МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки
(повне найменування інституту, назва факультету)

Кафедра програмованої електроніки, електротехніки і телекомунікацій
(повна назва кафедри)

«Допущений до захисту»
Завідувач кафедри _____ В. М. Рябенький
д.т.н., професор
« 16 » червня 2025 р.

Кваліфікаційна робота

на здобуття ступеня вищої освіти «бакалавр**»**
(освітньо-кваліфікаційний рівень)

на тему: Розробка бездротової автономної сигналізації

Виконав: студент 4391 групи
_____ І.О. Бецько
(підпис)

Керівник роботи:
професор каф. ПЕЕТ, к.т.н., доцент,
професор НУК
(посада, науковий ступінь, вчене звання)
_____ О. К. Жук
(підпис)

м. Миколаїв – 2025 року

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки

Кафедра програмованої електроніки, електротехніки і телекомунікацій
Спеціальність 172 «Електронні комунікації та радіотехніка»
Освітня програма Телекомунікації

«ЗАТВЕРДЖУЮ»
Гарант освітньої програми
_____ О.К.Жук
(підпис)
« 14 » квітня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття ступеня вищої освіти «бакалавр**»**
(освітньо-кваліфікаційний рівень)

Студенту Бецьку Іллі Олександровичу
(прізвище, ім"я, по батькові)

1. Тема роботи Розробка бездротової автономної сигналізації

керівник роботи Жук Олександр Кирилович, професор каф. ПЕЕТ, к.т.н., доцент, професор НУК
(прізвище, ім"я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ректора № УЧ-343 від « 23 » квітня 2025 року.

2. Термін подання роботи: 10 червня 2025 р.

3. Вихідні дані по роботі: Розробити дешеву енергоекономічну безпровідну сигналізацію з автономним блоком живлення, призначену для роботи у віддалених від міста населених пунктах, де відсутнє покриття стільникових операторів з використанням для передачі сигналу перспективної технології LoRa, яка ідеально відповідає усім поставленим перед сигналізацією вимогам.

4. Перелік питань, що належать до розробки (найменування розділів):

- Структура системи
- Захист безпровідної мережі і програма для комп'ютера
- Підпорядкований і головний пристрої
- Протокол обміну даними
- Охорона праці

5. Перелік презентаційних матеріалів:

• Структура системи
• Перевірка випадковості згенерованих чисел графічним способом
• Інтерфейс програми для комп‘ютера
• Діаграма станів і переходів головного пристрою
• Діаграма станів і переходів підпорядкованого пристрою
• Спосіб запобігання колізій

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
5.	Тубальцев А.М., доцент кафедри екології		

7. Дата видачі завдання «24» квітня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Структура системи	01.03.2025 р.	виконав
2.	Захист безпровідної мережі і програма для комп'ютера	15.03.2025 р.	виконав
3.	Підпорядкований і головний пристрої	01.04. 2025 р.	виконав
4.	Протокол обміну даними	01.05.2025 р.	виконав
5.	Охорона праці	01.06.2025 р.	виконав

Студент _____ І.О. Бецько
(підпис) (прізвище та ініціали)

Керівник роботи _____ О. К. Жук
(підпис) (прізвище та ініціали)

Анотація

Головною відмінністю розробленої сигналізації є її дешевизна та ввикористання передачі сигналу перспективної технології LoRa. Окрім основного завдання, а саме сповіщення про проникнення на об‘єкт, розроблена сигналізація виконує функції управління виходами і контролю станів датчиків, які можуть бути відключені з метою збереження енергії.

У розробці в повній мірі використовуються можливості мікроконтролера, а саме:

- захист інформації шифруванням і криптографічною хеш-функцією (з використанням бібліотеки від STMicroelectronics), окремий ключ шифрування закріплений за кожним передавачем;
- flash-пам‘ять мікроконтролера використовуються для емуляції EEPROM;
- апаратна генерація істинно випадкових чисел.

Розроблені програми для мікроконтролерів підпорядкованого і головного пристроїв, а також програма для комп‘ютера, що містить графічний інтерфейс користувача, зберігає дані про підключені пристрої і спрацювання сигналізації, взаємодіє з мікроконтролерами (змінює налаштування модемів, отримує апаратно згенеровані випадкові числа для ключів шифрування, виводить інформацію про спрацювання сигналізації). Велика увага приділена надійності комп‘ютерної програми та зручності роботи з графічним інтерфейсом користувача.

Головною перевагою розробленої системи є її автономність: має акумуляторне живлення, не потребує підключення до інтернету чи наявності покриття базової станції, не потребує використання додаткового специфічного програмного чи апаратного забезпечення. Передбачається використання системи у невеликих населених пунктах, де існує необхідність захисту приватної власності від зловмисників і не тільки.

