним використанням різних пристроїв, які призначені для різних країн, тобто в сукупності в одній системі ці пристрої працювати не будуть. Це пов'язано з різними ліцензованими частотами в різних країнах. Вважається більш надійним і вивченим протоколом, на відміну від ZigBee.

3) LoRa та LoRaWAN. LoRa створена для передавання невеликої кількості інформації на великі відстані, досить рідко (як правило, не частіше разу в 10 хв) і дуже енергоефективно. LoRa працює на різних частотах в різних країнах. В Європі - це 868 МГц. Ці частоти можуть бути використані вільно, хоч і з

обмеженнями. Дозволено передавання з потужністю менше 25 мВ і 1% часу. Мовлення на такій великій потужності дозволяє встановлювати зв'язок на кілометри, в ідеальних умовах - навіть на сотні кілометрів. Якщо говорити про реальне використання, ми можемо отримати покриття однієї базової станцією радіусу в 1 км в завантажених міських умовах, до 10-15 км в незавантажених умовах. LoRa (Long Range) позначає лише вид модуляції, тобто передавання сигналу між пристроями на фізичному рівні, а LoRaWAN (Long Range Wide-Area Network) - це протокол більш високого рівня. LoRaWAN дозволяє використовувати комунікацію на великі відстані за допомогою LoRa, для повноцінного IoT.

4) Bluetooth. Це мабуть найбільш невдалий протокол для девайсів середовища розумного будинку. По-перше, в більшості випадків можна отримати доступ до своїх девайсів лише перебуваючи поруч з ними. По-друге, навіть перебуваючи вдома, радіус дії сильно менше того ж Wi-Fi та ін. Проте є і цікаві рішення, які можна використовувати. При використанні Bluetooth є потенційні проблеми з завадами оскільки він працює на частоті 2,4 ГГц. Знову ж таки, чим більше пристроїв на вашій частоті, тим більше завад і, отже, латентність. Хоча Bluetooth існує вже 22 роки, він тільки недавно увійшов в індустрію Home Automation і, таким чином, не має так багато варіантів, доступних для споживача. Крім того, багато HUB не підтримують Bluetooth LE в даний час. Однак подивіться на це, щоб змінити, як деякі HUB, такі, як Wink, недавно запустили сумісність Bluetooth LE. Переваги Bluetooth LE - це спосіб енергоспоживання та вартість.

5) IR протокол зв’язку. Ще більш давня технологія, яку підтримують в РБ виключно для сумісності зі старими пристроями, які не мають альтернативних каналів управління. До них можна віднести кондиціонери, вентилятори і деякі люстри з пультом дистанційного керування. Для інтеграції цих, не особливо розумних пристроїв, використовують так звані IR-мости. Робити своє житло розумним, використовуючи цю технологію в чистому вигляді дуже складно. IR, по суті, складається з суцільних недоліків: маленький радіус дії, велика кількість

незрозумілих візуально команд, необхідність зчитувати кожну команду в ручному режимі, відсутність зворотного зв'язку.

6) Протокол Wi-Fi. Даний протокол використовується практично в кожному розумному будинку. Дуже популярне рішення для пристроїв, постійно підключених до електроживлення. Зазвичай цей стандарт зв'язку застосовується для того, щоб з'єднати смартфон або планшет з уже готовою автоматизованою системою. Мобільний пристрій завжди під рукою, а тому управляти будинком з його допомогою, зручніше, ніж використовувати для цієї мети комп'ютер, настінну сенсорну панель, пульт дистанційного керування або інтерпретатор мови. Особливо це актуально в тих випадках, коли для взаємодії з системою передбачено спеціальний додаток, а не тільки веб-інтерфейс. Іноді Wi-Fi застосовується для зв'язку з пристроями, які можуть функціонувати автономно, без допомоги «розумної» мережі. Останнім часом подібні пристрої набирають популярність, адже вони дозволяють долучитися до технологій розумного будинку, не витрачаючи час і сили на установку допоміжного обладнання. Для складних систем автоматизації Wi-Fi не підходить: модулі зв'язку цього стандарту дорогі, а швидкості передавання даних в рамках розумного будинку просто не затребувані.

7) Протокол зв’язку 433 MHz. Цей протокол пов'язує пристрої, які працюють як на 433 частоті, так і на 868, в принципі роботи яких, по суті, більше відмінностей і немає. Це дещо стара технологія, яку використовували, в основному, для управління світлом і деякими бездротовими датчиками. Недолік її в тому, що в більшості випадків ці пристрої працюють без зворотного зв'язку. Будувати надійну систему РБ на цій радіотехнології зараз не доцільно. Однак ця технологія успішно використовується в розумних вимикачах та датчиках компанії Noolite, а також термоголовках фірми MAX, Gidrolock і DeLumo, що працюють на частоті 868 МГц.

8) Протокол зв’язку Insteon. Insteon користується великою популярністю в США, проте в Європу та Україну він прийшов зовсім недавно. Фактором, що стримує поширення, стала несумісність початкової версії протоколу з нашими

електромережами: Insteon використовує проводку будівлі для передавання сигналів. Проте даний стандарт також підтримує зв'язок по радіоканалу, причому провідна і бездротова мережа функціонують одночасно, доповнюючи один одного і істотно підвищуючи надійність автоматизованої системи. Крім того, у Insteon немає проблем з чутливість та наводками. До плюсів Insteon також можна віднести топологію Mesh-мережі і сумісність з пристроями X10: є можливість поступово перейти зі старого стандарту на новий. Цікава особливість - можливість організувати працездатну мережу без використання центрального контролера. Звичайно, в цьому випадку функціонал РБ буде сильно обмежений. З точки зору проектування даний протокол схожий з Z-Wave: все стандартизовано, значна частина обладнання випускається під брендом Insteon фірмою Smartlabs. Систему для РБ на основі нового стандарту можна збирати поступово, докуповуючи необхідні компоненти за необхідності. Загалом, Insteon хороший, проте його недоліків можна віднести проблеми з доступністю необхідного обладнання в Україні та на ринку країн СНД.

Таким чином, залежно від поставлених завдань, бюджету, або технічних вимог, можна використовувати відповідні пристрої, поєднуючи та комбінуючи різні технології, наприклад, Zigbee і WiFi, і, додавши до цього, ще й Z-Wave.

1.2 Провідникові технології зв’язку

Протоколи цього типу використовуються в побуті користувачами набагато рідше, в силу того, що провід, що висить посеред стіни, по суті нікуди не сховаєш. Та й заздалегідь усе передбачити не у всіх виходить. Але величезною перевагою проводів, безсумнівно, є як стабільна робота пристроїв, так і незалежність від вбудованої батарейки, які періодично все ж доведеться міняти. Серед провідних протоколів можна виділити такі:

1) Протокол зв’язку RS-485. Напевно, найпопулярніший стандарт в провідних пристроях РБ. Протокол Modbus використовує стандарт зв’язку RS-485, як основу для зв'язку приймача і передавача. В даному варіанті використовується одна кручена пара, по якій передаються тільки дані. Живлення як на приймач, так

і на передавач, подається окремо. Обмін інформацією в даній мережі здійснюється шляхом передавання від передавача до приймача різниці напруг на кінцях сигнальних проводів. Максимально можлива кількість пристроїв, що під'єднані до однієї лінії, з урахуванням використання підсилювачів, - 256, а максимальна довжина кабелю може досягати 1200 метрів. В силу принципу роботи протоколу, необхідно забезпечити 24 відсутність наведень на дата-кабель, тому на великих відстанях дуже бажано використовувати екрановану виту пару.

2) Протокол зв’язку 1-Wire. З цим протоколом стикався практично кожен, хто користується домофонним ключем у вигляді таблетки. Для зв'язку пристрою з приймачем необхідно два контакти: дата і земля. У передавачі, зазвичай, встановлюється невеликий конденсатор, який, заряджаючись від даних контактів і підживлює чіп 1-wire. Крім домофонних ключів, складно знайти застосування даної технології для її спеціального використання, однак її можна зустріти в акумуляторах стільникових телефонів і ноутбуків. Використовуються вони, в основному, для передавання нескладних даних, у вигляді споживаного струму, температури і т.п.

3) Протокол зв’язку I²C. I²C - ще один представник протоколів з двопровідним з'єднанням пристроїв. Поширений в DIY середовищі, як простий спосіб взаємодії між платами, що не вимагає великої кількості приймачів. На одній парі провідників може бути підключено до 128 пристроїв. Швидкість передавання даних в даному протоколі - 100 Кбіт / с, однак вона може падати до 10 Кбіт/с, в разі включення в загальну шину повільних пристроїв. Саме цей протокол використовує, наприклад, контролер Wirenboard для обміну даними, що підключаються безпосередньо встик до головного пристрою, модулями.

4) Протокол зв’язку KNX. Протокол зв’язку KNX можна охарактеризувати трьома словами: дорого, престижно, надійно. Даний варіант вважається своєрідним лідером по престижності на ринку домашньої автоматизації. Ціни на продукцію, в основному, відповідні. Наприклад, для розуміння вартості даного рішення ціна на двоклавішний вимикач від Schneider Electric стартує від 10 тисяч гривень. І це ще не найдорожче рішення. Ну і звичайно ж, для налаштування та

подальшого запуску своїх девайсів знадобиться KNX контроллер, який дуже не дешевий. Протокол складний в налаштуванні і підійде для реалізації далеко не кожному покупцеві. У свою чергу, даний стандарт гарантує стабільність і надійність роботи системи в подальшому.

5) Протокол зв’язку CAN. Цей протокол часто використовують в автомобілебудуванні для зв'язку бортового комп'ютера з периферією машини. Цікавою особливістю даного протоколу є зворотна залежність швидкості передавання даних від довжини провідників. Дані порівняння пропускної швидкості відносно довжини наведенні в табл. 1.1. Чим більше довжина кабелю, тим повільніше вийде передавати по них інформацію. Для використання в системах «Розумний дім» даний варіант не підходить. У побуті застосовується, в основному, в кліматичному обладнанні, на кшталт котлів і кондиціонерів, для обміну даними з керуючого пульта до головного пристрою. Деякі, використовуючи спеціальні плати перетворювачі, перехоплюють команди і отримують управління технікою в своєму розумному будинку. На практиці ж мало де можна зустріти використання цього протоколу, як основного.

Таблиця 1.1 – Порівняння пропускної швидкості відносно довжини

Пропускна швидкість	Дальність
1 Мбіт / с	40 м
500 кбіт / с	100 м
125 кбіт / с	500 м
10 кбіт / с	5000 м

В результаті аналізу провідникових технологій зв’язку можна зробити висновок, що деякі протоколи дуже схожі один на одного, а деякі - абсолютно різні. Об'єднує їх усіх, по суті, тільки використання кабелю, або кабелів для прийому та передавання даних. Вагомим недоліком провідникових технології є те, що проектування РБ потрібно починати ще до проведення електроживлення в будинку або до закінчення «чорнових» робіт. При чому дане проектування є

досить складним і потребує вагомого досвіду та розрахунків для подальшого використання, адже змінити будь шо в уже наявній системі складно.

1.3. Порівняльний аналіз характеристик протоколів зв’язку.

Бездротові рішення можуть бути використані для організації бездротового зв'язку за допомогою призначених для користувача протоколів передавання даних, або для реалізації рішень, що використовують стандартні мережеві стеки комунікації на основі специфікації IEEE802.15.4 або рішень фірм-виробників компонентів для бездротових систем. Так, стандарт IEEE802.15.4 є основою для таких додатків, як ZigBee RF4CE (побутова електроніка), що підтримують профіль дистанційного керування (ZRC) або профіль пристроїв введення (ZID). Широке поширення отримали ZigBee PRO-сумісні бездротові мережі, такі як мережі автоматизації приміщень (ZHA), автоматизації будівель (ZBA), управління освітленням (ZLL) або інтелектуального розподілу електроенергії (ZSE). Стандарт IEEE 802.15.

ZigBee погано справляється з ситуаціями, коли в зоні дії мережі існують сильні завади, які створюються іншими пристроями. Будучи одноканальним рішенням, ZigBee далеко не завжди може ефективно боротися з завадами, які часто зустрічаються в перевантаженій смузі 2,4 ГГц, яка спільно використовується протоколом з такими технологіями, як Wi-Fi або Bluetooth. І в найближчому майбутньому ситуація стане ще гірше, так як завантаженість смуги 2,4 ГГц з кожним роком буде зростати.

Проблеми для ZigBee посилює ще той факт, що стандарт IEEE 802.15.4, що визначає фізичний рівень стека протоколів ZigBee, що обмежує, в тому числі швидкість передавання даних до 250Кбіт/с, знаходиться під контролем IEEE. Він використовується не тільки ZigBee, але і десятками інших рішень. Z-Wave Alliance визначає кожен окремий рівень моделі OSI, і тому всі рішення, що стосуються будь-якого аспекту зв'язку, знаходяться в руках однієї організації .

Що стосується безпеки, то ZigBee пропонує широкий спектр розширених заходів для забезпечення достатнього захисту даних, якими обмінюються

розумні пристрої. З 128-бітовим алгоритмом AES, використовуваним для шифрування даних та аутентифікації, і трьома типами ключів, використовуваних для управління безпекою, кінцевим користувачам на перший погляд не варто турбуватися. Однак, час від часу з'являються виникають проблеми із безпекою в пристроях з підтримкою ZigBee. Вони, в основному стосувалися незахищеного формування парних ключів при підключенні нового пристрою до мережі.

Одним з недоліків цієї технології є частотний діапазон. Вибір низькочастотного, стабільного і найбільш вільного діапазону для пристроїв малого радіусу дії, а не більше популярного і завантаженого (2,4 ГГц) виявився далекоглядним і правильним рішенням, позбавивши користувачів розумного будинку Z-Wave від серйозних проблем з завадами в сильно завантажених «частотах Wi-Fi ». Але в різних країнах для роботи пристроїв малого дії виділені різні частоти, наприклад, для всієї Європи (країни CEPT), а також Китаю та ряду інших країн Азії - це 868,42 МГц. А ось в США і Мексиці ці частоти зайняті технологією GSM, тому рішення Z-Wave там працюють на частоті 908, 42МГц, в Росії - для Z-Wave робочий діапазон - 869,0 МГц. Це означає, що, з точки зору звичайного користувача, докуповувати новий продукт в іншій країні і підключати його до своєї мережі домашньої автоматизації потрібно з великою обережністю. Наприклад, пристрій, створене для ринку США, буде несумісним з пристроями діапазону інших країн.

Bluetooth використовує той же діапазон 2,4ГГц, що і багато інших радіотехнології, таких як мікрохвильові печі, радіоняні або бездротові телефони. Незважаючи на те, що Bluetooth забезпечений певним інструментарієм для протидії завад, використання смуги частот 2,4 ГГц - це безсумнівний недолік. Адже, крім наявності постійних завад, у діапазону 2,4 ГГц є ще один великий недолік - сигнал на цій частоті згасає набагато швидше, ніж на частотах менше 1 ГГц, коли радіохвилі проникають крізь стіни та інші завади.

З цієї ж причини радіус дії технології Bluetooth Low Energy не є її сильною стороною. Незважаючи на теоретично досяжні «до 100 метрів в зоні прямої видимості», для Bluetooth четвертої версії при роботі двох пристроїв в

приміщенні можна розраховувати на відстань до 10 метрів. Плутанини додає і той факт, що ця цифра сильно залежить не тільки від завад і перешкод, які є на шляху поширення сигналу, але і налаштувань виробників, так як з Bluetooth Smart у них є можливість в певних межах коригувати потужність сигналу пристрою (в тому числі збільшувати його потужність і підвищувати енергоспоживання).

Bluetooth, Wi-Fi і ZigBee мають маленький радіус зв'язку, а мобільний зв'язок і Wi-Fi споживають занадто багато енергії. Комунікація через ZigBee і LoRa дуже енергоефективна. Обидві технології використовуються для передавання невеликої кількості даних. ZigBee відмінно показує себе на невеликих відстанях, LoRa ж створена для комунікації на великі відстані. Також вони мають різну топологію мережі.

В табл. 1.2 представлено порівняльна характеристика основних характеристик та технологічних параметрів для протоколів ближнього радіуса дії.

Таблиця 1.2 – Протоколи ближнього радіусу дії

Технічні характеристики	Wi-Fi	Bluetooth Low Energy	ZigBee	Z-Wave
Дальність	До 100 м	80 м	100 м/Mesh	30 м/Mesh
Частота	2.4 ГГц, 5 ГГц	2.4 ГГц	915 МГц, 2.4 ГГц	900 МГц
Швидкість передачі	Макс. 7 Гбіт/с	< 1 мбіт/с	250 кбіт/с	10-100 кбіт/с
Споживання енергії	Високе	Понижене	Низьке	Низьке
Аутентифікація	Так	Проблематично	Так	Так
Шифрування	Так	Так	Так	Так
Двонаправленість	Так	Так	Так	Так
Стандарт	IEEE 802.11	Bluetooth 4.0	ZigBee	Z-Wave
Маштабованість	Так	Так	Так	Обмежено

А ще, при використанні спільно Wi-Fi, Zigbee і Bluetooth, оскільки протоколи працюють на близьких радіочастотах, то їх хвилі можуть накладатися один на одного, утворюючи завади (див. рис. 1.1). Не варто цього боятися, так відбувається не у всіх, але треба пам'ятати даний факт при побудові мережі розумних пристроїв. Розподіл каналів зв’язку по протоколах показано на рис. 1.1.

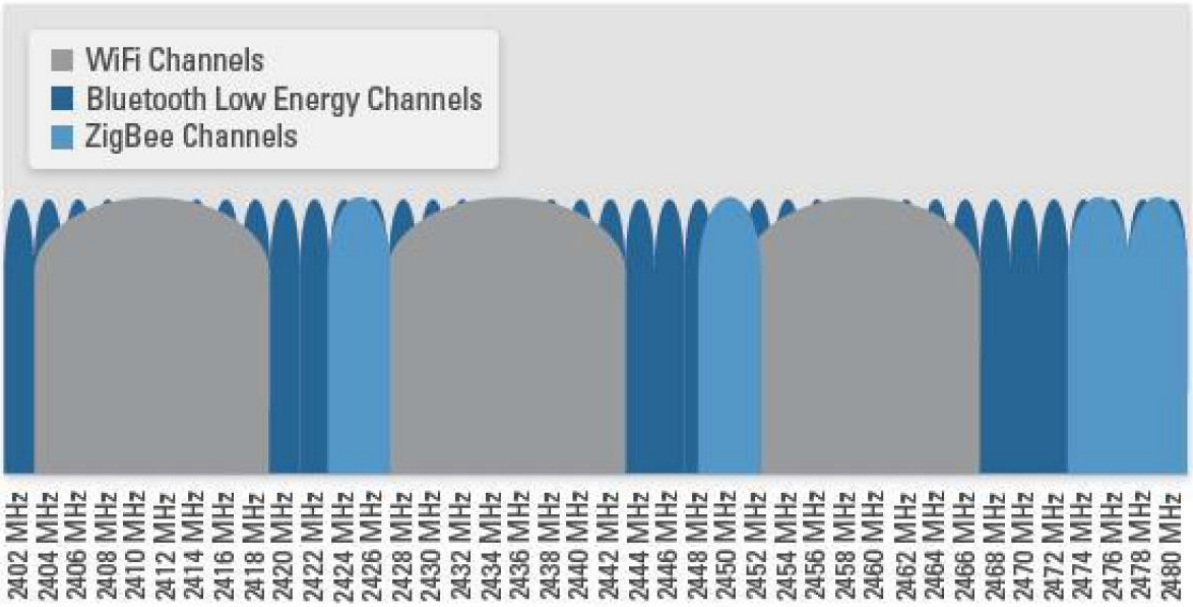

Рисунок 1.1. – Розподіл каналів зв’язку по протоколах

Перспективи використання Bluetooth Low Energy Mesh-мережа Bluetooth сильно відрізняється від інших технологій. Основна відмінність полягає в тому, як повідомлення поширюються через мережу. Як при маршрутизації на основі джерела повідомлення (Z-Wave), так і при маршрутизації на основі призначення (ZigBee, Thread), кожне повідомлення поширюється по певному шляху, передаючись від одного вузла до іншого, поки не досягне пункту призначення. Mesh-мережа Bluetooth використовує підхід, так званої керованої лавинної маршрутизації.