Ключові слова: охоронна сигналізація; інтерфейс програми для комп‘ютера; діаграма станів і переходів; спосіб запобігання колізій; генерування випадкових чисел

Abstract

The main difference of the developed alarm system is its low cost and the use of promising LoRa technology for signal transmission. In addition to the main task, namely, notification of intrusion into the object, the developed alarm system performs the functions of output control and sensor status control, which can be turned off to save energy.

The development fully uses the capabilities of the microcontroller, namely:

- information protection by encryption and cryptographic hash function (using a library from STMicroelectronics), a separate encryption key is assigned to each transmitter;

- the microcontroller's flash memory is used for EEPROM emulation;

- hardware generation of truly random numbers.

Programs for microcontrollers of the slave and master devices, as well as a computer program containing a graphical user interface, stores data about connected devices and alarm triggering, interacts with microcontrollers (changes modem settings, receives hardware-generated random numbers for encryption keys, displays information about alarm triggering). Much attention is paid to the reliability of the computer program and the convenience of working with the graphical user interface.

The main advantage of the developed system is its autonomy: it has battery power, does not require an Internet connection or base station coverage, does not require the use of additional specific software or hardware. The system is intended to be used in small settlements where there is a need to protect private property from intruders and not only.

Keywords: security alarm; computer program interface; state and transition diagram; method of preventing collisions; random number generation

ЗМІСТ

Кваліфікаційна робота 4
(прізвище, ім'я, по батькові) 5
Перелік умовних позначень, символів, одиниць, скорочень та термінів .. 7
Вступ 9
Розділ 1. Структура системи 14
1.1 Опис і складові системи 14
1.2 Елементна база 15
Висновки до розділу 1 18
Розділ 2. Захист безпровідної мережі і програма для комп'ютера 20
2.1 Конфіденційність 20
2.2 Цілісність 26
2.3 Автентичність 28
2.4 Огляд криптографічної бібліотеки STMicroelectronics 29
2.5 Генерація випадкових чисел 35
2.6 Вибір мови програмування і бібліотеки 41
2.7 Огляд графічного інтерфейсу користувача 43
Висновки до розділу 2 53
Розділ 3. Підпорядкований і головний пристрої 56
3.1 Вибір і огляд мікроконтролера підпорядкованого пристрою 56
3.2 Опис роботи програми підпорядкованого пристрою 59
3.3 Підключення Blue Pill підпорядкованого пристрою 61
3.4 Програмна реалізація деяких функцій підпорядкованого пристрою 62
3.5 Вибір і огляд мікроконтролера головного пристрою 66
3.6. Опис роботи програми головного пристрою 68
Висновки до розділу 3 69
Розділ 4. Протокол обміну даними 72
4.1 Провідний спосіб 72
4.2 Безпровідний спосіб 76
Висновки до розділу 4 77

Розділ 5. Охорона праці 79
5.1 Несприятливе освітлення 79
5.2 Психофізичні фактори 80
5.3 Небезпека загоряння і вибуху літій-іонних акумуляторів 83
Висновки до розділу 5 86
ВИСНОВКИ 87
Список використаних джерел 90

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

AES – Advanced Encryption Standard

ARM – Advanced RISC Machines

CBC – cipher block chaining

CMSIS – Common Microcontroller Software Interface Standard

EEPROM – electrically erasable programmable read-only memory

GSM – Global System for Mobile Communications

HAL – Hardware Abstraction Layer

HMAC – hash-based MAC

ID – identifier

IV – initialization vector

LoRa – Long Range

MAC – message authentication code

RTC – Real Time Clock

SHA – Secure Hash Algorithm

SRAM – static random-access memory

USB – Universal Serial Bus

WAN – wide area network

АГВЧ – апаратний генератор випадкових чисел

АЦП, ADC – аналого-цифровий перетворювач

ГВЧ, RNG – генератор випадкових чисел

ГІК (ГКІ) – графічний інтерфейс користувача

ГПВЧ – генератор псевдовипадкових чисел

МП – мова програмування

ОП – операційний підсилювач

ПЗ – пояснювальна записка

ПЗ – програмне забезпечення

ПК – персональний комп‘ютер

УСАПП, USART – універсальний синхронно-асинхронний прийомопередавач

УАПП, UART – універсальний асинхронний прийомопередавач

ВСТУП

Мікроелектроніка є дуже прибутковою галуззю сучасної промисловості. Позиція держави у світовій економіці значною мірою визначається розвитком мікроелектронної промисловості. Її продукти використовуються в усіх інших сферах професійної діяльності людини.

Для виготовлення конкурентних обчислювальних пристроїв необхідна наявність дорогої апаратури в поєднанні з висококваліфікованими спеціалістами. Велике число компанії, керівники яких розуміють неможливість наздогнати монополістів виробництва мікроелектронних приладів за сучасними технологічними процесами, переорієнтувалися на виробництво силових напівпровідникових приборів.

Мікроелектронна промисловість в Україні не розвинена, потенціал втрачений, шанси на покращення ситуації відсутні. Поки капіталісти примножують інвестиції, мікроелектроніка в Україні наближається до нуля; прірва поглиблюється і розширюється.

Зазначені аргументи враховувалися при виборі теми дипломного проекту. Якщо мікроелектроніка настільки важлива, а розробляти і виробляти напівпровідникову продукцію неможливо, необхідно хоча б бути до неї причетним. Причетність полягає у її використанні, а саме розробці електронних пристроїв на базі сучасних компонентів, створених провідними компаніями США і Європи і виготовлених в Тайвані, а також прогресивних технологій, які є результатами розумової діяльності кваліфікованих вмотивованих інженерів.

Питання захисту приватної власності ніколи і ніде не втрачало своєї актуальності. В розвинених країнах Заходу зловмисники рідше посягають на майно «простих людей», але в Україні маргінали не гребують крадіжками будь-чого, що можна здати на метал. Окрім крадіїв, завдати шкоди власності можуть вандали, тому сигналізація повинна повідомляти про проникнення на пункт охорони, а також здійснювати світло-звукове сповіщення.

Поставлене завдання розробки безпровідної сигналізації, головним призначенням якої є охорона приватної власності від зловмисників. Охоронна функція виконується шляхом повідомлення про спрацювання сигналізації на пункт охорони. Додатковими функціями, що були втілені у сигналізації є:

- автономна робота сигналізації;
- контроль станів датчиків;
- віддалене управління виходами.

Під автономністю сигналізації я розумію незалежність її роботи від зовнішніх факторів, що не є стандартним змістом цього словосполучення. Автономність полягає у таких принципах:

- робота сигналізації не має залежати від наявності покриття базової станції;
- працездатність сигналізації має підтримуватися впродовж тривалого часу за відсутності напруги в мережі;
- робота сигналізації не повинна потребувати специфічного стороннього ПЗ чи апаратури.

Сигналізація повинна мати такі властивості:

- надійність і захищеність від втручання зловмисників;
- дешевизна;
- функціональність і гнучкість налаштування;
- енергозбереження;
- простота використання.

Передбачається використання сигналізації у віддалених від будь-яких засобів комунікації дачних кооперативах, де будівлі можуть розміщуватися на значній відстані одна від одної. GSM – сигналізації не вирішують питання охорони дачі: дачу розкрадуть швидше, ніж власник до неї добереться. У деякій місцевості покриття може взагалі не бути, а де воно наявне – потребує

додаткових витрат на послуги оператора. Ще одним недоліком GSM є велике енергоспоживання.

LoRa (Long Range) є новою перспективною енергоекономічною технологією безпровідної передачі даних на велику відстань. Головними перевагами технології LoRa є:

- висока стійкість до завад;
- можливість автономної роботи пристроїв, що використовують LoRa, від акумулятору протягом тривалого часу за рахунок наднизького енергоспоживання модемів.

Semtech розробила протокол LoRaWAN і виробляє мікросхеми передавачів, що використовують запатентовану Semtech модуляцію LoRa.

Одним з можливих застосувань технології є системи домашньої безпеки (рис.0.1) [1].

Рис.0.1. Запропонована Semtech структура охоронної системи.

Запропонована Semtech система складається з 1 – датчиків, 2 – камери, 3 – брелка, 4 – безпровідної зовнішньої сирени, 5 – гібридного шлюзу, 6 – серверу, 7 – девайсів користувача.

Така система забезпечує найбільшу зручність користування, але вона містить у складі велике число компонентів, кожен з яких оснащений модемом і акумулятором, що збільшує ціну системи у рази, зростає ціна розробки такої системи.

Більшість наявних на ринку сигналізацій, у яких використовуються LoRa, побудовані схожим чином: вони мають сервер, який збирає інформацію про стани датчиків і завантажує її інтернет. Передбачається, що кожен користувач отримує повідомлення про проникнення на свій девайс і реагувати має сам. Така система не дозволяє захистити віддалену від міста приватну власність, отже сервер має бути замінений на пункт охорони.

					172.4391.КР.ПЗ.Р1		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Бецько І.О.			Структура системи	*Літ.*	*Арк.* 13 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Жук О. К.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 1. СТРУКТУРА СИСТЕМИ

1.1 Опис і складові системи

До складу розробленої сигналізації входять:

- головний пристрій і програма для нього;
- підпорядкований пристрій і програма для нього;
- програма для комп‘ютера;
- протоколи зв‘язку між елементами системи.

Структура системи наведена на рис.1.1.