Цей підхід є вкрай не оптимальним з точки зору використання пропускної здатності мережі, однак не вимагає побудови таблиць маршрутизації і не потребує складних процедурах відновлення працездатності мережі. Таким чином, керована лавинна маршрутизація використовує менше пам'яті і обчислювальних потужностей, що сприятливо позначається на підсумковій

вартості готових рішень. Вона також теоретично може демонструвати кращу стійкість до завад в діапазоні 2.4ГГц, ніж інші рішення, що працюють на тій же частоті, але тільки за умови досить щільного розташування сенсорів в мережі. Однак через таку високу ресурсоємність Mesh-мережі Bluetooth погано підходять для створення складних проектів домашньої автоматизації, не кажучи вже про різноманітні комерційні впровадження.

Сьогодні безумовний лідер по взаємодії між різними пристроями різних виробників в рамках одного протоколу - технологія Z-Wave. Z-Wave охоплює всі рівні моделі OSI. Але, на відміну від, наприклад, Bluetooth Smart (який також підтримує всі ці рівні), протокол Z-Wave спочатку розроблявся як технологія комірчастої мережі з високим рівнем відмовостійкості. Крім того, Z-Wave - єдина з популярних технологій, яка не використовує перевантажений до межі частотний діапазон 2,4 ГГц. Всі ці переваги дозволили Z-Wave Alliance створити, без перебільшення, найрозвиненішу в світі екосистему пристроїв РБ із більше ніж 100 млн впроваджень системи.

У Zigbee і Bluetooth Smart теж є шанси на розвиток. У першому випадку розробники намагаються вирішити проблему внутрішньопротокольної сумісності шляхом впровадження надбудови Dotdot. Але, з огляду на величезну інстальовану базу Zigbee-пристроїв колишніх поколінь і м'яку політику сертифікації Zigbee Alliance, навряд чи можна сподіватися на швидкий прорив в плані безпроблемної роботи гаджетів Zigbee різних виробників. Крім того, потенційним конкурентом Zigbee вважається протокол Thread, який поки є маловідомим на ринку розумних будинків.

У випадку з Bluetooth Low Energy, перспективи цього протоколу в чому залежать від того, наскільки успішними будуть спроби реалізувати в ньому топологію пористих мереж. Так чи інакше, і Bluetooth, і Zigbee, і Thread жорстко прив'язані до зашумлення радіодіапазону 2,4 ГГц. Ринок бездротових технологій РБ швидко змінюється. Незмінними залишаються тільки вимоги до енергоспоживання пристроїв, безпеки, відмовостійкості мережі, здатності

пристроїв протистояти радіозавадам, простоті підключення, а також взаємної сумісності продуктів одного і того ж стандарту зв'язку .

1.4. Висновки до розділу 1. Постановка задачі

В процесі проведення огляду літературних джерел встановлено, що з кожним роком кількість «розумних пристроїв» постійно буде зростати, що в свою чергу призведе до зайвого нагромадження в ефірі пакетів даних, спричиненого використанням одного і того ж діапазону частот.

В результаті аналізу технологій побудови систем «Розумний будинок» обґрунтовано доцільність використання безпровідних технологій та встановлено, що для обміну даними в таких системах у всьому світі надаються неліцензовані радіочастотні діапазони, які можуть використовуватися без оформлення спеціального дозволу і абсолютно безкоштовно за умови дотримання вимог щодо ширини смуги, випромінюваної потужності.

Обґрунтовано важливість вибору частоти передавання даних при проектуванні системи «Розумний будинок» та актуальність розробки адаптивного методу вибору каналів зв’язку з метою формування переліку пріоритетних вільних частот для обміну інформацією між модулями розумного будинку.

Метою даної роботи є створення ефективної та безпечної системи охорони для розумного будинку з використанням сучасних технологій зв'язку та з урахуванням факторів безпеки, з реалізацією наступних функцій:

- моніторинг стану системи по протоколу Wi-Fi;
- керування виконавчими механізмами та режимом роботи системи по радіоканалу;
- оповіщення спрацювання системи по GSM каналу;
- світлозвукова сигналізація спрацювання системи;
- доступ до системи за допомогою RFID-ключа;
- можливість підключення 3х датчиків інфрачервоного та 3 датчиків магнітного випромінювання для моніторингу території.

2. Науково-досілідна частина

2.1 Аналіз вразливостей і факторів, що впливають на систему зв'язку охоронної системи розумного будинку.

В даний час з усіх представлених на ринку технологій побудови IT-систем «розумний дім», можна виділити кілька готових до застосування комплексних систем, які є типовими представниками в своєму класі:

– централізовані;

– децентралізовані.

Також системи можна класифікувати на:

– дротові;

– бездротові.

На прикладі цих комплексних систем розглянемо основні фактори, що впливають на безпеку інформації, що захищається «розумного будинку», побудованого на основі готових систем.

Зазначені фактори поділяються на:

1) за ознакою ставлення до природи виникнення:

– об'єктивні;

– суб'єктивні.

2) по відношенню до об'єкта інформації:

– внутрішні;

– зовнішні.

Централізована система управління. Як правило, вона будується на основі застосування широкого спектра керуючих центральних контролерів і безлічі виконавчо-командних блоків. Керуючі контролери володіють великим набором вбудованих можливостей, сумісні з безліччю поширених протоколів передачі інформації .

Для даної системи фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 2.1 і табл. 2.2.

Розглянемо схему підключення пристроїв в децентралізованій мережевій технології (рис. 2.1).

Таблиця 2.1 – Об'єктивні чинники, що впливають на безпеку інформації, що захищається централізованої системи управління «розумним будинком».

Внутрішні чинники	**Зовнішні чинники**
Випромінювання акустичних сигналів супутні виголошуваної технічним засобом (ТЗ) мови	Збої, відмови і аварії систем забезпечення об'єкта інформації (ОІ)
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Термічні фактори (пожежі і т.д.)
Дефекти, збої і відмови, аварії ТС і систем обробки інформації	Кліматичні чинники (повені і т.д.)

Таблиця 2.2 – Суб'єктивні чинники, що впливають на безпеку інформації, що захищається централізованої системи управління будинком.

Внутрішні чинники	**Зовнішні чинники**
Розголошення інформації, що захищається особами, які мають до неї право доступу через передачу інформації за відкритими лініях зв'язку	Доступ до інформації, що захищається з застосуванням ТС знімання інформації
Несанкціонований доступ до інформації шляхом підключення до технічних засобів і систем ОІ	Несанкціонований доступ до інформації, що захищається шляхом використання закладних засобів
Використання програмного забезпечення (ПЗ) технічних засобів ОІ через внесення програмних закладок	Блокування доступу до інформації, що захищається шляхом перевантаження ТС обробки інформації помилковими заявками на її обробку

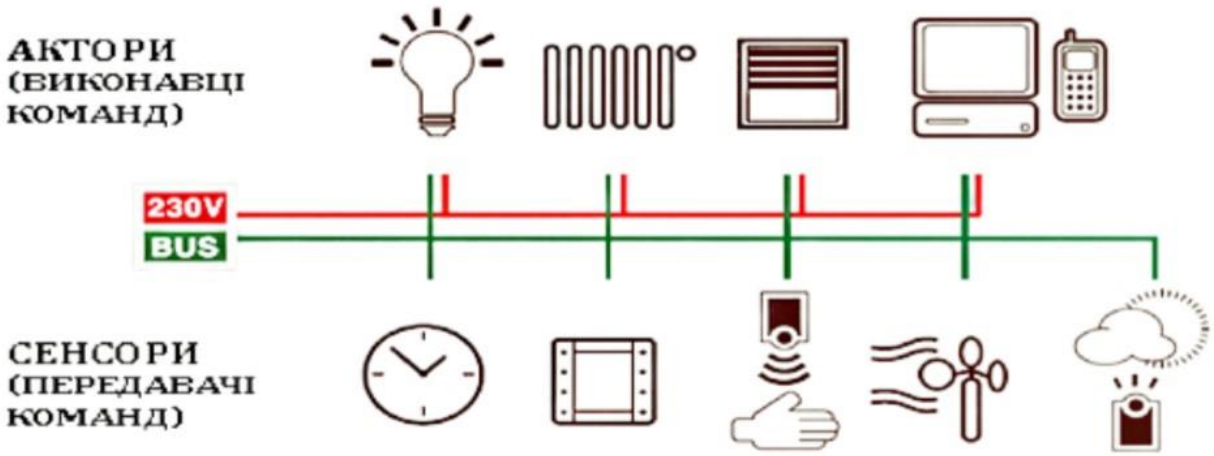

Рисунок 2.1 – Загальна схема підключення децентралізованої системи

Пристрої (передавачі або приймачі) в децентралізованій системі зв'язуються один з одним безпосередньо, без ієрархії або центрального контролюючого приладу. Компоненти здійснюють передачу послідовно, асинхронно, конфлікти при передачі повідомлень вирішуються розстановкою пріоритетів повідомлень. Призначена для передачі інформація збирається в пакети- «телеграми» і через шину передається приймачу або групі приймачів. Повідомлення отримують всі абоненти, але реагують на нього тільки ті, кому воно адресоване. Сьогодні децентралізовані системи підтримує обмін по крученій парі, безпосередньо по силової лінії, по радіо і по ІЧ-каналу. Для систем з децентралізованим управлінням фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 2.3 і табл. 2.4.

Таблиця 2.3 – Об'єктивні чинники, що впливають на безпеку інформації децентралізованої системи управління «розумним будинком» по ІЧ-каналу

Внутрішні чинники	**Зовнішні чинники**
Дефекти, збої і відмови ПЗ	Збій, відмови і аварії систем забезпечення ОІ
Наведення в лініях зв'язку, викликані побічними електромагнітними випромінюваннями, що несуть інформацію	Термічні фактори (пожежі і т.д.)
Наявність акустоелектричних перетворювачів в елементах ТС ОІ	Кліматичні чинники (повені і т.д.)

Система управління будинком X-10 - міжнародний відкритий промисловий стандарт, застосовуваний для зв'язку електронних пристроїв в системах домашньої автоматизації. Стандарт X10 визначає методи і протокол передачі сигналів управління електронними модулями, до яких підключені побутові прилади, з використанням звичайної електропроводки або бездротових каналів.

Таблиця 2.4 – Суб'єктивні чинники, що впливають на безпеку інформації децентралізованої системи управління «розумним будинком» по ІЧ-каналу

Внутрішні чинники	**Зовнішні чинники**
Неправомірні дії з боку осіб, які мають право доступу до інформації, що захищається, шляхом несанкціонованого зміни інформації.	Доступ до інформації, що захищається з застосуванням ТС технічної комп'ютерної розвідки.
Недоліки організаційного забезпечення захисту інформації при завданні вимог щодо захисту інформації.	Спотворення, знищення або блокування інформації шляхом розкрадання носія інформації.
Несанкціонований доступ до інформації шляхом внесення програмних закладок.	Спотворення, знищення або блокування інформації шляхом використання програмних або програмно-апаратних засобів при здійсненні мережевої атаки.

Мережа X10 включає в собі наступні основні компоненти: передавачі, приймачі, трансивери, пульти дистанційного керування та лінійні компоненти. Системам використовують провідні технології побудови системи «розумний дім» (зокрема стандарт X10) притаманні фактори, що впливають на безпеку інформації, що захищається представлені в табл. 2.5 і табл. 2.6.

Таблиця 2.5 – Об'єктивні чинники, що впливають на безпеку інформації в провідних системах управління «розумним будинком» (стандарт X10)

Внутрішні чинники	**Зовнішні чинники**
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Ненавмисні електромагнітні опромінення ОІ
Наведення в електричних ланцюгах ТС викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Електромагнітні фактори (грозові розряди і т.д.)
Наведення в ланцюгах заземлення викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Кліматичні чинники (повені і т.д.)

Таблиця 2.6 – Суб'єктивні чинники, що впливають на безпеку інформації в провідних системах управління «розумним будинком» (стандарт X10)

Внутрішні чинники	**Зовнішні чинники**
Розголошення інформації, що захищається особами, які мають до неї право доступу через осіб, які не мають права доступу до інформації, що захищається	Доступ до інформації, що захищається з застосуванням ТС радіоелектронної розвідки
Несанкціонований доступ до інформації шляхом порушення функціонування ТС обробки інформації	Спотворення, знищення або блокування інформації шляхом навмисного електромагнітного впливу по мережі електроживлення
Помилки користувачів або обслуговуючого персоналу при експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом навмисного силового впливу фізичної природи

Система управління будинком Z-Wave є запатентованим бездротовим протоколом зв'язку, розробленим для домашньої автоматизації, зокрема для контролю і управління в житлових і комерційних об'єктах. Технологія використовує малопотужні і мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку і різні пристрої, такі як освітлювальні прилади, прилади опалення, пристрої контролю доступу, розважальні системи і побутову техніку. Більшість систем використовують бездротові канали зв'язку схильні до факторів, що впливають на безпеку інформації.

Чинники, що впливають на безпеку інформації в системах управління будинком на основі технології Z-Wave представлені в табл. 2.7 і 2.8.

Таблиця 2.7 – Об'єктивні чинники, що впливають на безпеку інформації в провідних системах управління «розумним будинком» (стандарт Z-Wave)

Внутрішні чинники	**Зовнішні чинники**
Електромагнітні випромінювання і поля в радіодіапазоні	Ненавмисні електромагнітні опромінення ОІ
Побічні електромагнітні випромінювання на частотах роботи високочастотних генераторів пристроїв, що входять до складу ТЗ ОІ	Радіаційні опромінення ОІ
Побічні електромагнітні випромінювання на частотах самозбудження підсилювачів пристроїв, що входять до складу ТЗ ОІ	Природні явища, стихійні лиха

Таблиця 2.8 – Суб'єктивні чинники, що впливають на безпеку інформації в провідних системах управління «розумним будинком» (стандарт Z-Wave)

Внутрішні чинники	**Зовнішні чинники**
Несанкціонований доступ до інформації шляхом підключення до ТЗ і системам ОІ	Доступ до інформації, що захищається з застосуванням ТС радіоелектронної розвідки
Розголошення інформації, що захищається особам, які не мають до неї право доступу	Доступ до інформації, що захищається шляхом використання шкідливого ПЗ
Помилки обслуговуючого персоналу при експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом здійснення мережевої атаки

Таким чином розроблена система суб'єктивних і об'єктивних факторів, що впливають на систему «розумного будинку». Надалі ця система буде використана для аналізу загроз «розумного будинку».

Загрози конфіденційності, цілісності та доступності інформації IT-системи «розумного будинку»

Під загрозою безпеки інформації будемо розуміти сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації. Під вразливістю розуміється властивість інформаційної системи, що обумовлює можливість реалізації загроз безпеки оброблюваної в ній інформації.

Базовими загрозами інформаційній безпеці «розумного будинку» є:

– порушення конфіденційності;

– порушення цілісності;

– порушення доступності інформації.

У контексті аналізу «розумного будинку» під конфіденційністю мається на увазі такий стан IT-системи управління «розумним будинком», при якому відсутня можливість витоку інформації через підсистеми. Приклад реалізації

загрози - витік персональної інформації або витік інформації про конфігурацію IT-систем «розумного будинку».

Цілісність інформації - це достовірність і повнота інформації отримується системою від різних датчиків і пристроїв, встановлених в системі, наприклад, при отримання невірної інформації системою про наявність в приміщенні людини може привести до помилкового спрацьовування системи контролю доступу.

Доступність інформації стосовно «розумному будинку» - це стан інформації або ресурсів IT-системи, при якому суб'єкти або сама система, що мають права доступу, можуть реалізувати різні дії відповідно до сценарію роботи (вимикати / включати датчики, відкривати замки і т.д .). Приклад реалізації даної загрози - виведення з ладу комунікаційного обладнання системи.

Загрози інформаційної безпеки за своєю природою виникнення можна розділити на 2 групи: загрози, зумовлені людським фактором і загрози середовища (природні).

Зокрема, загрози першої групи розрізняються за способом здійснення: цілеспрямовані (навмисні) і випадкові (ненавмисні). Деякі приклади таких загроз наведені в табл. 2.9, варто відзначити, що загрози другої групи (загрози середовища), не піддаються прогнозуванню, і як правило, під ними мають на увазі природні катаклізми.

Іншим суттєвим фактором для визначення загроз інформаційної безпеки є ідентифікація можливих джерел загроз в залежності від їх розташування: внутрішні і зовнішні. До внутрішніх загроз відносяться загрози, розташовані всередині контрольованої зони, до зовнішніх - зовні (табл. 2.10). Більш повний список загроз можна подивитися на сайті бази даних загроз безпеки інформації.

Таблиця 2.9 – Класифікація загроз безпеки інформації ІТ-системи «розумного будинку»

Загрози, обумовлені людським фактором		**Загрози середовища**
Цілеспрямовані	**Випадкові**	
Модифікація інформації	Помилки ПЗ	Пожежа
Перехоплення інформації	Помилки користувача	Затоплення
Розкрадання обладнання	Помилки при обслуговуванні	Блискавка
Хакерська атака	Апаратні відмови	Землетрус
Шкідливе програмне забезпечення (ПЗ)	Помилки маршрутизації	Екстремальні величини температури і вологості

Таблиця 2.10 – Приклади внутрішніх і зовнішніх загроз інформації ІТсистеми «розумного будинку»

Внутрішні загрози	**Зовнішні загрози**
Загроза застосування коду або даних	Загроза відключення (екранування) контрольних датчиків
Загроза використання механізмів розробника	Загроза спотворення вводиться і виводиться на периферійні пристрої інформації
Загроза підміни програмного забезпечення	Загроза несанкціонованого віддаленого внеполосного доступу до апаратних засобів
Загроза доступу / перехоплення / зміни HTTP- cookies	Загроза подолання фізичного захисту
Загроза доступу до локальних файлів сервера за допомогою URL	Загроза межсайтовой підробки запиту

Оцінювання ризиків інформаційної безпеки «розумного будинку»

Загрози інформаційної безпеки ІТ-системи «розумний дім» в першу чергу залежать від обраних способів і технологій побудови даної системи, так як на визначення можливих загроз впливає склад обладнання. Для оцінки ризиків інформаційної безпеки «розумного будинку» розглянемо найбільш ймовірні загрози, реалізація яких може призвести до порушення інформаційної безпеки «розумного будинку» побудованого з централізованого технології .

Далі виявлені загрози зіставляються з уразливими, і визначається, які властивості активу (конфіденційність – К, цілісність – Ц, доступність – Д) можуть порушувати ті чи інші загрози (табл. 2.11).

Таблиця 2.11 – Загрози і уразливості безпеки «розумного будинку»

№	Загроза	Уразливість	Властивості, які загроза може порушити		
			К	Ц	Д
1	2	3	4	5	6
1	Атаки на центральний сервер	Підключення мережі «розумного будинку» до Інтернету. Недостатня ефективність захисту мережі «розумного будинку»	+	+	+
2	Впровадженн я шкідливого коду або програми	Підключення мережі «розумного будинку» до Інтернету. Відсутність (недостатня ефективність) механізмів захисту трафіку	+	+	+
3	Перехоплення і підміна переданого сигналу	Можливість доступу зловмисника до мереж передачі інформації. Відсутність (недостатня ефективність) механізмів захисту трафіку	+	+	
4	Доступ до мережі нелегітимних користувачів	Відсутність (недостатня ефективність) механізмів аутентифікації і ідентифікації	+		

Продовження Таблиці 2.11 – Загрози і уразливості безпеки «розумного будинку»

1	2	3	4	5	6
5	Використан ня механізмів розробника	Відсутність (недостатня ефективність) механізмів аутентифікації і ідентифікації	+	+	
6	Тривале утримання обчислювальних ресурсів користувачами	Слабкі механізми балансування навантаження і розподілу обчислювальних ресурсів			+
7	Доступ до захищених файлів з використанням обхідного шляху	Слабкості механізму розмежування доступу	+	+	
8	Відключенн я контрольних датчиків	Відсутність (недостатня ефективність) системи контролю доступу			+
9	Подолання фізичного захисту об'єкта	Уразливості в системі контролю фізичного доступу	+		+
10	Крадіжка апаратури чи носіїв інформації	Незахищене зберігання	+	+	+
11	Знищення апаратури або носіїв інформації	Відсутність системи автономного електроживлення. Чутливість до перепадів напруги			+
12	Помилки користувача	Відсутність механізмів моніторингу. Складний призначений для користувача інтерфейс	+		
13	Помилки ПЗ	Використання неліцензійного ПЗ	+		
14	Стихійні лиха	Відсутність (недостатня ефективність) системи фізичної охорони об'єкта		+	

Найбільш небезпечними загрозами є:

– атаки на центральний сервер;

– впровадження шкідливого коду або програми;

– перехоплення і підміна переданого сигналу;

– використання механізмів розробника;

– відключення контрольних датчиків;

– подолання фізичного захисту об'єкта.