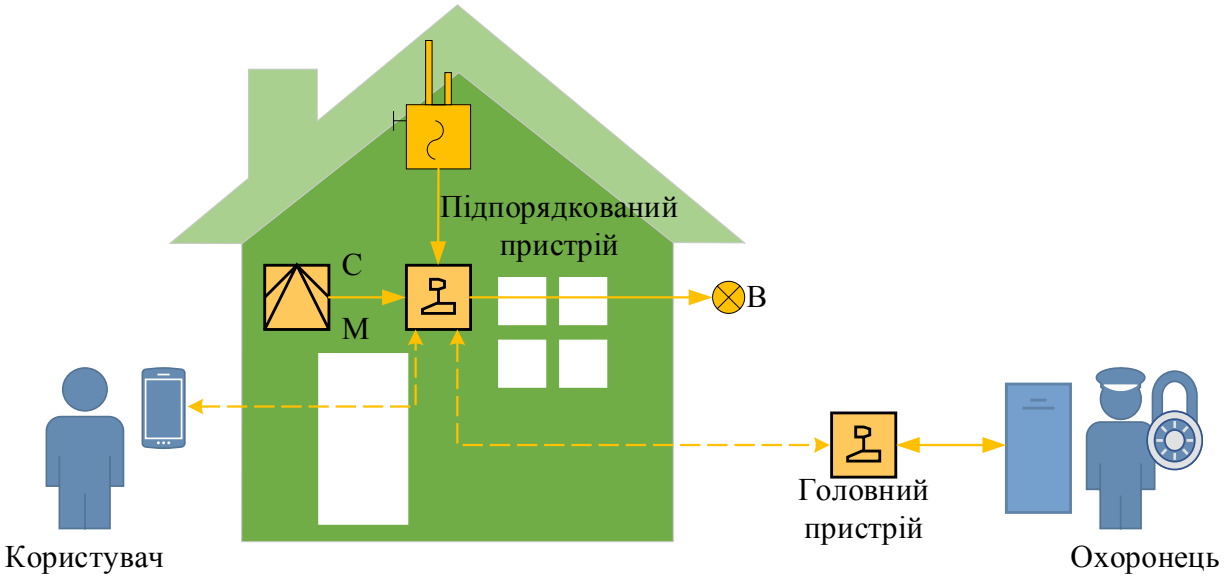


Рис.1.1. Структура системи.

На рис.1.1 присутні :

- користувач, який активує і дезактивує сигналізацію за допомогою смартфону;
- об‘єкт, що охороняються, з підпорядкованим пристроєм та підключеними до нього датчиками;
- підключені до виходів користувача підпорядкованого пристрою навантаження (засоби світло-звукового сповіщення та інше);
- головний пристрій та оператор (охоронець, сторож).

Функції і детальний описи кожної програмної складової і протоколу

містяться у присвячених ним розділах.

1.2 Елементна база

Елементна база розглядається не на рівні електронних компонентів, а на рівні побудованих з них пристроїв/модулів.

1.2.1 Налагоджувальні плати на STM32

Головний і підпорядкований пристрої побудовані на налагоджувальних платах, які мало відрізняються від будь-яких інших налагоджувальних плат для мікроконтролерів загального призначення. Налагоджувальні плати разом із власне мікроконтролерами призначені для обслуговування інтересів розробника програми, тому їх опис розміщений у розділах про вибір мікроконтролерів.

1.2.2 EBYTE E32-868T20D

Спільним для двох пристроїв є використання у них модулів EBYTE E32-868T20D з антенами TX868-JKD-20. Перевагами таких модулів є простота їх використання і налаштування. Суттєвим недоліком модулів є обмеження можливостей технології LoRa і мікросхеми SX1276, які наклали розробники модулів. Головним обмеженням є потужність передачі – 100 мВт.

На момент придбання комплект з двох модулів і двох антен коштував 14$. Самостійна розробка друкованих плат, їх виготовлення і компоненти коштували б набагато дорожче (при виготовленні двох пристроїв), тому використання E32-868T20D було оптимальним рішенням на момент початку розробки.

E32-868T20D містять у своєму складі мікросхему SX1276 і мікроконтролер серії STM32F0, а також елементи, призначені для забезпечення роботи зазначених мікросхем.

Для отримання і передачі даних і налаштувань E32-868T20D має УАПП і ще 3 виводи:

- входи M0 і M1, що визначають режим енергоспоживання і дозволяють повідомити модулю, як сприймати прийняті по

УАПП байти (дані/налаштування);

- вихід AUX, який виконує індикацію станів передачі даних і налаштування.

У режимі сну ({M0,M1} = 0b00) дозволяє змінювати такі параметри:

- адрес;
- канал;
- швидкість УАПП і швидкість безпровідної передачі;
- канал;
- режим передачі (адресний чи прозорий).