Також небезпечними є ризики, пов'язані з несправністю в роботі систем електроживлення і помилками користувача і / або ПЗ.

У зв'язку з цим необхідно застосувати такі захисні заходи, для зниження ризиків, пов'язаних з реалізацією даних загроз:

1) застосування механізмів ідентифікації і аутентифікації користувачів;
2) застосування механізмів шифрування і контролю цілісності переданих даних;
3) використання антивірусного ПЗ;
4) організація системи контролю управління доступом;
5) використання механізмів розподілу навантажень;
6) періодична перевірка працездатності всіх елементів систем;
7) використання резервного джерела живлення.

Аналіз протоколів передавання даних для впровадження безпечних автоматизованих систем «розумного будинку»

Для подібного критичного механізму безпеки необхідно знайти протокол передачі інформації, який би відповідав критеріям забезпечення конфіденційності, цілісності і доступності даних, важливим пунктом буде спосіб спілкування з іншими структурними елементами житлового приміщення: розвиток систем «розумний дім» і бездротових модулів домашньої автоматизації призвело до часткової уніфікації даного сегмента і є можливість використання загальної мережевої інфраструктури.

Однак, незважаючи на розвиток і поступову офіційну і неофіційну стандартизацію технологій сегмента «розумний будинок» і будь-якої домашньої

автоматизації, залишається проблема вибору протоколів передачі інформації між керованими пристроями, датчиками і іншими елементами приміщень. Особливо гостро стоїть проблема, коли необхідно забезпечити конфіденційність і цілісність циркулюючих даних.

Метою дослідження є пошук захищеного мережевого протоколу, що дозволяє при його використанні в пристроях автоматичного сигналізування виключити вплив на конфіденційність, цілісність інформації без використання спеціальних програмно-апаратних рішень. Також необхідно забезпечити доступність даних пристроїв шляхом можливості вести автономну роботу. Основні захищені протоколи можна умовно розділити на два великі класи: застосовні при дротових рішеннях (наприклад, IPsec, SSL, TLS); застосовні при створення бездротових систем (ZigBee, Z-Wave, Thread, WeMo). У житлових приміщеннях застосовуються різні пристрої і технології, які, як правило, є надбудовою до вже існуючої інфраструктури, тому основним напрямком аналізу є бездротові протоколи, що дозволяють зручно реалізувати мережеве взаємодія. Провідні рішення варто розглядати тільки в умовах впровадження домашньої автоматизації на ранніх етапах будівництва окремих приміщень або квартир, а також при проектуванні критичних елементів системи . При використанні бездротових протоколів і пристроїв постає питання їх можливості забезпечити належний рівень конфіденційності і цілісності даних. Це пов'язано впливом на вже існуючі бездротові мережі в зоні застосування, поширеність протоколу зв'язку, можливість перехоплення сигналу з його подальшим аналізом або атакою. Також є додаткові вимоги щодо забезпечення доступності даних в «розумному будинку» і здатності вести автономну роботу.

Розглянемо чотири основних бездротових технології, за допомогою яких можна реалізувати систему автоматизації в захищеному виконанні. В якості порівняльних характеристик будемо досліджувати:

1) Шифрування даних: наявність і надійність технології для створення конфіденційного каналу передачі даних. Можливість використання в якості основної або додаткової можливості.

2) Топологія мережі: можливі варіанти підключення пристроїв в мережу.

3) Забезпечення доступності та автономності: наявність додаткових алгоритмів самоорганізації мережі і самовідновлення.

4) Швидкість передачі даних: висока пропускна здатність для забезпечення швидкого відгуку між запитом на дію і його виконанням, а також запасом ресурсу при завантаженні каналів передачі даних.

В першу чергу розглянемо шифрування. Для створення захищеної передачі даних, дана характеристика буде ключовою. Всі протоколи використовують шифрування, проте воно дуже сильно різниться. Якщо порівнювати Zig-Bee і ZWave, то вони обидва використовують AES-128, ключовою відмінністю Z-Wave є можливість використання даної технології тільки на відведених вузлах системи, а не повсюдно, як це реалізовано у Zig-Bee. Threadиспользует сучасні протоколи на основі еліптичних кривих, для яких ще не знайдено субекспоненціальное алгоритмів рішення. WeMo в даному випадку суперечливий, його можливості шифрування цілком і повністю залежать від можливостей маршрутизатора, це TKIP / AES шифрування. З точки зору доступності та можливостей серед 49 перерахованих алгоритмів необхідно використовувати Zig-Bee. У подальшому майбутньому протокол Threadімеет шанси замінити Zig-Bee, за умови, що збережеться швидкість шифрування. Також якщо порівняти алгоритми AES (ZigBee, WPA2, ZWave) і связку J-PAKE + NISTP-256 на рисунку 2.2, то можна переконатися в ефективності алгоритму AES для швидкої передачі великих обсягів даних. Однак на практиці все алгоритми прагнуть використовувати команди невеликої довжини, тому критерій швидкості буде помітний лише при використанні протоколів для нестандартних ситуацій. пристроїв шляхом можливості вести автономну роботу.

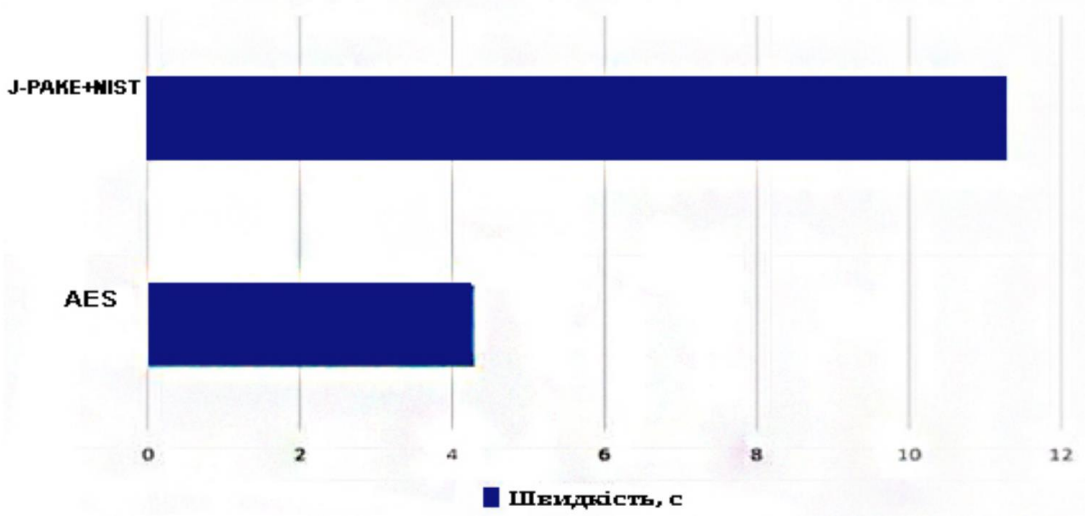

Рисунок 2.2 – Порівняння швидкості шифрування протоколів AES і зв'язки NISTP-256 + J-PAKE на прикладі кількох тестів (Менше, краще).

З точки зору створюваної топології мережі, існує два основні варіанти в пропонованих протоколах. Перший - мережа типу «зірка», є деяка центральне пристрій, який виступає в ролі єднальної ланки. Легко розгорнути, проте є наслідки у вигляді порушення доступності, при виході центрального блоку з ладу. Подібну мережу можуть розгорнути протоколи WeMo і Zig-Bee. Другий тип - чарункова, децентралізована мережа. Zig-Bee, Z-Wavei Thread підтримують цю технологію, останні два використовують як єдино можливу. Дана мережа, в силу своєї децентралізованість підвищує показники доступності всієї мережі.

Доступність є другим важливим критерієм для організації захищеного «Розумного будинку». Якщо в потрібний момент не будуть передані дані з датчиків руху, датчиків пожежі та інших, можуть статися різні надзвичайні ситуації. Протокол WeMo повністю залежить від маршрутизатора, тому в разі його відмови не має можливості забезпечення автономної роботи пристроїв «розумного будинку. Якщо розглядати Z-Wave, даний протокол зберігає працездатність при відсутності основного джерела електроживлення. Zig-Beei Thread крім харчування від акумуляторів мають алгоритми самоорганізації і самовідновлення мережі, що дозволяє зберігати доступність даних інфраструктури приміщень, в умовах недоступності окремих її вузлів.

Швидкість передачі даних протоколів, що працюють на малопотужних частотах, які не є їх сильною стороною, проте для передачі базових команд їх ресурсів більш ніж досить. В даному критерії виділяється лише WeMo, швидкість передачі даних в якому залежить від пропускної можливості маршрутизатора. Окремо необхідно відзначити питання про заміну захищених бездротових протоколів на російські аналоги. Незважаючи на те, що є особливі протоколи передачі інформації, що використовуються в АСУ ТП або бездротова технологія MeshLogic, технічні особливості не дозволяють їх правильно застосовувати в системах домашньої автоматизації в поточному вигляді. Об'єднавши дані разом, ми отримаємо зведену таблицю.

Таким чином, з точки зору основних характеристик найбільше підходить технологія Zig-Bee, він максимально закриває проблеми забезпечення конфіденційності, цілісності і доступності даних в системах з автоматичним сигналізування. Протокол Thread використовує більш сучасні технології, проте недавній випуск основних специфікацій і відсутність додаткової інформації про застосовуваних пристроях не дозволяє говорити про нього, як про повноцінну заміну Zig-Bee, можливо лише в найближчому майбутньому. Протокол WeMo не підходить для створення захищених систем «розумний дім».

2.2 Розгляд технології KeeLoq.

KeeLoq - це запатентований апаратно-виділений блоковий шифр, який використовує нелінійний зворотний зв'язок регістр зсуву (NLFSR). Протокол односпрямованої передачі команд був розроблений Фредеріком Брювером з Nanoteq (Pty) Ltd., криптографічний алгоритм був створений Гідеоном Куном з Університету Преторії, а силіконова реалізація була розроблена Віллемом Смітом з Nanoteq Pty Ltd (Південна Африка) в середині 1980-х. KeeLoq було продано Microchip Technology Inc у 1995 році за 10 мільйонів доларів. Він використовується в кодерах і декодерах «з стрибкоподібною перебудовою коду», таких як NTQ105/106/115/125D/129D, HCS101/2XX/3XX/4XX/5XX та MCS31X2. KeeLoq використовується або використовувався в багатьох системах

віддаленого доступу без ключа такими компаніями, як Chrysler , Daewoo , Fiat , GM , Honda , Toyota , Volvo , Volkswagen Group , Clifford, Shurlok та Jaguar .

Кодери KeeLoq з "стрибкоподібною зміною коду" шифрують заповнені 0 32-бітний блок із шифром KeeLoq для створення 32-бітного "коду перемикання". 32-бітовий вектор ініціалізації лінійно додається (XORed) до 32 молодшим значним бітам ключа до шифрування і після дешифрування.

Шифр KeeLoq приймає 64-бітові ключі та шифрує 32-бітові блоки, виконуючи свій однобітовий NLFSR за 528 раундів. Функція зворотного зв'язку NLFSR: 0x3A5C742E або F(a,b,c,d,e) = d ⊕ e ⊕ ac ⊕ ae ⊕ bc ⊕ be ⊕ cd ⊕ de ⊕ ade ⊕ ace ⊕ abd ⊕ abc.

KeeLoq використовує біти 1, 9, 20, 26 і 31 стану NLFSR як вхідні дані під час шифрування і біти 0, 8, 19, 25 і 30 під час дешифрування. Його вихідні дані лінійно комбінуються (XORed) з двома бітами стану NLFSR (біти 0 і 16 при шифруванні та біти 31 і 15 при дешифруванні) і з бітом ключа (біт 0 стану ключа при шифруванні та біт 15 зі стан ключа при розшифровці) і передається назад у стан NLFSR кожному етапі.

Для простоти індивідуальні реалізації «стрибкоподібної зміни коду» зазвичай не використовують одноразові криптографічні номери або мітки часу . Це робить протокол уразливим для атак з повторенням : наприклад, заглушивши канал під час перехоплення коду, злодій може отримати код, який можна буде використовувати на пізнішому етапі. Подібний «код-грабер», хоч і цікавий теоретично, мабуть, не так широко використовується викрадачами автомобілів.

Детальний опис недорогого прототипу пристрою, розробленого та побудованого Самі Камкаром для цієї техніки з'явилася в 2015 році. Пристрій розміром з гаманець можна було заховати на замкненому автомобілі або поруч із ним, щоб отримати єдиний код доступу без ключа, який буде використаний пізніше для розблокування автомобіля. Пристрій передає сигнал глушіння, щоб заблокувати прийом автомобілем сигналів ковзного коду від брелка власника, одночасно записуючи ці сигнали від обох його двох спроб, необхідних розблокування автомобіля. Записаний перший код передається автомобілю лише

тоді, коли власник робить другу спробу, тоді як записаний другий код зберігається для використання у майбутньому. Було оголошено про демонстрацію DEF CON 23.

Криптоаналіз

KeeLoq вперше було проаналізовано Андрієм Богдановим, який використовував метод «ковзної середньої» і ефективні лінійні наближення. Микола Куртуа атакував KeeLoq, використовуючи метод «ковзної середньої» і алгебраїчні методи. Атаки Богданова і Куртуа не представляли загрози актуальним реалізаціям алгоритму, які, найімовірніше, більш уразливі для «брутфорса» ключового простору.

Окрема реалізація «плаваючого коду» також часто вразлива для атаки з повторенням відправки пакетів, яка створює перешкоди на каналі, перериває і захоплюючи сам код і надалі збільшуючи час виконання в 4 рази від стандартного часу. Ця вразливість KeeLoq дозволила створити так звані «грабери», популярні у викрадачів, які використовують мікросхеми FPGA для перебору основного ключа KeeLoq.

У 2007 році дослідники із групи COSIC університету в місті Левен (Бельгія), у співпраці з колегами з Ізраїлю, виявили новий спосіб атаки на систему. Використовуючи деталі алгоритму, які витекли в широкі маси в 2006 році, дослідники почали вивчати вразливі місця алгоритму. Після визначення частини ключа, що відповідає за певні моделі автомобіля, унікальний біт ключа може бути зламаний при перехопленні синхронізації ключа і автомобіля. Методи шифруванні та дешифрування відображені на рисунках 2.3 та 2.4.

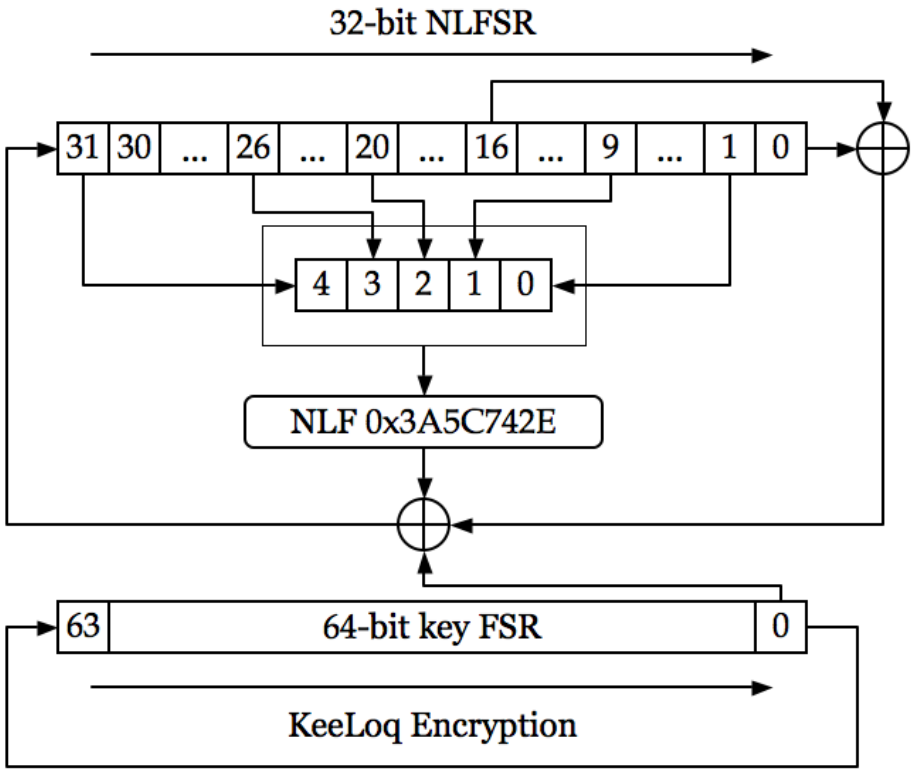

Рисунок 2.3 – Шифрування KeeLoq

Приклади реалізації алгоритму на мові С:

```
# define KeeLoq_NLF		0x3A5C742E
# define bit(x,n)		(((x)>>(n))&1)
# define g5(x,a,b,c,d,e)
(bit(x,a)+bit(x,b)*2+bit(x,c)*4+bit(x,d)*8+bit(x,e)*16)

u32 KeeLoq_Encrypt (const u32 data, const u64 key){
	u32	x = data, r;
	for (r = 0; r < 528; r++)
		x =
(x>>1)^((bit(x,0)^bit(x,16)^(u32)bit(key,r&63)^bit(KeeLoq_NLF,g5(x,1,9,20,26,31))
)<<31);
	return x;
}
```

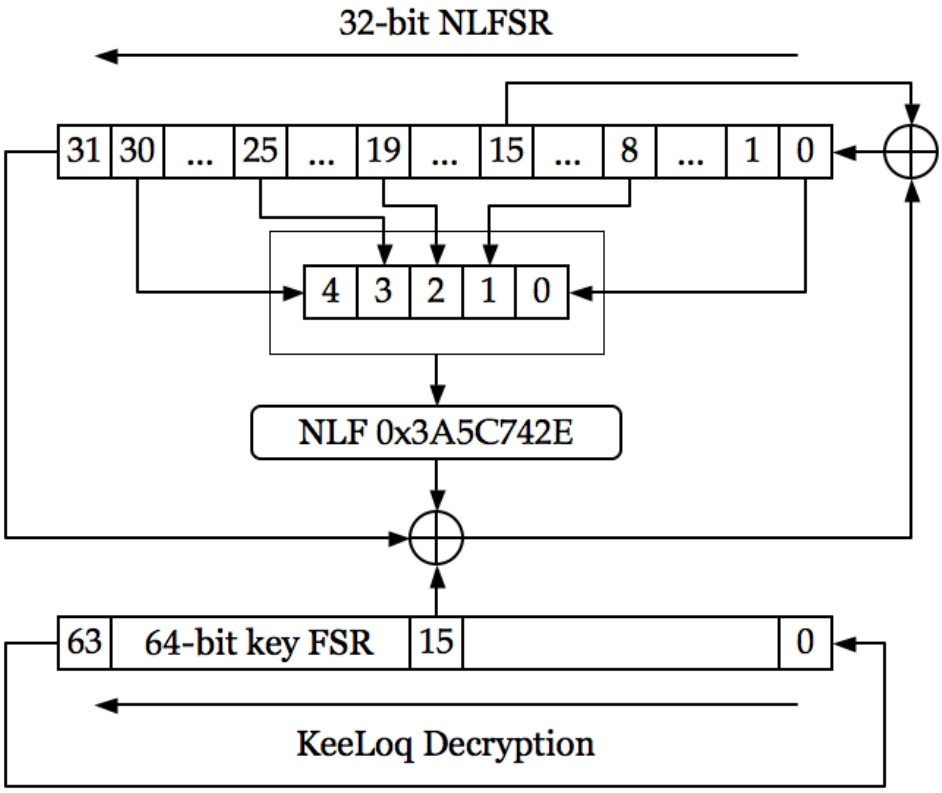

Рисунок 2.4 – Дешифрування KeeLoq

Приклади реалізації алгоритму на мові С:

```
u32 KeeLoq_Decrypt (const u32 data, const u64 key){
        u32    x = data, r;
        for (r = 0; r < 528; r++)
                x = (x<<1)^bit(x,31)^bit(x,15)^(u32)bit(key,(15-
r)&63)^bit(KeeLoq_NLF,g5(x,0,8,19,25,30));
        return x;
}
```

Способи атаки на KeeLoq

Існує чотири способи атаки на шифр KeeLoq: Слайд атака, кореляційний підхід, лінійний крок і атака по іншим каналах.