1.2.3 USB-TTL перетворювач на CP2102

Хоча обидва використаних мікроконтролери мають USB, я вирішив використовувати для їх підключення до комп‘ютеру USB-TTL перетворювач. Перетворювач коштує 2$ і значно зменшує обсяг роботи програміста, а також обсяг знань, що необхідно мати для встановлення зв‘язку між комп‘ютером і мікроконтролером. USB також потребує наявності платних ідентифікаторів.

1.2.4 Акумулятори і плати контролю заряду акумулятору

Автономне живлення забезпечують літій-іонні акумулятори 18650 у кількості 2 шт. на пристрій. Акумулятори підключені послідовно, оскільки на налагоджувальних платах містяться лінійні стабілізатори AMS1117-3.3, які мають пряме падіння напруги 1.1-1.3В і потребують для стабільної роботи не менше за 4.8В вхідної напруги. Акумулятори не можуть бути підключені до мікроконтролера і модема напряму, оскільки мікроконтролери STM32 допускають напругу живлення до 3.6В.

Розглядалися у якості стабілізаторів TPS76333, які мають пряме падіння напруги до 500мВ і струм до 150мА, чого достатньо для роботи пристрою, але вони можуть бути використані лише за умови виготовлення друкованої плати. З TPS76333 можна було б забезпечити живлення пристрою від одного акумулятору.

Використовується плата контролю заряду на TP4056. Плата

забезпечує безпеку роботи з акумуляторами (захист від короткого замикання, захист від перезаряду тощо), тому її опис у присвяченому охороні праці розділі.

1.2.5 Модуль AT-09 на мікросхемі CC2541

Bluetooth 4.0 використовується для підключення смартфону користувача до підпорядкованого пристрою. Модуль на CC2541 забезпечує передачу даних на дистанцію до 10м, має енергоспоживання < 1мА у режимі очікування; мікросхема сумісна за логічними рівнями і напругою живлення з мікроконтролерами STM32; обмін даними здійснюється по УАПП.

Висновки до розділу 1

Структура розробленої сигналізації схожа на запропоновану Semtech, але змінена згідно з вимогою дешевизни і через відсутність підключення до інтернету.

Розроблені усі елементи системи, окрім програми для смартфону, призначеної для зняття об'єкту з сигналізації шляхом передачі команди і паролю у вигляді *off01234567*, і постановки на сигналізацію командою *on*. Пропонується використовувати з цією метою Bluetooth-термінал.

У розробленій системі використана сучасна елементна база, але вона не ідеально задовольняє вимогам. Головний і підпорядкований пристрої складаються з модулів. Зазначені факти визначають один з напрямів вдосконалення системи – перехід на більш досконалу елементну базу (STM32L0/L4/WB/WL замість STM32F1/F4, SX1276 замість E32-868T20D, NFC замість Bluetooth, мікросхема пам'яті ATECCx08A у кожному мікроконтролері) і розробку друкованих плат.

					172.4391.КР.ПЗ.Р2		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Бецько І.О.			Захист безпровідної мережі і програма для комп'ютера	*Літ.*	*Арк.* 19 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Жук О. К.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 2. ЗАХИСТ БЕЗПРОВІДНОЇ МЕРЕЖІ І ПРОГРАМА ДЛЯ КОМП'ЮТЕРА

Найбезпечнішим способом передачі даних на великі відстані є провідна передача, коли кабель прокладений на контрольованій території. Реалізація провідної передачі даних не є дешевою, та вона не задовольняє вимогам, які висуваються до охоронної сигналізації: оскільки територія не є повністю контрольованою, кабель може бути пошкоджений хуліганами чи зловмисниками.

Безпровідна передача даних не має такого недоліку, але має інші вади: невелика дальність передачі; високий рівень шумів може спотворити дані, що передаються; дані можуть бути зчитані зловмисником; зловмисник може підміняти дані. Зазначені проблеми можуть бути вирішені шляхом задоволення таких вимог:

- використання фізичного рівня LoRa;
- конфіденційності (інформація повинна бути надійно зашифрована);
- цілісності (дані не повинні бути змінені третьою особою);
- автентичності (надійна перевірка того, що дані отримані від правильного джерела).

2.1 Конфіденційність

Конфіденційність інформації – неможливість прочитання інформації стороннім; властивість інформації бути відомою і доступною тільки правомочним суб'єктам системи.

Під шифром розуміється сукупність методів и способів оборотного перетворення інформації з метою її захисту від несанкціонованого доступу (забезпечення конфіденційності інформації).

Складовими елементами шифру є:

- алфавіт для запису вихідних повідомлень (інформації, захист якої виконується; відкритого тексту) й зашифрованих повідомлень (закритих повідомлень, шифротекстів, шифрограм, криптограм);
- алгоритми криптографічного перетворення (шифрування и дешифрування);
- множина ключів.