Слайд атака

Вперше такий тип атаки запропонували Д.Вагнер (David Wagner) і А.Бірюков(Alex Biryukov). Вона застосовується, переважно, до, багатораундових кодів, кожен раунд яких являє собою складне перетворення вихідного блоку з

використанням лише одного ключа. Ключ може повторюватися, так і бути різним для кожного раунду. Важливим є те, що раунди повинні бути ідентичні і легко оборотні.

На першому етапі необхідно набрати близько $2n/2$ (де n - довжина вгадуваного ключа в бітах) пар відкритий зашифрований текст. Цього виявляється достатньо, згідно парадоксу днів народжень, щоб зі значною вірогідністю наткнутися на ―slide pairs.

Далі (M,C) – одна з таких пар. F – функція перетворення раунду. Суть методу: якщо (M',C') така, що P'= F(K,M) і C'= F(K,C), K і є шуканий ключ рисунок 2.5.

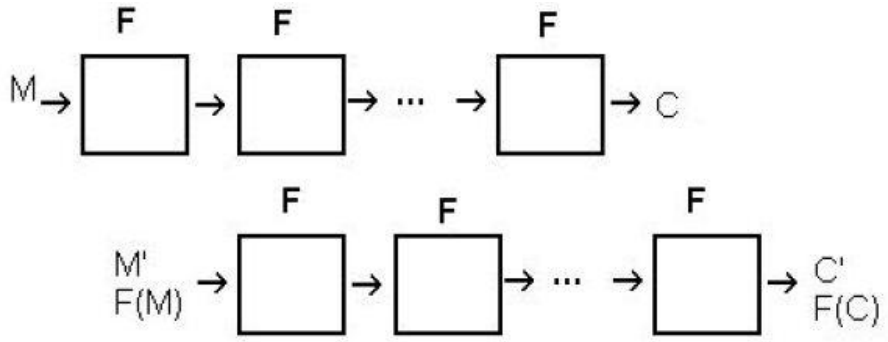

Рисунок 2.5 – Слайд атака

Для Keeloq оборотні перші 32 біта. Отже, частина ключа (<=32b) можна визначити таким методом.

Кореляційний підхід

Для подальшого визначення ключа можливе використання властивості NLF-Cor(F)=1.

Виявляється, що для рівномірно розподілених $x2,x3,x4$ має місце наступне:

– Pr {NLF($x4$, $x3$, $x2$, $x1$, $x0$) = 0 | $x0 \oplus x1 = 0$} = 5/8

– Pr {NLF($x4$, $x3$, $x2$, $x1$, $x0$) = 1 | $x0 \oplus x1 = 1$} = 5/8

Використовуючи це і аппроксимуючи NLF по ймовірності, можна домогтися визначення чергової частини ключа.

Лінійний крок

Останні 16 біт ключа визначаються досить просто якщо відомі всі попередні. Ґрунтуючись на тому, що якщо ми знаємо повністю 48 стан в циклі, то можемо записати:

$y^{64}16=NLF(y^{48}31,y^{48}26,y^{48}20,y^{48}9,y^{48}1)\oplus y^{48}0\oplus y^{48}16\oplus k48$

Звідси знаходимо - $k48$. Абсолютно аналогічно $k49...k63$. Андрій Богданов оцінює складність всіх трьох атак укупі ~2^{52}.

Атака по стороннім каналах

У березні 2008 року дослідники з кафедри «вбудовуваної безпеки» Рурського університету міста Бохум (Німеччина) представили повний злом дистанційного керування ключем, заснований на технології KeeLoq RFID. Їх атака працює на всіх відомих автомобілях і системах розподілу контролю доступу, що використовують шифр Keeloq. «Бохумська» атака дозволяє відновлювати секретні криптографічні ключі, вбудовані в приймач, так і в пульт дистанційного управління. Їх спосіб заснований на управлінні енергоспоживанням пристрою під час шифрування. Використовуючи так звану «атаку по сторонніх каналах» до розподілу живлення, дослідники можуть отримати потрібний ключ від виробників приймача, який можна використовувати як «майстер-ключ» для генерації потрібного ключа для дистанційного пульта певного виробника.

На відміну від криптографічних атак, описаних вище, які вимагають перебору порядку 65536 пар «текст-шифр» і кілька днів розрахунку на персональному комп'ютері для відновлення ключа, атака по іншим каналам може бути застосована до так званого режиму «плаваючого коду» KeeLoq, який широко використовується для систем дистанційного ключа» (гаражі, автомобілі).

Найсерйознішим наслідком атаки по сторонніх каналах, є те, що атакуючий, вивчивши раніше головний ключ системи, може скопіювати будь-який законний кодувальник і перехоплювати тільки два необхідних повідомлення від цього датчика на відстані 100 метрів. Інша атака дозволяє скидати внутрішній

лічильник одержувача (двері гаража, автомобіля), який позбавляє законного користувачі можливості відкривати двері.

Мікрочип на базі KeeLoq IC представлений в 1996 році, використовує 60-бітне початкове зміщення. Якщо використовується 60-бітне початкове зміщення, то зловмисникові потрібно приблизно 100 днів на обробку на спеціальному обладнанні для «брутфорса», перш ніж система буде зламана.

2.3 Розгляд технології LoRa.

Абревіатурою LoRa (Long Range) позначають вид модуляції, тобто рівень L1 по моделі OSI. Протокол канального рівня носить ім'я LoRaWAN. Але найчастіше «Лорою» називають сукупну систему, яка використовує LoRa на фізичному і LoRaWAN на канальному рівні.

Архітектура була спочатку розроблена Cycleo у Франції, але потім придбана Semtech Corporation (французьким виробником електроніки змішаних сигналів) в 2012 р. за 5 мільйонів доларів готівкою. Альянс LoRa був сформований в березні 2015 р. Альянс є органом стандартизації для специфікації і технології LoRaWAN. Туди також входить процес дотримання і сертифікації для забезпечення сумісності і відповідності стандарту. Альянс підтримується IBM, Cisco і більш ніж 160 іншими учасниками.

LoRaWAN запрацювала в Європі з розгортанням мереж KPN, Proximus, Orange, Bouygues, Senet, Tata і Swisscom. Оскільки LoRa є нижньою частиною стека, вона був прийнята в конкуруючих архітектурах в LoRaWAN. Наприклад, SymphonyLink - це рішення LPWAN від Link Labs на основі LoRaPHY, що використовує восьмиканальну базову станцію з субгігагерцами для промислових і муніципальних розгортань IoT. Ще одним конкурентом, що використовує LoRa, є Haystack, який виробляє систему DASH7. DASH7 - повний мережевий стек на LoRaPHY (а не тільки рівень MAC).

Фізичний рівень LoRa.

LoRa являє собою фізичний рівень мережі LoRaWAN. Вона керує модуляцією, потужністю, приймачем і передавальними радіостанціями, а також формує сигнали.

Архітектура заснована на наступних діапазонах в просторі SM без ліцензування:

− 915 МГц - в США з обмеженнями потужності, але без обмеження робочого циклу;

− 868 МГц - в Європі з 1% -им і 10% -им робочим циклом;

− 433 МГц - в Азії.

Похідним від Chirp Spread Spectrum (CSS) є метод модуляції, що використовується в LoRa. CSS балансує швидкість передачі даних з чутливістю в смузі фіксованого каналу. CSS був вперше використаний в 1940-х рр. для військового довгохвильового зв'язку з використанням модульованих імпульсів чірпа для кодування даних і був визнаний особливо стійким до перешкод, ефектів Доплера і багатопроменевого розповсюдження. Чірпи - це синусоїдальні хвилі, які з часом збільшуються або зменшуються. Оскільки вони використовують весь канал для зв'язку, вони відносно надійні в плані перешкод. Ми можемо уявити сигнали чірпів зі збільшенням або зменшенням частот (звук, як поклик кита). Частота передачі бітів - бітрейт, де LoRa є функцією швидкості чірпа і швидкості передачі символів. Бітрейт представлений R, коефіцієнт розширення S, смуга пропускання B. Тому бітрейт (біт/с) може варіюватися від 0,3 до 5 Кбіт/с і виводиться як:

$$R_b = S \times \frac{1}{\left[\frac{2^S}{B}\right]}.$$

Така форма модуляції допускає малу потужність для великих відстаней, як показали військові. Дані кодуються з використанням збільшення або зменшення частоти, і кілька передач можуть бути відправлені з різною швидкістю передачі даних на тій же частоті. CSS дозволяє отримувати сигнали на рівні 19,4 дБ нижче рівня шуму, використовуючи FEC. Група також поділяється на кілька

піддіапазонів. LoRa використовує канали 125 кГц і виділяє шість каналів 125 кГц і стрибкоподібне пересилання псевдовипадкових каналів. Кадр буде передаватися з певним коефіцієнтом розширення. Чим вище коефіцієнт розширення, тим повільніше передача, але тим довший діапазон передачі. Кадри в LoRa є ортогональними, що означає, що кілька кадрів можуть відправлятися одночасно, поки кожен відправляється з іншим коефіцієнтом розширення. Всього є шість різних коефіцієнтів розширення (від SF = 7 до SF = 12).

Типовий пакет LoRa містить преамбулу, заголовок і корисне навантаження від 51 до 222 байт.

Мережі LoRa мають потужну функцію, звану Adaptive Data Rate (ADR). По суті, це дозволяє динамічно масштабувати ємність, ґрунтуючись на щільності вузлів і інфраструктурі. ADR контролюється управлінням мережею в хмарі. Вузли, близькі до базової станції, можуть мати більш високу швидкість передачі даних через достовірность сигналу. Вузли, що знаходяться в безпосередній близькості, можуть передати дані і звільнити свою смугу пропускання і швидко увійти в стан сну в порівнянні з віддаленими вузлами, які передають з меншою швидкістю.

У таблиці 2.12 описані властивості висхідної і низхідної лінії зв'язку.

Таблиця 2.12 – Стандарти IEEE 802.11

Властивість	Висхідне з’єднання	Низхідне з’єднання
Модуляція	CSS	CSS
Втрати радіоканалу	156 дБ	164 дБ
Швидкість передачі (адаптивна)	Від 0.3 до 5 кб/с	Від 0.3 до 5 кб/с
Розмір повідомлення на корисне навантаження	0-250 байт	0-250 байт
Тривалість повідомлення	Від 40 мс до 1.2 с	Від 20 до 160 мс

Продовження Таблиці 2.12 – Стандарти IEEE 802.11

Енергія, витрачена на повідомлення	$E_{tx} = 1.2s * 32mA = 11uAh$ При повній чутливості прийому $E_{tx} = 40ms * 32mA = 0.36uAh$ При мінімальній чутливості прийому	$E_{tx} = 160ms * 32mA = 0.5uAh$

Рівень MAC LoRaWaN.

LoRaWAN представляє MAC, який знаходиться поверх LoRaPHY. MACадреса LoRaWAN є відкритим протоколом, в той час як PHY закритий. Існує три протоколи MAC, які є частиною рівня каналу передачі даних. Всі три балансують затримки і використання енергії. Клас А є найкращим для зменшення енергоспоживання при максимальній затримці. Клас В знаходиться між класом А і класом С. Клас С має мінімальну затримку, але найвищий рівень використання енергії.

Двонаправлені кінцеві пристрої «класу А» (Bi-directional end-devices, Class A). Кінцеві пристрої «класу А» дозволяють організувати двонаправлений обмін. Причому зв'язок може ініціювати тільки кінцевий пристрій, після чого виділяються два тимчасових вікна, протягом яких очікується відповідь від мережі. Інтервал передачі планується кінцевим пристроєм на основі власних потреб в зв'язку з невеликими випадковими тимчасовими флуктуаціями (протокол типу ALOHA). Кінцеві пристрої «класу А» застосовуються в додатках, де передача даних від мережі можлива тільки як відповідна реакція на отримання даних від кінцевого пристрою і потрібно максимальний час роботи від автономного джерела живлення.

Двонаправлені кінцеві пристрої «класу Б» (Bi-directional end-devices, Class B) на додаток до функцій пристроїв «класу А», відкривають додаткові вікна прийому за розкладом. Для того, щоб відкрити вікно прийому, кінцеве пристрій

синхронізується за спеціальними сигналами від шлюзу (по маяках - Beacon). Це дозволяє мережі знати час, коли кінцевий пристрій готовий приймати дані.

Двонаправлені кінцеві пристрої «класу С» з максимальним прийомним вікном (Bi-directional end-devices, Class C). Кінцеві пристрої «класу С» мають майже безперервно відкрите вікно прийому. Приймальне вікно закривається тільки на час передачі даних. Цей тип кінцевих пристроїв підходить для задач, коли необхідно отримувати великі обсяги даних і не потрібна тривала робота від автономного джерела живлення.

Стек протоколу LoRa / LoRaWAN можна візуалізувати так, як показано в таблиці 2.13.

Таблиця 2.13 – Стек протоколів LoRa і LoRaWAN. Порівняння зі стандартною моделлю OSI

<table>
<tr><td colspan="3">Стек протоколів LoRa /LoRaWAN</td><td>Спрощена модель OSI</td></tr>
<tr><td colspan="3">Прикладний рівень</td><td>3. Прикладний рівень</td></tr>
<tr><td colspan="3">Рівень LoRaWAN</td><td rowspan="2">2. Канальний рівень</td></tr>
<tr><td>Клас А</td><td>Клас В</td><td>Клас С</td></tr>
<tr><td colspan="3">Модуляція LoRaPHY</td><td rowspan="4">1. Фізичний рівень</td></tr>
<tr><td colspan="3">LoRaPHY регіональний діапазон ISM</td></tr>
<tr><td>LoRaPHY Європейський діапазон 868 МГц</td><td>LoRaPHY Європейський діапазон 433 МГц</td><td>LoRaPHY Європейський діапазон 915 МГц</td></tr>
</table>

Для безпеки LoRaWAN шифрує дані з використанням моделі AES128. Одна з відмінностей в безпеці від інших мереж - LoRaWAN відокремлює аутентифікацію і шифрування. Аутентифікація використовує один ключ (NwkSKey), а призначені для користувача дані - окремий ключ (AppSKey).

Щоб під'єднатися до мережі LoRa, пристрої відправлять запит JOIN. Шлюз відповість адресою пристрою і маркером аутентифікації. Ключ додатку і мережевого сеансу буде отримано під час процедури JOIN. Цей процес називається Over the Air Activation (OTAA). В якості альтернативи пристрій на основі LoRa може використовувати активацію за допомогою персоналізації. У цьому випадку постачальник/оператор LoRaWAN попередньо розподіляє 32-розрядні мережеві і сеансові ключі, і клієнт повинен замовити план підключення і відповідний набір ключів. Ключі будуть замовлятися у виробника кінцевої точки з ключами, вбудованими в пристрій.

LoRaWAN - це асинхронний протокол на основі ALOHA. Чистий протокол ALOHA був спочатку розроблений в Гавайському університеті в 1968 р. як форма зв'язку з множинним доступом до тих пір, поки не існували такі технології, як CSMA. У ALOHA клієнти можуть передавати повідомлення, не знаючи, чи знаходяться інші клієнти в процесі передачі одночасно. Немає ніяких застережень або методів мультиплексування. Основним принципом є хаб (або шлюз в разі LoRaWAN), який негайно ретранслює отримані пакети. Якщо кінцева точка зауважує, що один з її пакетів не був підтверджений, він буде чекати, а потім повторно передасть пакет. У LoRaWAN колізії виникають тільки в тому випадку, якщо при передачах використовуються одні й ті ж канали та частота поширення.

Підтвердження отримання повідомлень.

Технологія LoRa визначає два типи повідомлень - повідомлення, що вимагає підтвердження отримання та повідомлення без підтвердження. Тип повідомлення - Confirmed (UL / DL) / Unconfirmed (UL / DL), визначається значенням поля MType (MessageType) заголовка MAC рівня.

Якщо відправником повідомлення, що вимагає підтвердження, є кінцевий пристрій (End Node), то мережа підтверджує отримання такого повідомлення всередині вікон прийому, відкритих кінцевим пристроєм відразу після сеансу передачі.

Якщо відправником повідомлення, що вимагає підтвердження, є мережа (LoRa gateway - шлюз), то момент передачі підтвердження визначається кінцевим пристроєм (End Node). Підтвердження може бути послано негайно (в т.ч. в складі порожнього повідомлення), що спрощує логіку функціонування End Node, або в складі чергового повідомлення, що несе корисне навантаження, що скорочує завантаження радіоканалу.

У будь-якому випадку, підтверджується завжди тільки останнє отримане повідомлення. Повідомлення, що є підтвердженням, характеризується встановленим бітом ACK заголовка MAC рівня. Повторна передача підтверджень не передбачена.

Необхідність повторної передачі непідтверджених повідомлень (або його видалення), а також моменти передачі і кількість повторів визначається логікою функціонування мережевого сервера і кінцевого пристрою відповідно. При кожній повторній передачі можливе зниження швидкості потоку даних (data rate), що підвищує перешкодозахищеність. Також передбачена можливість забезпечення параметрів повторної передачі в кінцеві пристрої з боку мережі.

У разі неотримання мережевим сервером встановленого числа підтверджень від кінцевого пристрою, дане кінцеве пристрій може бути промарковано як недоступне (unreachable) аж до отримання від нього будь-якого першого вхідного повідомлення.

3. Вибір та обґрунтування алгоритму функціонування та структурної схеми системи

В розділі описані головні кроки та етапи роботи.

3.1 Алгоритм роботи

Блок-схеми алгоритму роботи охоронної системи зображені на рисунку 3.1, рисунку 3.2, рисунку 3.3.