Шифрування – процес застосування шифру до інформації, що захищається, тобто перетворення вихідного повідомлення в зашифроване.

Дешифрування (розшифрування) – процес, зворотний до шифрування, тобто перетворення зашифрованого повідомлення в вихідне.

Ключ - змінний параметр шифру, що забезпечує вибір одного перетворення з сукупності всіх можливих для даного алгоритму і повідомлення. У загальному випадку, ключ – це мінімальна інформація (за винятком повідомлення, алфавітів і алгоритму), необхідна для шифрування і дешифрування повідомлень.

2.1.1 Порівняння алгоритмів шифрування

Шифрування може бути симетричним і асиметричним. Принципова відмінність між цими двома методами полягає в тому, що алгоритми симетричного шифрування використовують один ключ, в той час як асиметричні використовують два різних, але пов'язаних між собою ключа. Така різниця хоч і здається простою, але вона представляє великі функціональні відмінності між двома формами шифрування і способами їх використання.

При симетричному шифруванні отримувач повинен мати той же секретний ключ, що і відправник. Недоліком симетричного шифрування є можливість зловмисника розшифрувати дані, дізнавшись ключ шифрування.

Асиметричний шифр дозволяє вільно передавати ключ, що використовується для шифрування, а для розшифрування необхідно мати приватний ключ, що забезпечує більшу безпеку.

Окрім відсутності необхідності для однієї з сторін тримати в секреті ключ при асиметричному шифруванні, зазначені шифри відрізняються за такими показниками:

- довжина ключа – у табл.2.1 [2] зіставлені довжини ключів симетричного алгоритму з довжиною ключа алгоритму з відкритим ключем RSA аналогічної криптостійкості;

Табл. 2.1. Порівняння довжин ключів.

Довжина симетричного ключа, біт	Довжина ключа RSA, біт
56	384
64	512
80	768
112	1792
128	2304

- швидкість шифрування-розшифрування на два-три порядки менша при асиметричному шифруванні;
- число ключів, у великих мережах воно менше при асиметричному шифруванні.

Враховуючи вищу швидкість шифрування-розшифрування і меншу довжину ключа, для безпровідної передачі інформації був обраний симетричний шифр.

Наразі існують такі симетричні шифри:

- блокові шифри, які обробляють інформацію блоками певної довжини (зазвичай 64, 128 біт), застосовуючи до блоку ключ в установленому порядку, зазвичай, декількома циклами перемішування і підстановки, що називаються раундами. Результатом повторення раундів є лавинний ефект – втрата відповідності бітів у блоках відкритих і зашифрованих даних.
- потокові шифри, в яких шифрування проводиться над кожним бітом або байтом вихідного (відкритого) тексту з

використанням гамування. Поточний шифр може бути легко створений на основі блочного (наприклад, ГОСТ 28147-89 в режимі гамування), запущеного в спеціальному режимі.

Такі відомі симетричні шифри використовувалися раніше чи використовуються нині:

- блочні: AES, ГОСТ 28147-89, DES, 3DES, RC2, RC5 тощо;
- потокові: RC4, SEAL, WAKE.

2.1.2 Шифрування AES-128

В розробленій сигналізації використовується симетричний алгоритм блочного шифрування AES-128. AES (Advanced Encryption Standard) має розмір блоку 128 біт, ключі можуть бути 128, 192, 256-бітними; вибраний 128-бітний ключ. AES прийнятий в якості стандарту шифрування урядом США за результатами конкурсу AES. Станом на 2009 рік AES є одним з найпоширеніших алгоритмів симетричного шифрування [3].

У червні 2003 року Агентство національної безпеки США постановило, що шифр AES є досить надійним, щоб використовувати його для захисту відомостей, що становлять державну таємницю. Аж до рівня SECRET було дозволено використовувати ключі довжиною 128 біт, для рівня TOP SECRET були потрібні ключі довжиною 192 і 256 біт [4].

У розробці використовується криптографічна бібліотека від STMicroelectronics, яка містить функції для роботи з AES-128, бібліотека описана в окремому підрозділі.

2.1.3 Режим шифрування

При симетричному шифруванні блоковим шифром однакових блоків однаковим ключем отримується однаковий шифротекст, що дозволяє зловмиснику відстежити структуру даних, що передаються. Для ліквідації цього недоліку необхідно використати правильний режим шифрування.

Режим шифрування – такий алгоритм застосування блочного шифру, який дозволяє перетворювати відкритий текст в шифротекст і, після передачі

цього шифротекста по відкритому каналу відновити відкритий текст. Як видно з визначення, сам блоковий шифр тепер є лише частиною іншого алгоритму – алгоритму режиму шифрування. Це обумовлено тим, що блоковий шифр працює тільки з окремим блоком даних, в той час як алгоритм режиму шифрування має справу вже з цілим повідомленням, яке може складатися з деякого числа цілих блоків *n*, або бути доповненим.