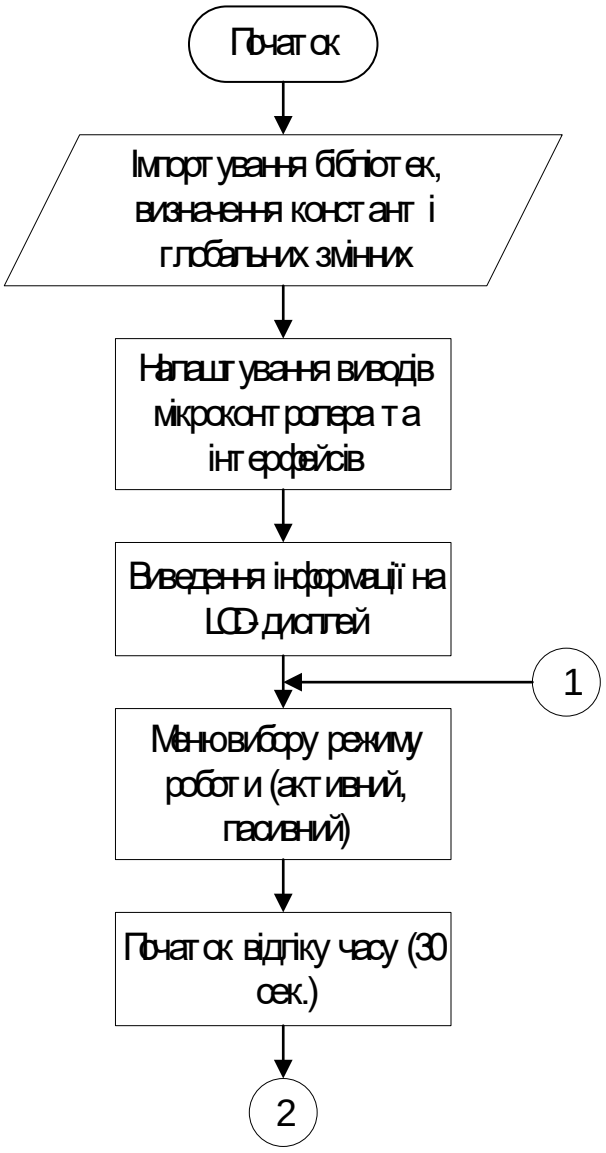

Рисунок 3.1 – Блок-схема алгоритму роботи охоронної системи

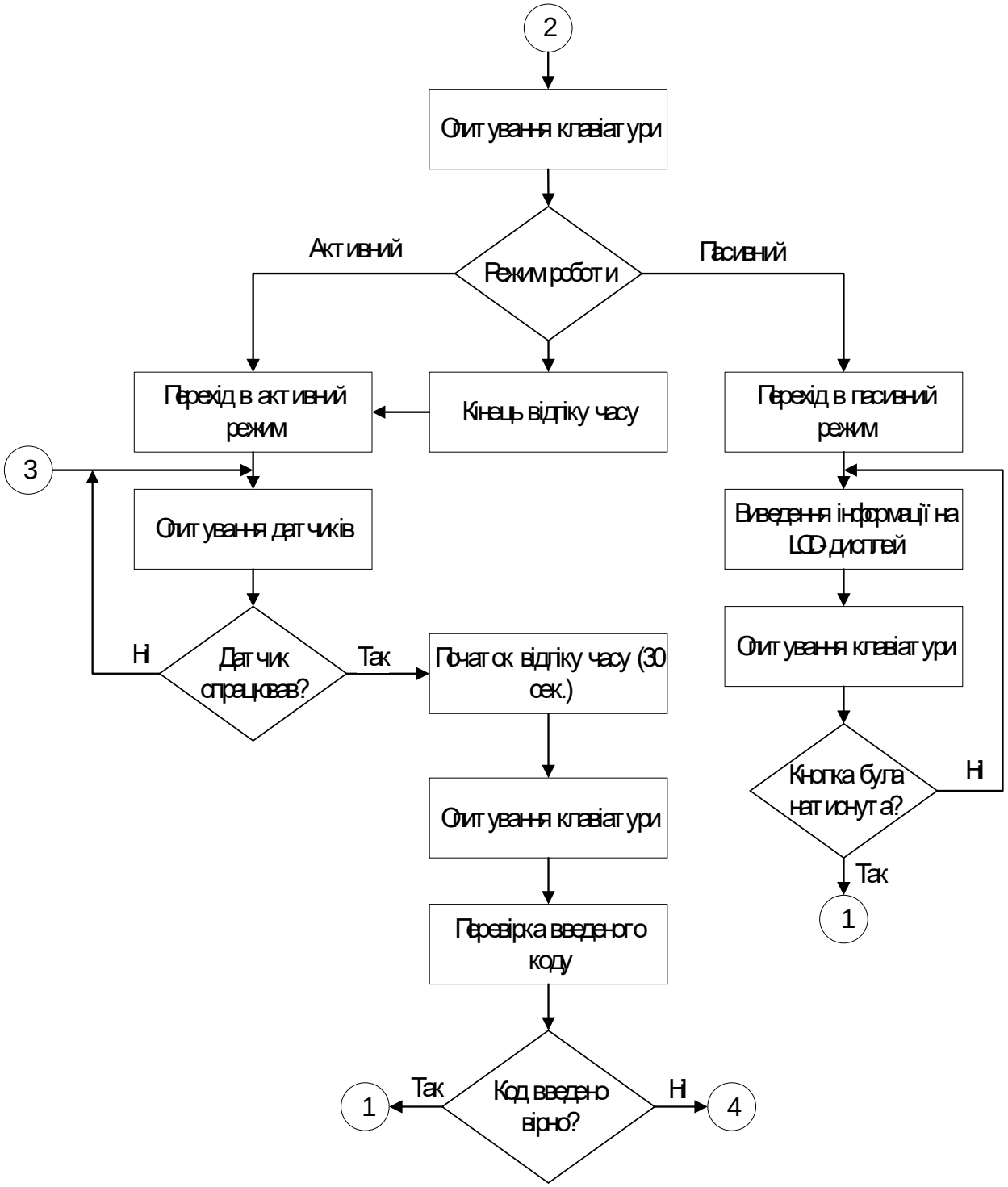

Рисунок 3.2 – Блок-схема алгоритму роботи охоронної системи (продовження)

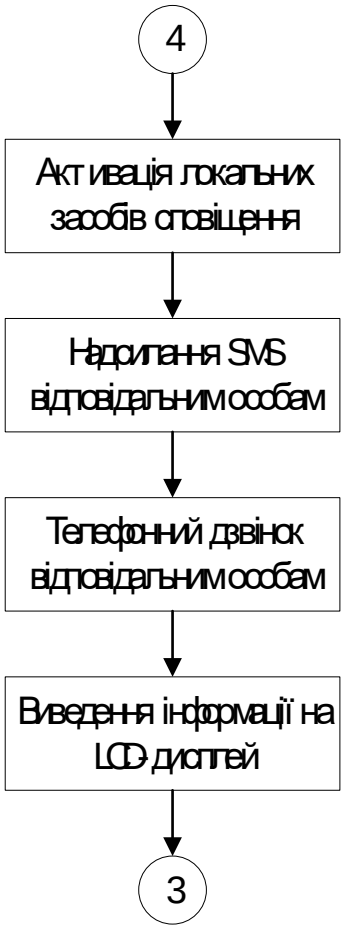

Рисунок 3.3 – Блок-схема алгоритму роботи охоронної системи (продовження)

Програма починається з імпорту необхідних бібліотек та ініціалізації режимів роботи виводів мікроконтролера. Блок-схема алгоритму роботи програми складається з кількох перевірок, три з яких пов’язані з опитуванням та перевіркою показів давачів, а дві – для перевірки стану клавіатури.

З метою реалізації принципу модульності та підвищення зручності, програма поділена на такі частини:

1) блок ініціалізації;

2) блок опитування та зміни станів системи;

3) блок обробки станів.

Відповідно до завдання охоронна система може перебувати у чотирьох режимах:

1) пасивний режим: стан давачів ігнорується, використання приміщення відбувається у звичному режимі;

2) режим охорони: усі давачі активні, приміщення знаходиться під охороною;

3) режим тривоги: спрацював давач руху або відкриття дверей, у користувача є 30 секунд, для того щоб ввести секретний код;

5) режим спрацювання: активуються засоби сповіщення.

Головна програма, яка виконується в циклі починається з процесу зчитування значень на усіх виводах мікроконтролера, до яких під'єднані давачі. Це цифрові входи для клавіатури, а також аналогові входи. Після запису усіх даних у відповідні змінні починається процес їх опрацювання. Для зміни режиму роботи системи з «пасивний» в режим «активний» необхідно натиснути необхідну клавішу згідно відображеній на дисплеї інформації, після цього залишити приміщення за 30 секунд. За цей проміжок часу мікроконтролер припинить виконувати свої функції для того, щоб користувач міг встигнути вийти з приміщення і щоб не відбулося спрацювання сигналізації.

В ПЗ є частина коду, яка відповідає за налагодження. Організовано це шляхом передачі через послідовний порт значення змінних, в які записані дані від давачів та інформація про стан системи. Це дає змогу слідкувати за зміною режимів системи в динаміці.

Наступною частиною коду є блок опрацювання режимів роботи системи. Цей код призначений для того, щоб виконати дії, які відповідають тому чи іншому режиму роботи. В цьому коді виконуються певні дії в залежності від визначеного набору умов:

1) Охорона – на виводи, до яких під'єднаний модуль звукової сигналізації та, подається низький рівень напруги через те, що в цьому режимі система не повинна їх вмикати.

2) Тривога – початок часового відліку. Якщо за визначений період часу не буде введений вірний код, то система змінить режим роботи на «спрацювання».

3) Спрацювання – на виводи, до яких під'єднані засоби сповіщення подається високий рівень напруги. Застосовуючи стандартну бібліотеку

здійснюється генерація команди для надсилання SMS-повідомлення з наперед визначеним текстом та здійснення дзвінка на заданий номер абонента.

Після виконання цієї частини коду керування переходить на початок циклу. Таким чином реалізовується постійний моніторинг стану приміщення системою охоронної.

3.2 Структурна схема системи

Структурна схема представлена на рисунку 3.2. На ній зображені головні структурні блоки та схема їх комутації.

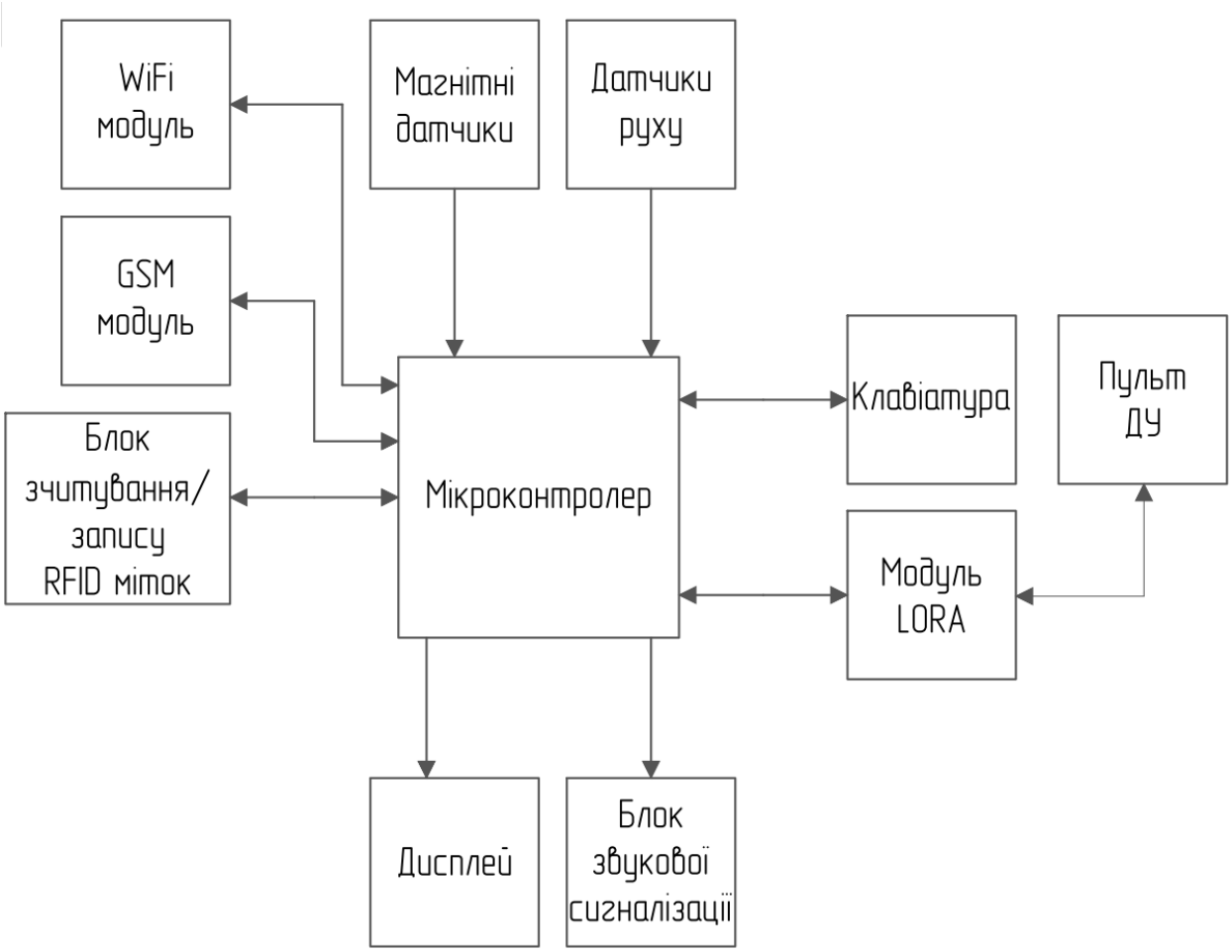

Рисунок 3.2 – Структурна схема

Структурна схема складається з наступних блоків:

1) Мікроконтролер – слугує центром системи, виконує функції керування периферійними пристроями;

2) WiFi модуль – в даній системі використовується для моніторингу за станом системи;

3) GSM модуль – використовується як модуль оповіщення відповідальних осіб, про стан системи, в GSM мережі;

4) Блок зчитування /запису RFID міток – цей блок використовується для ідентифікації об'єктів за допомогою RFID-технологій;

5) Сенсорний вузол – блок який об’єднує в собі магнітні датчики та датчики руху;

6) Блок виводу інформації, локального оповіщення – блок виводу інформації на дисплей та звукової сигналізації;

7) Блок локального управління – клавіатурний блок;

8) Блок дистанційного управління – дистанційний зв'язок за допомогою технології LoRa і можливість керування з використанням пульта ДУ.

4. Розробка функціональної схеми

Функціональна схема представлена на рисунку 4.1.

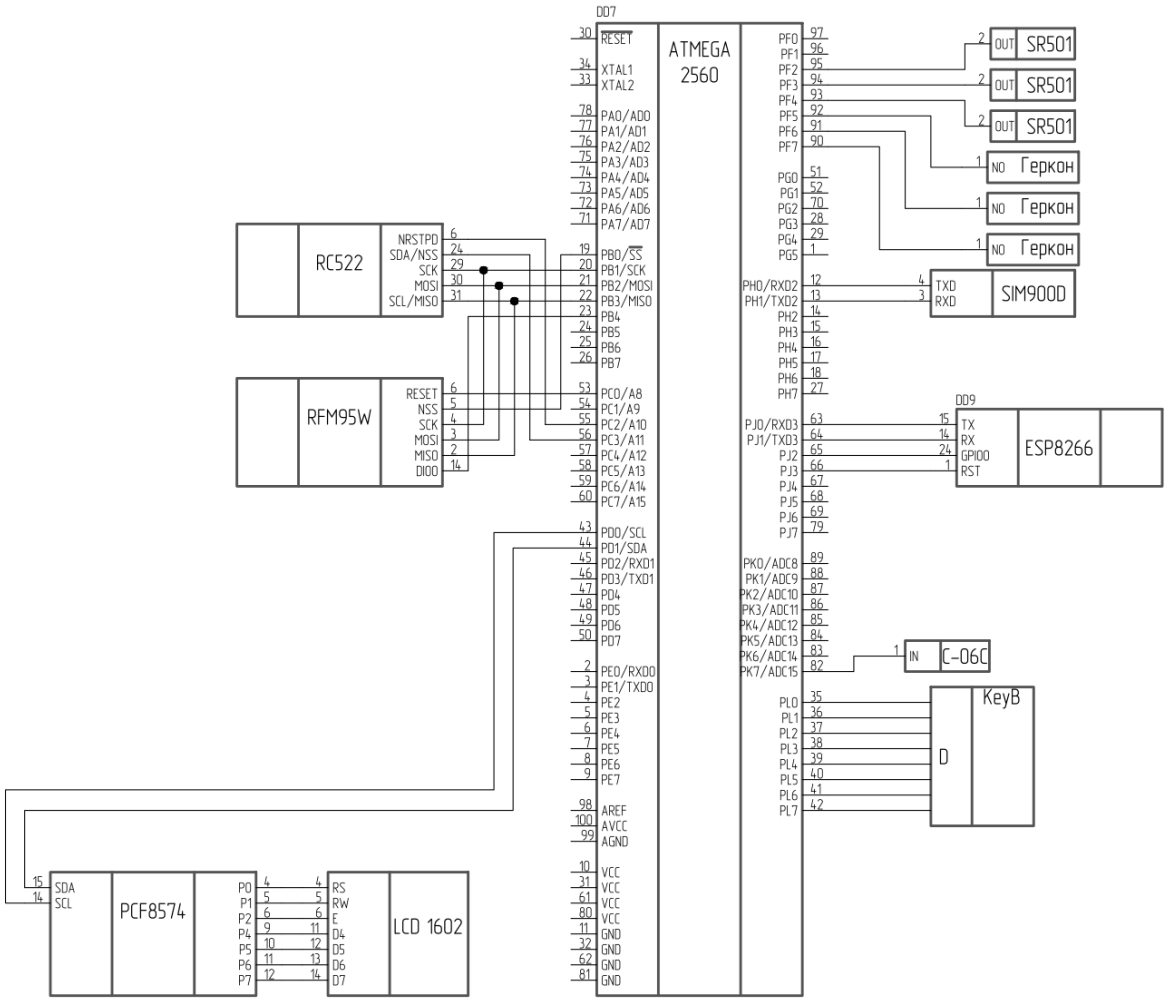

Рисунок 4.1 – Функціональна схема

Функціональна схема системи складається з ряду блоків, які співпрацюють для забезпечення різних функцій та операцій. Ось опис функцій та взаємодій кожного блоку:

1) Мікроконтролер:
   - Функція: Виконання функцій керування периферійними пристроями та координація роботи системи.
   - Взаємодія: Отримання та обробка сигналів від інших блоків, відправлення команд периферійним пристроям.

2) WiFi модуль:
   - Функція: Моніторинг за станом системи та можливість передачі даних через WiFi мережу.
   - Взаємодія: Збір інформації та передача її мікроконтролеру для подальшого аналізу.
3) GSM модуль:
   - Функція: Модуль оповіщення відповідальних осіб про стан системи через GSM мережу.
   - Взаємодія: Отримання сигналів від мікроконтролера та надсилання повідомлень адміністраторам чи відповідальним особам.
4) Блок зчитування/запису RFID міток:
   - Функція: Ідентифікація об'єктів за допомогою RFID-технологій.
   - Взаємодія: Обмін інформацією з мікроконтролером для визначення стану та ідентифікації об'єктів.
5) Сенсорний вузол:
   - Функція: Об'єднання магнітних датчиків та датчиків руху для виявлення подій та руху в зоні моніторингу.
   - Взаємодія: Передача сигналів про виявлені події мікроконтролеру.
6) Блок виводу інформації, локального оповіщення:
   - Функція: Виведення інформації на дисплей та звукова сигналізація для локального оповіщення користувача.
   - Взаємодія: Отримання сигналів від мікроконтролера для відображення та передачі звукових сигналів.
7) Блок локального управління (клавіатурний блок):
   - Функція: Надання можливості користувачеві локально керувати системою за допомогою клавіатури.
   - Взаємодія: Введення команд та передача їх мікроконтролеру.

8)Блок дистанційного управління:

- Функція: Дистанційний зв'язок за допомогою технології LoRa та можливість керування з використанням пульта ДУ.
- Взаємодія: Приймання команд від пульта ДУ та передача їх мікроконтролеру для відповідної реакції.

Ця функціональна схема визначає основні завдання та взаємозв'язки між блоками системи, створюючи комплексну та узгоджену систему контролю та управління.

5. Вибір елементної бази та розробка принципових електричних схем блоків

5.1 Мікроконтролерний блок

При розробці даної системи було обрано мікроконтроллер Atmel ATmega2560, який зображено на рисунку 5.1.

Рисунок 5.1 – Мікроконтролер Atmel ATmega2560

Вибір даного мікроконтролера зумовлено підтримкою всіх необхідних інтерфейсів та функцій, достатньою продуктивністю, малою споживчою потужністю та наявністю необхідних периферійних пристроїв.

Таблиця 5.1 – Характеристики мікроконтролера ATmega2560

Параметр	**Значення**
Робоча напруга	5В
Напруга живлення (рекомендований)	7-12В
Напруга живлення (граничне)	6-20В
Цифрові входи / виходи	54 (з яких 15 можуть використовуватися в якості ШІМ-виходів)
Аналогові входи	16
Максимальний струм одного виведення	40 мА
Максимальний вихідний струм виводу 3.3V	50 мА
Flash-пам'ять	256 КБ з яких 8 КБ використовуються завантажувачем
SRAM	8 КБ
EEPROM	4 КБ
Тактова частота	16 МГц

У мікроконтролері ATmega2560 присутній такий набір периферійних пристроїв:

- Одинадцять 8-и бітних портів вводу виводу загального призначення;
- Два 8-ми бітних лічильника з індивідуальними предільниками та режимом порівняння та 4-а ШІМ каналами;
- Чотири 16-и бітних лічильника з індивідуальними предільниками та режимом порівняння та режимом захвату та 12-а ШІМ каналами;

- Лічильник реального часу із індивідуальним джерелом тактових сигналів;
- Аналоговий компаратор;
- 16-и канальний, 10-бітний АЦП;
- Чотири інтерфейси USART;
- SPI інтерфейс із режимами головного та веденого;
- TWI (I^2C) інтерфейс;
- Сторожовий таймер;
- Програмовані зовнішні переривання .

Розширена структура мікроконтролерів ATmega сімейства AVR представлена на рис. 5.2. До складу мікроконтролерів ATmega сімейства AVR входить центральний процесорний пристрій, який складається із арифметикологічного пристрою, різних типів пам'яті та периферійних пристроїв.

Центральний процесорний пристрій включає арифметико-логічний пристрій, в якому реалізовані всі схеми по арифметичній та логічній обробці даних. Математичні на логічні дії виконуються над даними, що розташовуються у одному або декількох із 32 регістрів загального призначення.

Центральний процесорний пристрій має 32 8-и бітні регістри загального призначення (r0-r31), які зібрані в так званий «регістровий файл». Останні 6 регістрів (r26-r31) зібрані в регістрові пари X, Y, Z для отримання 16-и бітних регістрів. 16-и бітні регістри використовуються в ряді команд, як правило в командах непрямої адресації пам'яті.

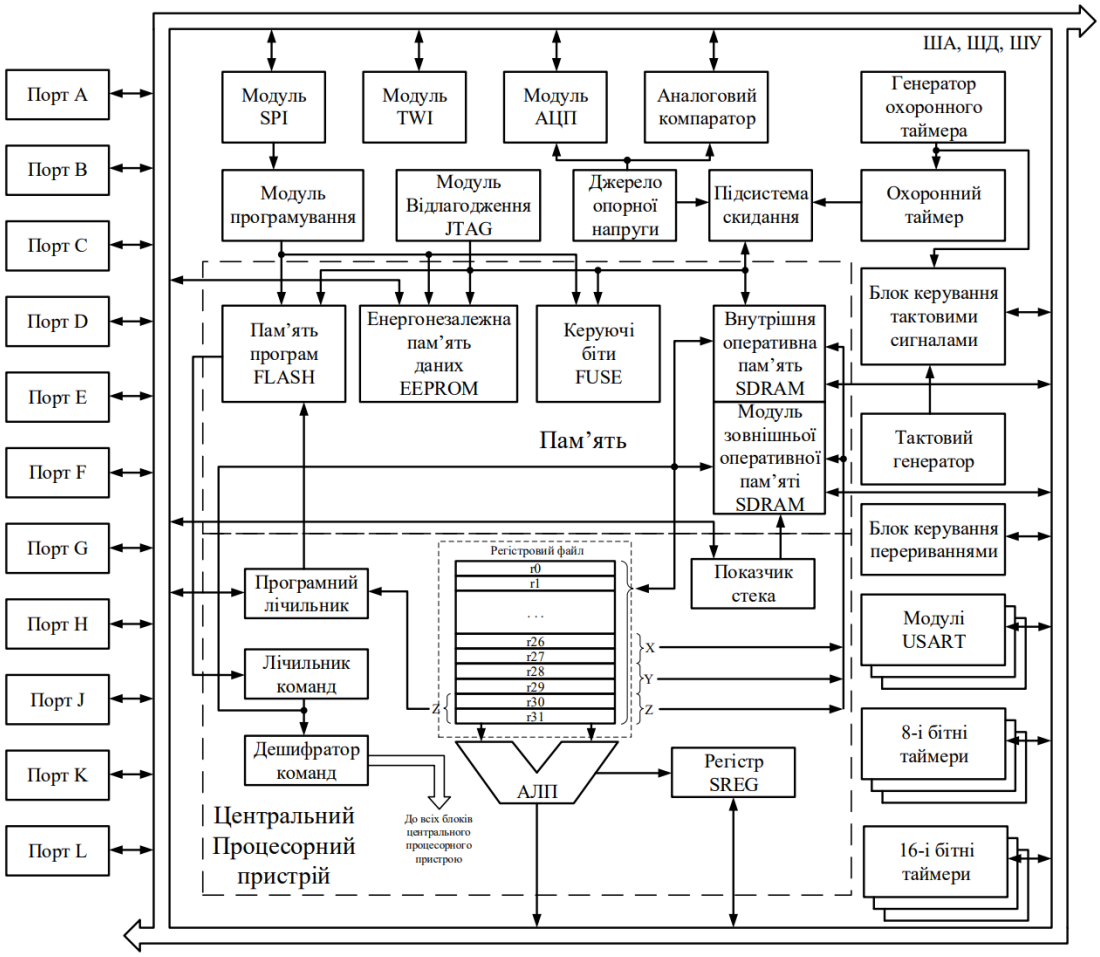

Рисунок 5.2 – Структура мікроконтролера ATmega 2560

Враховуючи велику кількість внутрішніх периферійних пристроїв та обмежену кількість виводів мікросхеми мікроконтролера, один і той самий вивід може використовуватися при роботі різних внутрішніх периферійних пристроїв. Базовим призначенням більшості виводів мікросхем мікроконтролерів ATmega сімейства AVR є виводи портів вводу/виводу загального при значення. При роботі на ці виводи інших внутрішніх периферійних пристроїв говорять про альтернативні функції виводів. Принципова схема мікроконтролера ATmega 2560 представлена на рисунку 5.3.

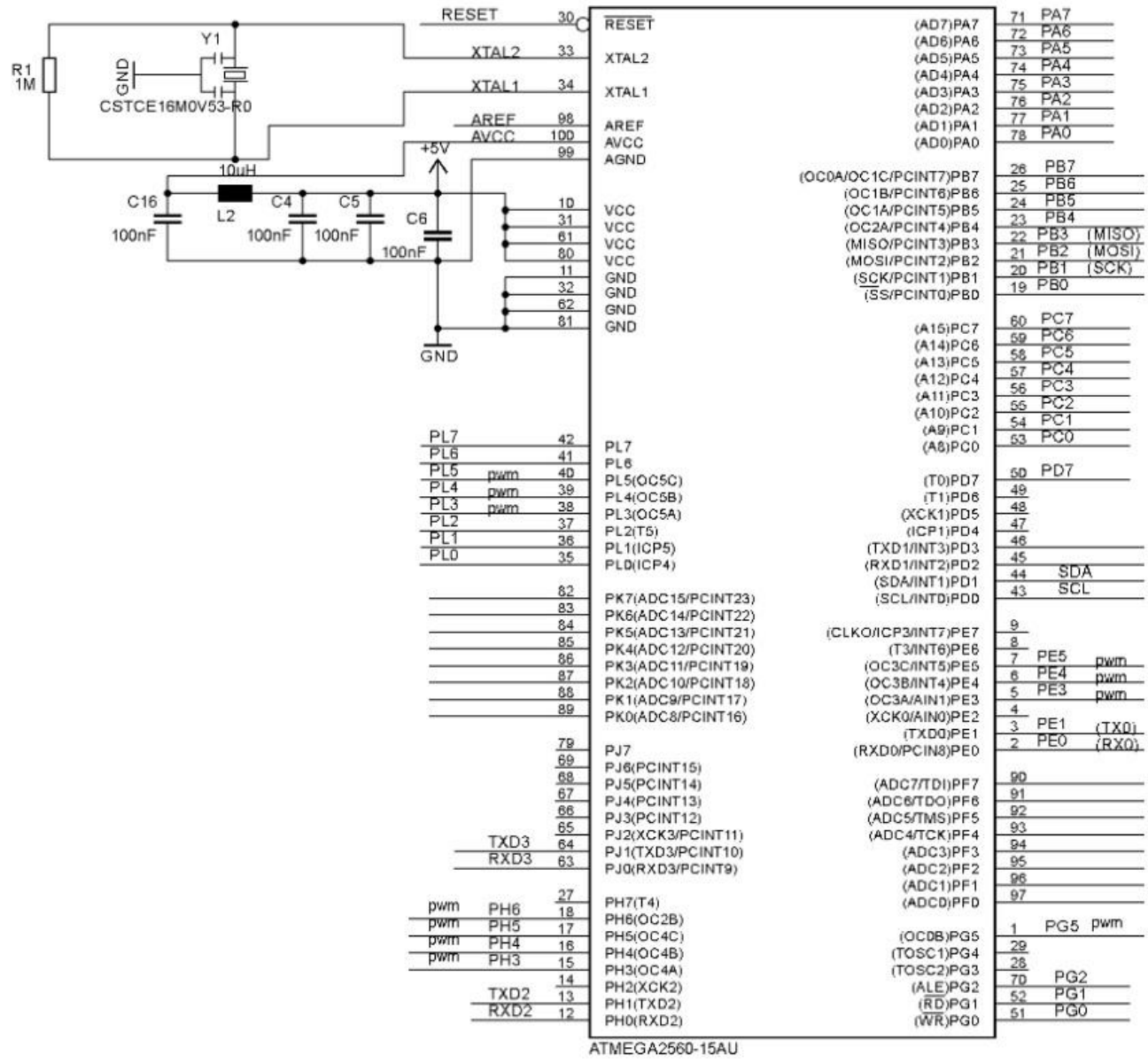

Рисунок 5.3 – Принципова схема мікроконтролера ATmega 2560

Загальна інформація про призначення пінів для ATmega2560:

Цифрові піни:

- PORTA (PA0 - PA7): Цифрові входи/виходи 0-7.
- PORTB (PB0 - PB7): Цифрові входи/виходи 8-15.
- PORTC (PC0 - PC7): Цифрові входи/виходи 16-23.
- PORTD (PD0 - PD7): Цифрові входи/виходи 24-31.
- PORTE (PE0 - PE7): Цифрові входи/виходи 32-39.

- PORTF (PF0 - PF7): Цифрові входи/виходи 40-47.
- PORTG (PG0 - PG7): Цифрові входи/виходи 48-55.
- PORTH (PH0 - PH7): Цифрові входи/виходи 56-63.
- PORTJ (PJ0 - PJ7): Цифрові входи/виходи 64-71.
- PORTK (PK0 - PK7): Цифрові входи/виходи 72-79.
- PORTL (PL0 - PL7): Цифрові входи/виходи 80-87.

Аналогові піни:

- ADC0 - ADC15 (PF0 - PF7, PK0 - PK7): Аналогові входи.

Живлення та інші піни:

- VCC, GND: Живлення та земля.
- AREF: Напруга опорного входу для аналого-цифрового перетворення.

Піни для інтерфейсів зв'язку:

- RX0, TX0: Серійний порт 0 (USART0).
- RX1, TX1: Серійний порт 1 (USART1).
- RX2, TX2: Серійний порт 2 (USART2).
- RX3, TX3: Серійний порт 3 (USART3).
- MISO, MOSI, SCK, SS: SPI (Serial Peripheral Interface).
- SCL, SDA: I2C (Inter-Integrated Circuit).

Інші піни:

- RESET: Сигнал скидання мікроконтролера.
- XTAL1, XTAL2: Піни для підключення кварцевого резонатора або генератора годинника.

5.2 Розробка Wi-Fi блоку

В якості Wi-Fi модулю було обрано трансівер ESP8266, підключення модулю до мікроконтролера ATmega 2560 зображена на рисунку 5.4.

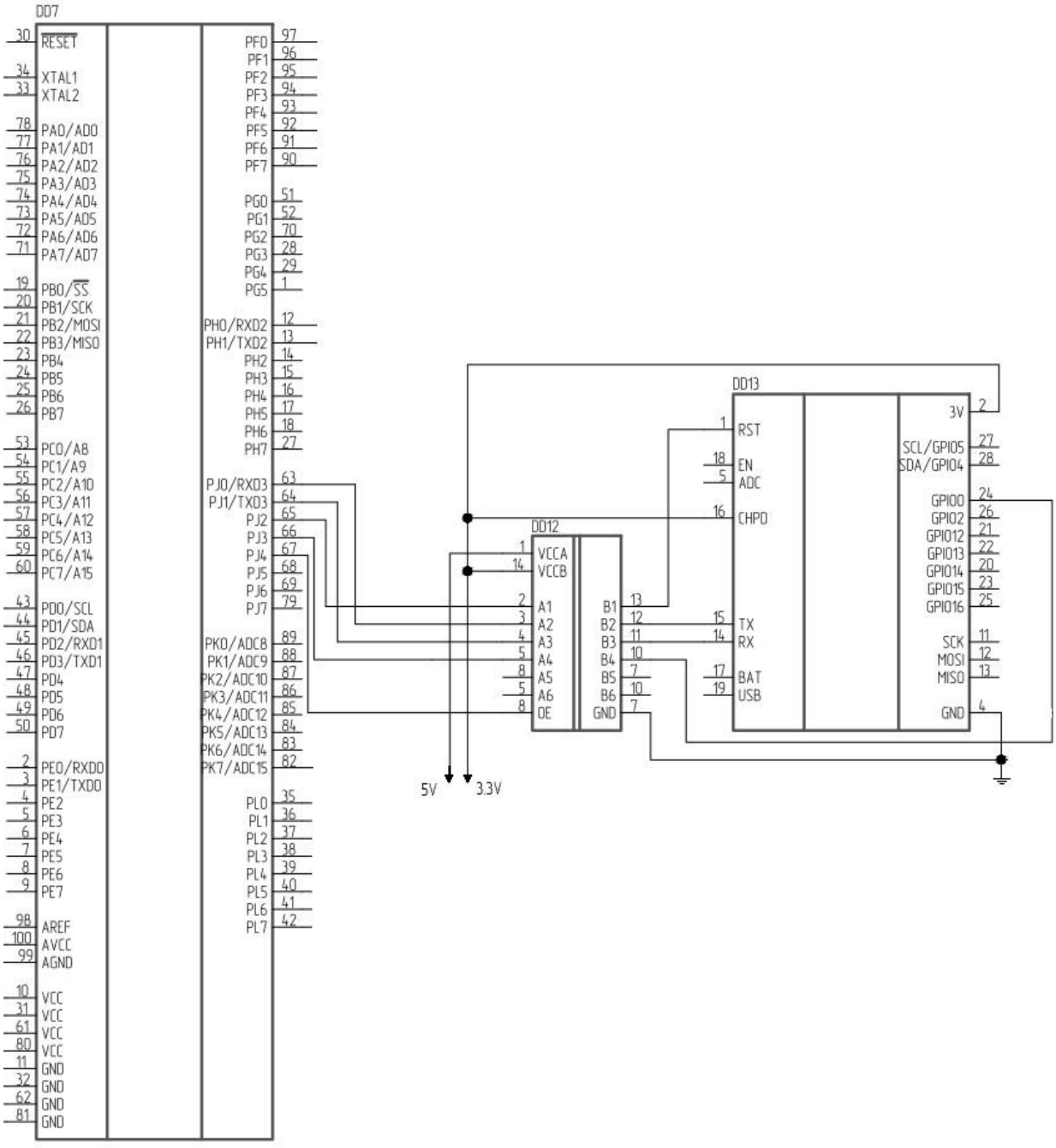

Рисунок 5.4 – Схема підключення модулю ESP8266

Трансівер ESP8266 використовує логічні рівні 3.3В, тому для узгодження логічних рівнів між мікроконтролером ATmega 2560 та модулем було використано узгоджувач логічних рівнів TXB0104D. Модуль підключено по

інтерфейсу UART порту мікроконтролера PJ на піни RXD3(63) та TXD3(64), з'єднаними з відповідними портами на модулі TX(15) та RX(14) відповідно.

Для реалізації обміну даними з веб-інтерфейсом, надсилання даних щодо стану системи був задіяний цифровий порт модулю GPIO0(24). Дане підключення слугує для ознайомчих цілей з можливостями Wi-Fi модулю.

В цілому даний модуль слугує для можливості маштабування проєкту у майбутніх версіях, розширення спектру можливостей, таких як надсилання/отримання команд керування, отримання інформації з сенсорів та реалізації веб-інтерфейсу охоронної системи.

5.3 Розробка GSM блоку

В якості GSM модулю було обрано трансівер SIM900D, підключення модулю до мікроконтролера ATmega 2560 зображена на рисунку 5.5.

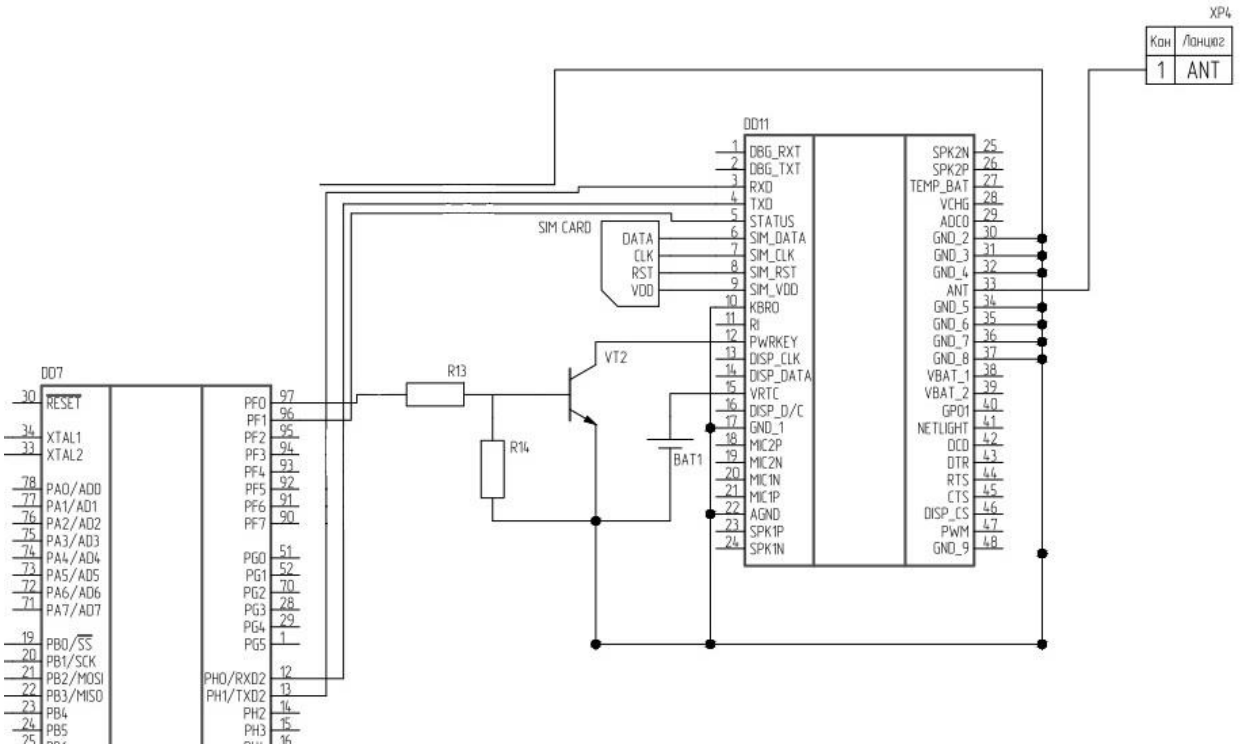

Рисунок 5.5. – Схема підключення модуля SIM900D

Підключення модуля SIM900D до мікроконтролера ATmega2560 включає використання виводів PF0-PF1 для передачі та прийому даних по UART, а також PH0-PH1 для керування модулем. У схемі використано два резистори та один транзистор для правильної регуляції напруги та керування живленням. Додатково

використовується акумулятор напругою 3.7В для забезпечення живлення модуля SIM900D. Це підключення дозволяє мікроконтролеру взаємодіяти з GSM-модулем, використовуючи інтерфейс UART для передачі команд та отримання даних.

5.4 Розробка блоку зчитування/запису RFID міток

Модуль RC522 є RFID-читачем, і його підключення до мікроконтролера ATmega2560 дозволяє здійснювати ідентифікацію та взаємодію з RFID мітками чи картками. На рисунку 5.6 зображено схему підключення модулю.