У «Рекомендаціях щодо режимів роботи блочних шифрів» НІСТ США [5] представлені п'ять режимів шифрування, що відносяться до будь-якого схваленого НІСТ блокового шифру:

- ECB (Electronic Code Book) – електронна кодова книга;
- CBC (Cipher Block Chaining) – зчеплення блоків за шифротекстом;
- CFB (Cipher Feed Back) – зворотне завантаження шифротекста;
- OFB (Output Feed Back) – зворотне завантаження вихідних даних;
- CTR (Counter) – шифрування з лічильником.

Найпростішим режимом є ECB (рис.2.1), але він не дозволяє приховати структуру даних, тож не використовується у розробці, натомість використаний алгоритм CBC (рис.2.2).

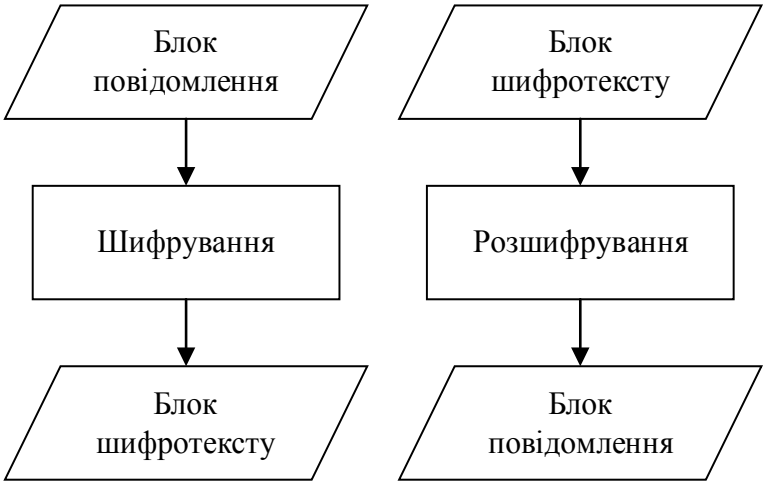


Рис.2.1. Режим шифрування ECB.

З рис.2.2. можна побачити, що режим CBC потребує передачі незашифрованого вектору ініціалізації для розшифрування даних.