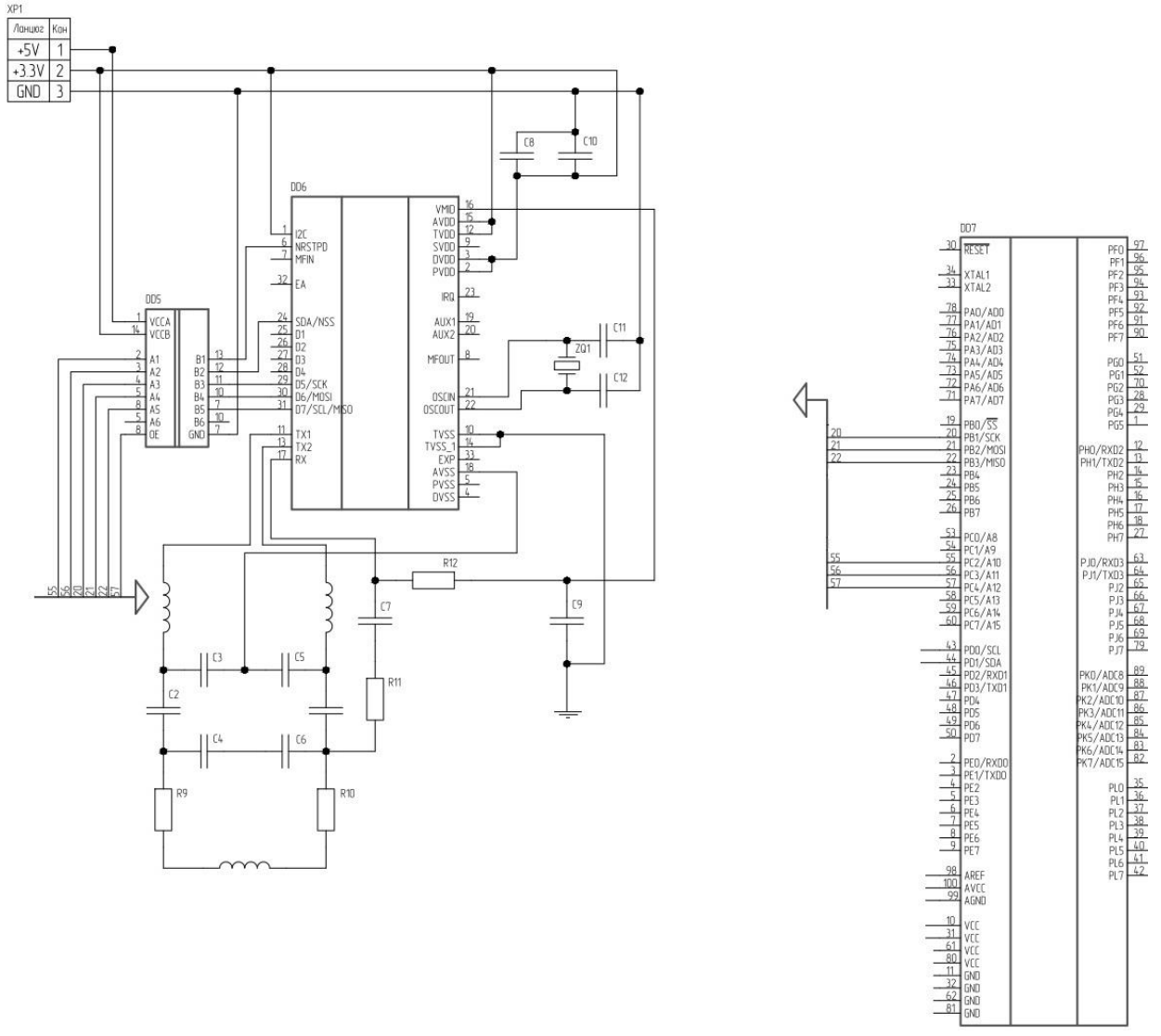

Рисунок 5.6. – Схема підключення модуля RC522

Підключення модуля RC522 до мікроконтролера ATmega2560 використовує піни для здійснення комунікації через інтерфейс SPI, зокрема

виводи PB1-PB3 для ліній MOSI, MISO, та SCK, а також PC2-PC4 для SS (Slave Select), RST та OE (Output Enable). Узгоджувач логічних рівнів TXB0104D використовується для забезпечення сумісності рівнів логіки між ATmega2560, який працює на рівні 5 В, і RC522, який оптимально функціонує на рівні 3.3 В. Це дозволяє стабільно та ефективно взаємодіяти з RFID-читачем, забезпечуючи надійну ідентифікацію та обробку RFID-міток у системі.

5.5 Розробка сенсорного блоку

Для підключення датчиків було використано цифрові входи мікроконтролера ATmega2560. Схема підключення зображена на рисунку 5.7.

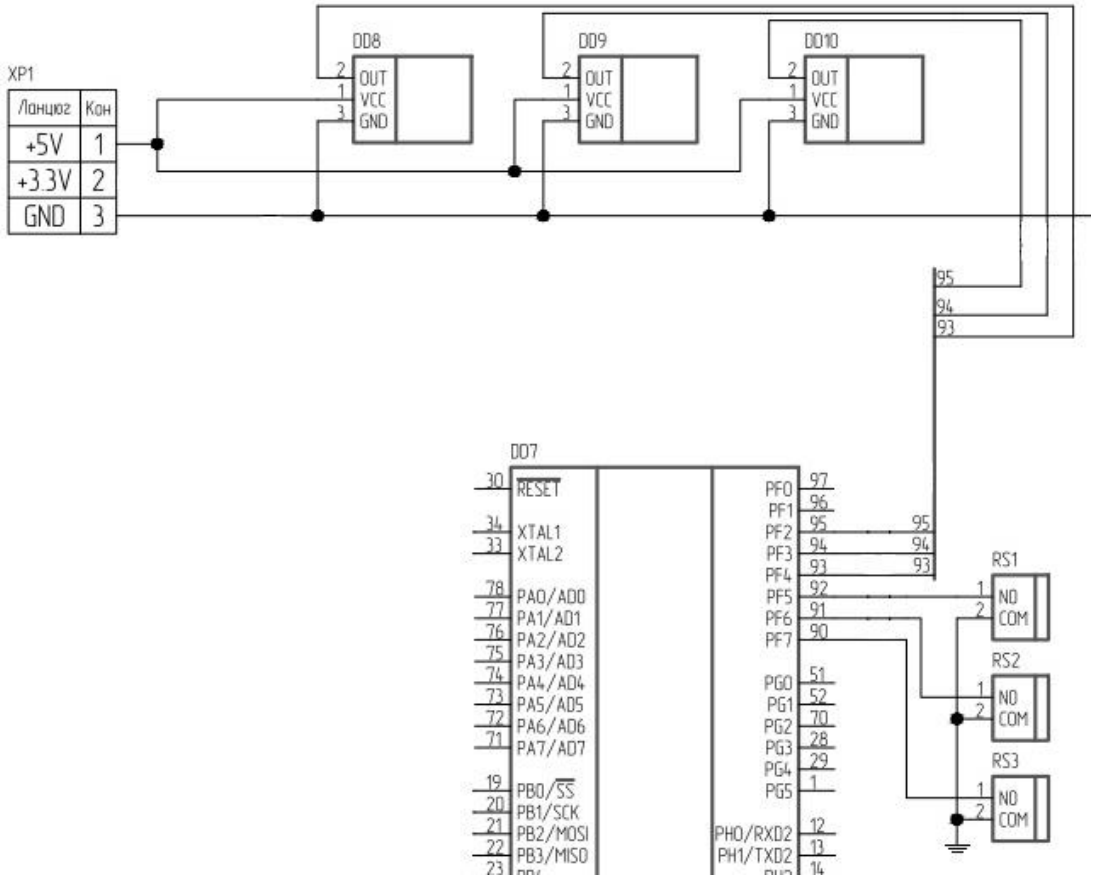

Рисунок 5.7. – Схема підключення датчиків

Підключення датчиків до мікроконтролера ATmega2560 включає використання виводів PF2-PF7 для забезпечення логічного з'єднання. Кожен датчик з'єднаний із відповідним входом мікроконтролера, що дозволяє системі

ефективно отримувати дані з усіх шести датчиків. Це підключення дозволяє зчитувати і обробляти інформацію від різних датчиків, розширюючи можливості системи контролю, і забезпечує надійну інтеграцію датчикованої інформації в мікроконтролерну платформу.

5.6 Блок виводу інформації, локального оповіщення

Для локальної взаємодії з системою було обрано дисплей LCD1602, який підключається до мікроконтролера через мікросхему PCF8574. Також в даному блоці бередбачена звукова сигналізація яка підключена до цифрового виходу мікроконтролера. Схема підключення зображена на рисунку 5.8.

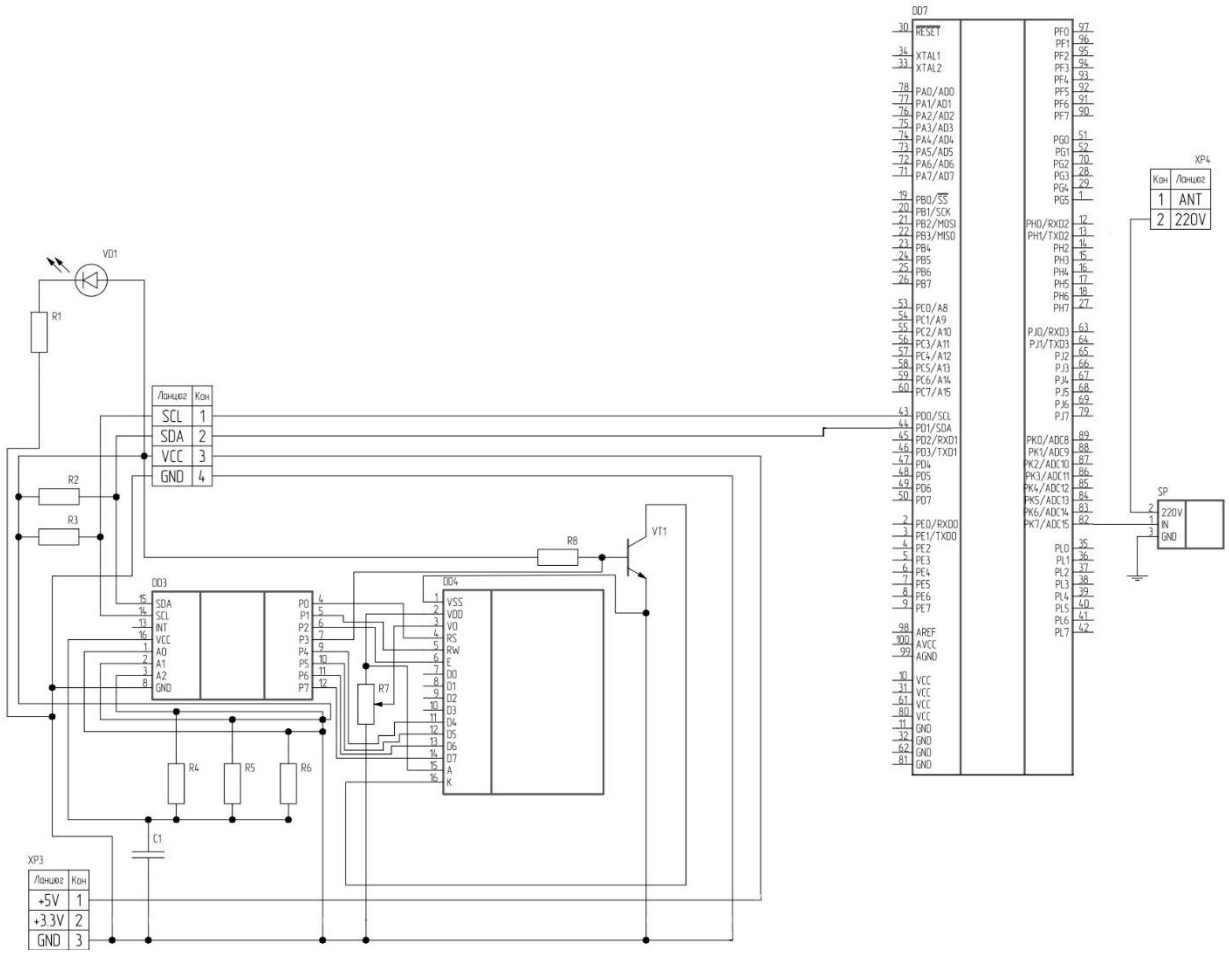

Рисунок 5.8. – Схема підключення дисплею та звукової сигналізації

Підключення LCD1602 до мікроконтролера ATmega2560 через інтерфейс PCF8574 включає використання двох виводів PD0-PD1 для здійснення комунікації за протоколом I2C. Для забезпечення надійної роботи LCD та його

підсвічування в схемі використано 7 резисторів для поділу напруги та забезпечення потрібних рівнів сигналів, 1 транзистор для керування підсвічуванням, 1 потенціометр для налаштування контрастності дисплея, 1 конденсатор для стабілізації живлення, і 1 світлодіод для індикації стану пристрою.

Додатково, на порт PK7 підключено вхід сирени, яка живиться від мережі 220В. Це доповнення в системі створює локальний оповіщувальний блок, який може включатися в разі необхідності оповіщення або сигналізації. Система отримує можливості виведення інформації на LCD, індикацію стану за допомогою світлодіоду та активує оповіщення через сирену.

5.7 Блок локального управління (клавіатурний блок)

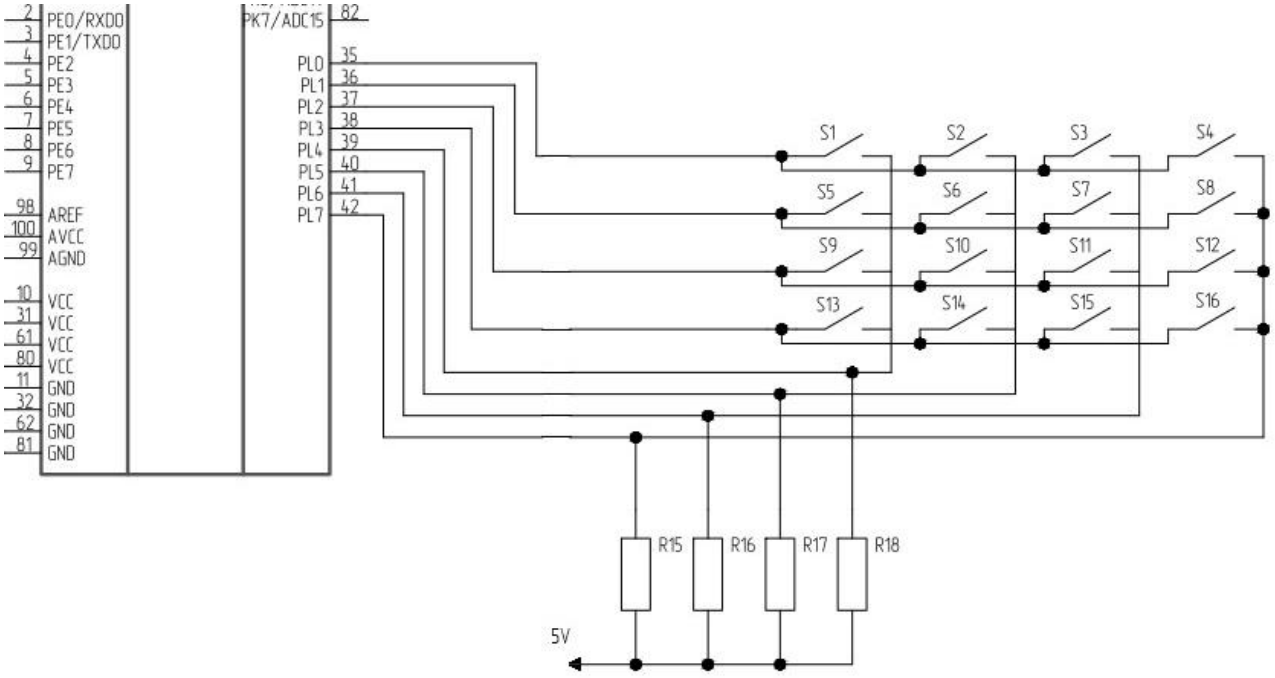

Рисунок 5.9. – Схема підключення клавіш

Підключення 16 клавіш до мікроконтролера ATmega2560 використовує виводи PL0-PL7 для забезпечення логічного з'єднання. Кожна клавіша зазначена окремим входом, що дозволяє мікроконтролеру спостерігати та реагувати на стан кожного ключа. Для кожного виводу використовуються відповідні резистори для

створення делікатного подільника напруги та ефективного визначення стану "натиснуто/не натиснуто". Це підключення дозволяє мікроконтролеру зчитувати введення від 16 клавіш, розширюючи можливості системи.

5.8 Блок дистанційного управління

Для реалізації блоку дистанційного управління було обрано модуль RFM95W LoRa. Схема підключення зображена на рисунку 5.10.

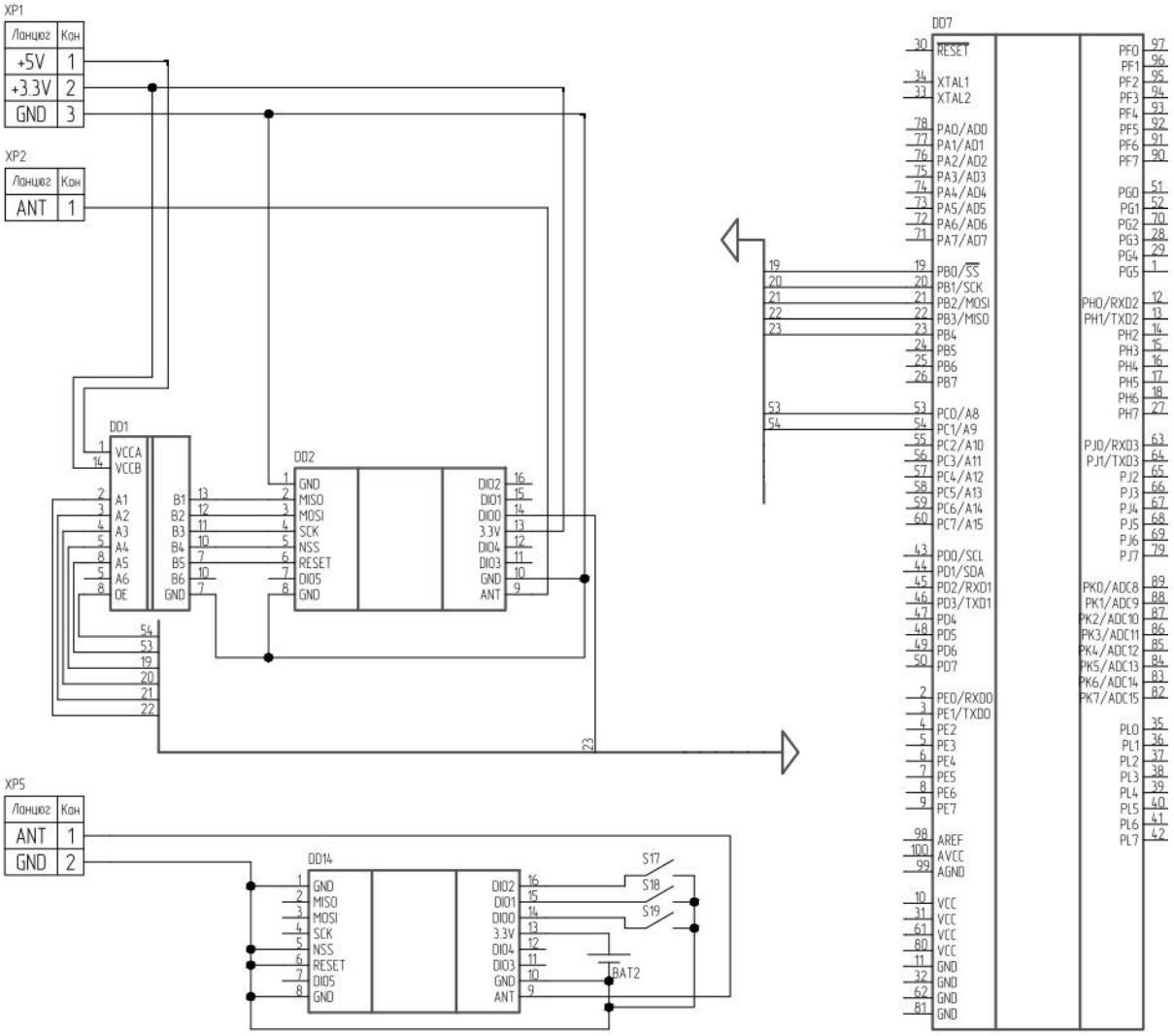

Рисунок 5.10. – Схема підключення модуля LoRa

Підключення модуля RFM95W до мікроконтролера ATmega2560 ретельно налаштоване для ефективного використання функціональності радіомодуля в системі зв'язку. Використані виводи, такі як PB0-PL4 та PC0-PC1, призначені для передачі та прийому даних, а також для прийому та передачі сигналів керування.

Для забезпечення сумісності рівнів логіки між ATmega2560 та RFM95W використовується узгоджувач логічних сигналів TXB0104D. Це важливо для вирішення можливих різниць у напругах та забезпечення стабільної комунікації.

Модуль RFM95W встановлено в системі для взаємодії з пультом ДУ, який також використовує RFM95W. Пульт ДУ оснащений трьома клавішами і живиться від батарейки 3.7В. Це дозволяє використовувати беспровідний канал для дистанційного керування, а також обміну командами або даними між пультом та мікроконтролером.

Узагальнено, це підключення створює потужну систему для бездротового зв'язку та дистанційного керування, що може бути використана в різних сценаріях, включаючи віддалені системи моніторингу, автоматизації або вдосконаленої системи управління.

Розробка програмного забезпечення МК для роботи системи

Нижче наведена спрощена програма модулю

```
#include <SoftwareSerial.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <MFRC522.h>
#include <Keypad.h>
#include <RH_RF95.h>

#define RFM95_CS 53
#define RFM95_RST 9
#define RFM95_INT 2

RH_RF95 rf95(RFM95_CS, RFM95_INT);

SoftwareSerial espSerial(2, 3); // RX, TX
SoftwareSerial gsmSerial(4, 5);  // RX, TX
String ssid = "WiFiSSID";
String password = "WiFiPassword";
String serverUrl = "http://web-server-endpoint";
String phoneNumber = "+380XXXXXXXXX";
String alarmDeactivationCode = "123456";  // Пароль для зняття з сигналізації

MFRC522 mfrc522(10, 9, 8, 7, 6); // SDA, SCK, MOSI, MISO, RST

const int motionSensorPin = A0;
const int magneticSensorPin = A1;
```

```
LiquidCrystal_I2C lcd(0x27, 16, 2);

// Клавіатура
const byte ROW_NUM = 4; // чотири рядки
const byte COLUMN_NUM = 4; // чотири стовпці

char keys[ROW_NUM][COLUMN_NUM] = {
  {'1', '2', '3', 'A'},
  {'4', '5', '6', 'B'},
  {'7', '8', '9', 'C'},
  {'*', '0', '#', 'D'}
};

byte pin_rows[ROW_NUM] = {A2, A3, A4, A5}; // піни рядків
byte pin_column[COLUMN_NUM] = {A6, A7, 8, 9}; // піни стовпців

Keypad keypad = Keypad(makeKeymap(keys), pin_rows, pin_column, ROW_NUM,
COLUMN_NUM);

bool alarmActive = true;

void setup() {
  Serial.begin(9600);
  espSerial.begin(9600);
  gsmSerial.begin(9600);
  SPI.begin();
  mfrc522.PCD_Init();
  lcd.begin(16, 2);
  lcd.backlight();
```

```
  pinMode(motionSensorPin, INPUT);
  pinMode(magneticSensorPin, INPUT);

  connectToWiFi();

  /RFM95W
  if (!rf95.init()) {
    Serial.println("LoRa init failed");
    while (1);
  }

// Налаштування частоти (в МГц)
  rf95.setFrequency(868.0);

  // Налаштування потужності передавача (в децибелахміліватах)
  rf95.setTxPower(23, false);  // Другий параметр - "високий" або "низький" рівень потужності
}

}

void loop() {
  int motionSensorValue = digitalRead(motionSensorPin);
  int magneticSensorValue = digitalRead(magneticSensorPin);

  if (alarmActive) {
    // Введення коду для зняття з сигналізації через клавіатуру
    char key = keypad.getKey();
```

```
    if (key) {
      checkAlarmDeactivationCode(key);
    }
  }

  sendToWebInterface("Motion Sensor: " + String(motionSensorValue) + ", Magnetic Sensor: " + String(magneticSensorValue));

  if (mfrc522.PICC_IsNewCardPresent() && mfrc522.PICC_ReadCardSerial()) {
    String tagId = "";
    for (byte i = 0; i < mfrc522.uid.size; i++) {
      tagId += String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
      tagId += String(mfrc522.uid.uidByte[i], HEX);
    }
    sendToWebInterface("RFID Tag ID: " + tagId);
  }

  delay(1000);

  if (rf95.available()) {
    // Отримати пакет
    uint8_t buf[RH_RF95_MAX_MESSAGE_LEN];
    uint8_t len = sizeof(buf);

    if (rf95.recv(buf, &len)) {
      buf[len] = '\0'; // додаткове додавання нуль-термінатора для перетворення у рядок
      String message = String((char*)buf);
```

```
      // Перевірити повідомлення від пульта ДУ
      if (message == "DISARM") {
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Alarm Deactivated");
        delay(2000);
        alarmActive = false;
      }
    }
  }

  delay(1000);
}

void sendToWebInterface(String data) {
  espSerial.println("AT+CIPSTART=\"TCP\",\"" + serverUrl + "\",80");
  if (espSerial.find("OK")) {
    String postData = "data=" + data;
    String postRequest = "POST " + serverUrl + " HTTP/1.1\r\n";
    postRequest += "Host: " + serverUrl + "\r\n";
    postRequest += "Content-Type: application/x-www-form-urlencoded\r\n";
    postRequest += "Content-Length: " + postData.length() + "\r\n\r\n";
    postRequest += postData;

    espSerial.println("AT+CIPSEND=" + String(postRequest.length()));
    delay(1000);
    espSerial.print(postRequest);
    delay(1000);
```

```
  }
}

void connectToWiFi() {
  espSerial.println("AT+CWMODE=1");
  delay(1000);
  espSerial.println("AT+CWJAP=\"" + ssid + "\",\"" + password + "\"");
  delay(5000);
}

void checkAlarmDeactivationCode(char key) {
  static String enteredCode = "";
  enteredCode += key;

  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Enter Code:");
  lcd.setCursor(0, 1);
  lcd.print(enteredCode);

  if (enteredCode.length() == alarmDeactivationCode.length()) {
    if (enteredCode == alarmDeactivationCode) {
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Alarm Deactivated");
      delay(2000);
      enteredCode = "";
      alarmActive = false;
```

```
    } else {
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("Invalid Code");
      delay(2000);
      enteredCode = "";
    }
  }
}
```

6. Техніко економічна частина

7.1 Розрахунок повної собівартості пристрою.

Собівартість продукту – це матеріальні затрати в грошовій формі, які підприємство витрачає на виробництво та підготовку до збуту продукції. Собівартість продукції в галузі виробництва включає в себе вартість матеріалів, затрати на робочу силу та накладні витрати на виробництво.

Витрати, що пов’язані з виробництвом та збутом електронного пристрою, що був розроблений, можливо робити на наступні групи:

- Сировинні матеріали: Вартість всіх матеріалів, які використовуються для виробництва пристрою.
- Проміжні матеріали і компоненти: Вартість всіх додаткових матеріалів та компонентів, які також використовуються під час виробництва.
- Витрати на транспортування та логістику: Вартість транспортування матеріалів та готової продукції.
- Праця: Вартість працівників, які беруть участь у виробництві, включаючи зарплату та витрати на соціальні пакети.
- Загальновиробничі витрати: Витрати, пов'язані з управлінням підрозділу, витрати на службові відрядження працівників цеху (підрозділу), амортизаційні відрахування від вартості основних фондів загальноцехового призначення і т.д. .
- Витрати на обладнання та амортизацію: Вартість використання обладнання та амортизація його вартості.
- Витрати на управління та адміністрування: Витрати на управлінську діяльність та адміністративні витрати.
- Витрати на збут: Інші витрати, пов'язані з виробництвом, такі як витрати на рекламу, оплату послуг та інше.

1. Витрати на матеріали та комплектуючі

Всі необхідні компоненти для приладу та їх вартість в продажу наведені в таблиці нижче. Ціни на комплектуючі взяті з сайті виробника та посередників що вказані нижче. Всі ціни станом на 20.12.2023.

- «Arduino.ua» - https://arduino.ua/
- «Microchip» - https://www.microchipdirect.com/
- «Prom» - https://prom.ua/ua/

Таблиця 7.1 – Ціни на електричні компоненти системи

Назва	Ціна, грн
Мікроконтролер ATMEGA2560-16AU	756.00
Wi-Fi модуль, трансівер ESP8266 ESP-01S	139.83
GSM модуль SIM900D SCM	665.50
Узгоджувач рівнів TXB0104	68.00
Трансівер LoRa RFM95W-868S2	378.00
Модуль розширення I^2C PCF8574	49.00
Дисплей LCD 1602	122.36
Матрична клавіатура 4x4	50.99
Сирена світлозвукова Дует (С-06С-220)	628.49
Стабілізатор напруги 5В DW01A	3.68
Стабілізатор напруги 3.3В CS8182	54,00
Додаткові елементи	127.23

На основі даних з таблиці можливо підрахувати загальну вартість комплектуючих пристрою C_n яка дорівнює 3043,08 грн.

2. Витрати на проміжні матеріали і компоненти

Окрім основних комплектуючих до вартості пристрою потрібно додати затрати на сировинні компоненти, що використовуються при виробництві. Матеріали та ціна таких компонентів наведені в таблиці нижче.

Таблиця 7.2 – витрати на сировину і матеріали

Матеріал, сировина	Норма витрат, кг.	Ціна за одиницю грн/кг.	Вартість, грн.
Припой LC60- 0.38/0.25	0,015	2325	3,4
Флюс NC-559-asm flute	0,01	12236	12,3
Склотекстоліт для друкованих плат	0,07	1200	84

Так виходить, що затрати на додаткову проміжну сировину виходять 99,7грн

На основі отриманих даних можливо порахувати вартість пристрою з додатковими затратами що становить 3043,08 + 99,7 = 3142,78 грн

3. Витрати на транспортування та логістику

Витрати на транспортування та логістику визначаються як 10 – 20% вартості комплектуючих і комплектуючих. Так виходить, що дана стаття витрат становить від 315 до 629 грн. Отже вартість пристрою з урахуванням транспортування та логістику дорівнює 3142,78 + 629 = 3771,78 грн.

4. Витрати на основну заробітну плату.

При виробництві пристрою роботи ведуться в 2 напрямках апаратній та програмній. Для цього необхідні наступні фахівці: інженер – електронщик та програміст. Обов’язками працівників буде виготовлення друкованих плат, монтаж компонентів на друкованій платі, написання та прошивання мікроконтролерів.

Витрати на заробітну плату визначаються наступним співвідношенням

$$З_0 = \sum_{i=1}^{n} T_{гі} * H_{чі}$$

(7.1)

де *Т*гі - середня годинна тарифна ставка 1 робочого задіяного у виробництві продукту (грн. / год); Нчі - витрачений працівником час на виготовлення і налагодження приладу (годин.); n - кількість працівників задіяних у виробництві.

Заробітна плата для кожного працівника визначається. При врахуванні 8 годинного робочого дня, та терміні роботи в 21 робочий день в місяць виходить 168 годин робочого часу. Так середньочасова трудова ставка, орієнтовно, визначається наступним співвідношенням.

$$Т_{гі} = \frac{Т_{мі}}{В_{фі} * В} \quad (7.2)$$

Тм*і* - місячна заробітна плата фахівця (грн.); Вф*і* - фактично відпрацьований час за розрахунковий період (місяць), днів (змін);

8 - кількість відпрацьованих годин за зміну.

$$Т_{гі} = \frac{Т_{мі}}{В_{фі} * В} = \frac{17000}{21 * 8} = 101(\frac{грн}{год})$$

(7.3)

$$З_0 = \sum_{i=1}^{n} T_{гі} * H_{чі} = 101 * 8 = 808(грн) \quad (7.4)$$

До витрат пов'язаних з заробітною платою також потрібно віднести додатки, які включають в себе премії 15%, та відрахування пов'язані з пенсійним фондом, що становить 33.2%, соціальне страхування 2.9% , фонд зайнятості 1,9%. Всього виходить 38% відрахувань. Так співвідношення нижче показують преміювання та вирахування в грн.

$$З_{пр} = З_О \frac{З_д}{100} = 808 \frac{15}{100} = 121(грн) \quad (7.5)$$

Де Зд – відсоток преміювання.

$$В_{соц} = (З_О + З_Д) * \frac{38}{100} = (808 + 121) * \frac{38}{100} = 353\ (грн) \quad (7.6)$$

5. Загальновиробничі витрати

Витрати, пов'язані з управлінням підрозділу, витрати на службові відрядження працівників цеху (підрозділу), амортизаційні відрахування від вартості основних фондів загальноцехового призначення і т. д.

Визначаються в розмірі 130-250% від основної заробітної плати: 808 · 1,5 = 1212 (грн.).

6. Витрати на обладнання та амортизацію

Вартість використання обладнання та амортизація його вартості. Затрати на утримання та експлуатацію устаткування становлять в середньому 130% від заробітної плати. Так виходить 808 * 1,3 = 1050,4 грн

Сума статей 1.1 - 1.6 являє виробничу собівартість приладу (установки). Маємо: 3771,78 + 808 + 1212 + 121 + 353 +1050,4 = 7316,18 грн.

7. Витрати на управління та адміністрування

Витрати на управлінську діяльність та адміністративні витрати можуть включати в себе:

Витрати, пов'язані з управлінням підприємства;

- Витрати на пожежну і сторожову охорону;
- Витрати, пов'язані з підготовкою (навчанням) і перепідготовкою кадрів;
- Витрати на оплату відсотків за фінансові кредити, а також відсотків за товарні і комерційні кредити; витрати, пов'язані з оплатою відсотків за користування матеріальними цінностями, взятими в оренду (лізинг);
- Витрати, пов'язані з оплатою послуг;
- Податкові відрахування.

Визначаються в розмірі 140-200% відсотків від основної заробітної плати.

Орієнтовна затрати на адміністративні послуги складуть 150% від основної заробітної плати – 1212 грн.

8. Витрати на збут:

Витрати, пов'язані з виробництвом, такі як витрати на рекламу, оплату послуг та підготовку до реалізації. Такі витрати можуть коливатися від 5 до 10% від виробничої собівартості 134 * 0,1 = 648 грн.

Сума всіх вище перелічених витрат складає повну собівартість пристрою і становить 7316,18 + 1212 + 648 = 9176,18 грн.

Таблиця 7.3 – Калькуляція собівартості приладу

Назва	Ціна, грн
1. Витрати на матеріали та комплектуючі	3043,08
2. Витрати на проміжні матеріали і компоненти	99,7
3. Витрати на транспортування та логістику	629
4. Витрати на основну заробітну плату.	1302
5. Загальновиробничі витрати	1212
6. Витрати на обладнання та амортизацію	1050
7. Витрати на управління та адміністрування	1212
8. Витрати на збут	648
Повна собівартість	9195,78

7.2 Визначення ціни пристрою

Оптова ціна пристрою, що проектувався, визначається за наступним виразом:

$$Ц_{опт} = С + П \qquad (7.7)$$

В якому П – величина прибутку, С – собівартість.

Значення прибутку визначається з урахуванням показника рентабельності Р виготовлення продукту, та представлений формулою нижче:

$$Р = (П/С) * 100\% \qquad (7.8)$$

Зазвичай показник рентабельності не перевищує 35%, в нашому випадку приймаємо це значення за 8%.

Підставимо значення у формулу й знайдемо оптову ціну виробу. Так оптова ціна виходу становить:

$$Ц_{опт} = С + \frac{Р*С}{100} = 9195 + \frac{8*9195}{100} = 9930{,}60 \text{ (грн)} \qquad (7.9)$$

Роздрібна ціна розраховується з додавання ПДВ, що рівняється 120%. Вираз для розрахунку наведений нижче:

$$Ц_{роз} = 1{,}2 * Ц_{опт} = 1{,}2 * 7703{,}12 = 11916{,}72$$

(7.10)

Так в розділі було розраховано собівартість пристрою, оптову та роздрібну вартість для оцінки економічної вигоди. Пристрій можливо вважати конкурентоспроможним та економічно вигідним для подальшого розвитку.

Висновок

В кваліфікаційній роботі магістра було розроблено електронну охоронну систему розумний дім

При виконанні роботи було проведено аналіз вразливостей і факторів, що впливають на систему зв'язку охоронної системи розумного будинку, розглянуто методи шифрування та інтерфейси бездротового зв’язку.

Система побудована на базі мікроконтролера ATmega 2560.

Для побудови системи було розроблено алгоритм роботи системи, структурна схема пристрою, та спроектовано функціональну та принципіальну схему.

Були здійснені розрахунки для визначення собівартості, економічної рентабельність та конкурентоспроможність пристрою. Також було визначено, що елементна база є доступною та розповсюджена.

Так можливо зробити висновок що розроблена система має обширний спектр можливостей до модернізації та масштабування.

Список літератури

1. П. В. Мокренко . Елементи і пристрої фізичної та електронної охорони об'єктів. Нац. ун-т «Львів. політехніка». — Л. : Фенікс, 2000. — 186 с.
2. Г. Б. Сухоруков. "Охорона інформації: підручник." - Київ: Видавництво Логос, 2015. - 328 с.
3. Мельничук Р.А., Ларченко Л.В. Системи безпеки розумного будинку. / Р.А. Мельничук, Л.В. Ларченко // CXIII Міжнародна інтернет-конференція «Розвиток науки та техніки під час воєнного стану». – м. Херсон, 28 листопада, 2022.– С. 156-158.
4. І. О. Іванов, Т. П. Сидоренко. "Мережеві технології та інформаційна безпека." - Київ: Національний технічний університет України "КПІ", 2017. - 240 с.
5. О. В. Колісник, О. В. Тимчик. "Системи виявлення та протидії кіберзлочинності." - Київ: Видавничий дім "Ін Юре", 2019. - 184 с.
6. В. П. Прасолов, В. А. Безсмертний. "Інтеграція засобів технічної охорони та відеоспостереження." - Харків: Компанія "Смарт", 2008. - 120 с.
7. В. С. Литвин, О. В. Рибалка. "Сучасні системи безпеки: теорія та практика." - Київ: Центр учбової літератури, 2016. - 288 с.
8. М. С. Федоренко, В. М. Ситник. "Безпека інформаційних технологій в органах державного управління." - Київ: Видавничий центр НАДУ, 2014. - 272 с.
9. В. В. Баканов. "Системи захисту інформації: підручник." - Київ: Каравела, 2013. - 416 с.
10. Ю. П. Шеленков, Ю. В. Даниленко. "Організація захисту інформації на підприємствах та в установах." - Київ: КНЕУ, 2006. - 304 с.
11. В. А. Романенко, О. І. Соломчук. "Основи захисту інформації в комп'ютерних системах." - Київ: Видавництво Національного університету "Львівська політехніка", 2010. - 320 с.

12. О. В. Самойленко. "Безпека інформаційних технологій." - Київ: Видавничий дім "Ін Юре", 2018. - 232 с.
13. Максимов М.Г. "Вступ до системного програмування мікроконтролерів AVR". Солон-Прес, 2018. 368 с.
14. Фабіровський, С., та О. Москалюк. "Розробка безпровідної системи завадостійкої сигналізації на базі технології LORA". Information and communication technologies, electronic engineering 1, № 1, 2021р.: 94–104.
15. The History of the Remote Control. URL: https://www.firefold.com/blogs/news/the-history-of-the-remote-control.
16. The Definitive History Of Smart Home Devices. URL: https://www.smarthomepoint.com/history/.
17. Robert Faludi. Building Wireless Sensor Networks: with ZigBee, XBee, Arduino, and Processing. 2019. 322с.
18. Томас М. Сігру, Джеймс Ф. Келлер. Digital Transformation: Survive and Thrive in an Era of Mass Extinction. 2019 рік. 256 с.
19. Мартін Форд. The Rise of Robots: Technology and the Threat of a Jobless Future. 2020 рік. 368 с.
20. LoRa and LoRaWAN: A Technical Overview, Semtech Corporation URL: https://lora-developers.semtech.com/documentation/tech-papers-and-guides/loraand-lorawan/ (дата звернення 19.11.2021).
21. Офіційний сайт LoRa альянсу // https://www.lora-alliance.org/.
22. What is LoRa? // Technology - MickMake - Live. Learn. Make. URL: https://www.mickmake.com/post/what-is-lora-technology