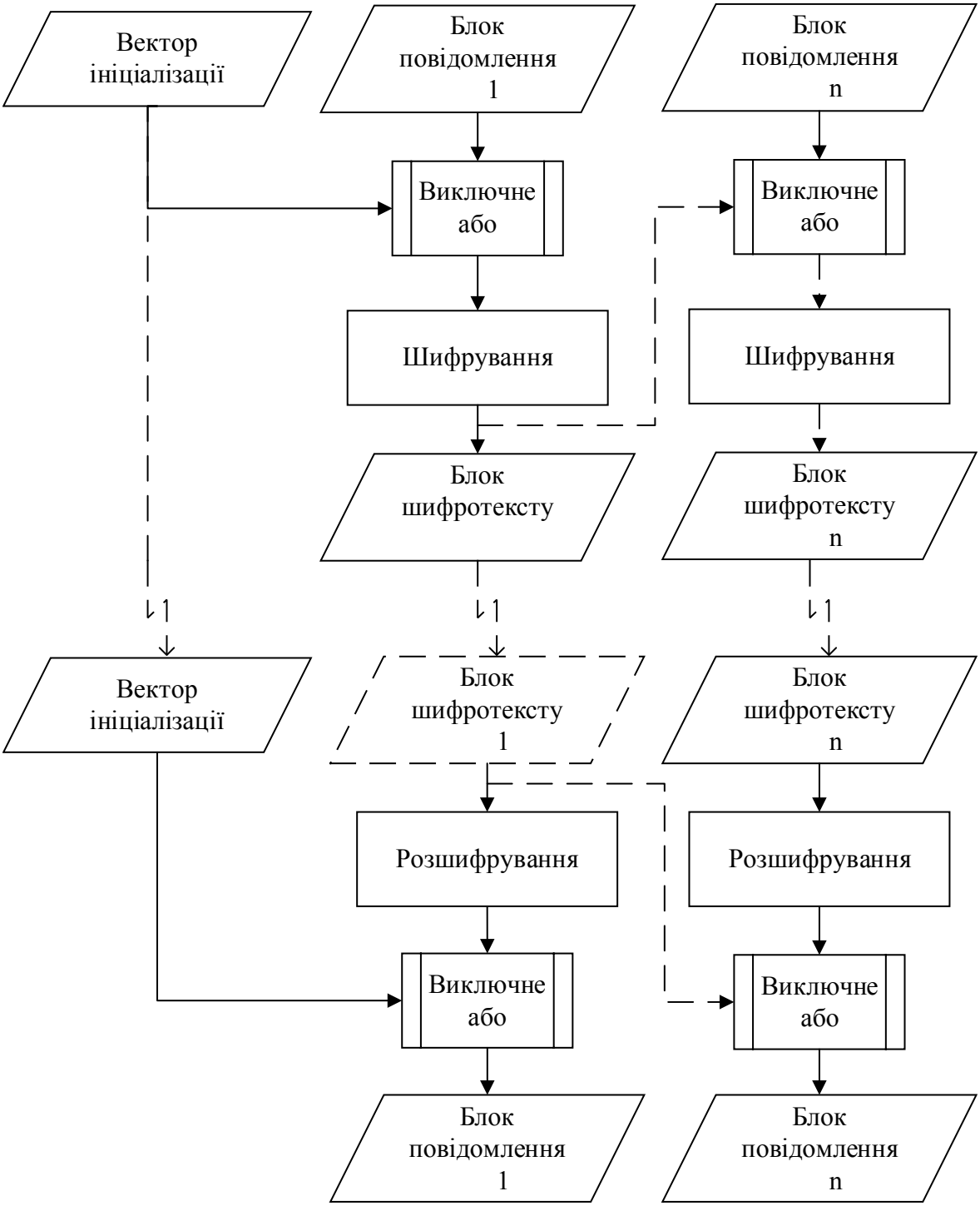


Рис.2.2. Режим шифрування CBC.

Вектор ініціалізації *IV* – це службовий блок даних, який використовується в режимі CBC для приховання структури корисних даних. IV передається незашифрованим, він має бути випадковим при кожній передачі даних, не повинен повторюватися.

Шифрування E_k ключем k першого і наступних блоків повідомлення

P_1, P_i і розшифрування D_k відповідних блоків шифротекста C_1, C_i в режимі CBC описується виразами:

$$C_1 = E_k(P_1 \hat{} IV)$$

$$C_ = E_k(P_i \hat{} C_{-1}), \text{ де } i = 1 \ldots n$$

$$P_1 = D_k(C_1) \hat{} IV$$

$$P_i = D_k(C_) \hat{} C_{-1}, \text{ де } i = 1 \ldots n$$

Перед шифруванням повідомлення в режимі CBC останній блок має бути доповнений до розміру блоку (16 байт). Доповнення може виконуватися декількома різними способами. В розробці використовується доповнення у цілих байтах, при якому значення кожного доданого байту дорівнює числу доданих байт. Наприклад, якщо повідомлення має довжину 45 байтів, останній блок доповнюється трьома байтами {0x03, 0x03, 0x03}.

Функції на мові Сі, що виконують доповнення і шифрування AES-128 в режимі CBC, а також розшифрування і виокремлення корисних даних наведені у додатку А.

2.2 Цілісність

Цілісність інформації – термін, який в контексті розробки означає, що дані не були змінені при їх передачі незахищеним каналом.

Порушити цілісність інформації можуть такі фактори:

- помилка при передачі (завада);
- втручання зловмисників.

Для перевірки цілісності можуть бути використані хеш-функції. Хеш-функція – легко обчислювана функція, яка перетворює вихідну послідовність довільної довжини (прообраз) в число фіксованої довжини. Результат застосування хеш-функції до повідомлення має назву хеш (хеш-код, хеш-образ, дайджест повідомлення (message digest)).

Не всі хеш-функції здатні протистояти криптоаналізу. Отже, не всі хеш-функції є стійкими до втручання зловмисників. У розробці для перевірки

цілісності використана криптографічна (придатна для застосування у криптографії) хеш-функція.

До криптографічних хеш-функцій висуваються такі вимоги:

- для повідомлення *x* неможливо (немає ефективного поліноміального алгоритму [6]) знайти інше повідомлення *y* таке, що $h(x) = h(y)$ при $x \neq y$. Ця властивість називається стійкістю до колізій;
- для певного значення *h(x)* неможливо знайти повідомлення *x*. Ця властивість називається опором до знаходження першого прообразу. Функції, у яких відсутня ця властивість, уразливі для атак пошуку другого прообразу [6];
- при наявності повідомлення m_1, має бути важко знайти інше повідомлення m_2 таке, що $h(m_1) = h(m_2)$ при $m_1 \neq m_2$. Це властивість називається опором пошуку другого прообразу.

На сьогоднішній день широко відомі такі хеш-функції [6]:

- MD4 – швидка у розрахунку, оптимізована під 32-розрядні системи. Розроблена у 1990 р. Рональдом Рівестом, була зламана у 1993 р., не рекомендується до використання;
- MD5 – схожа на MD4, але більш безпечна і на 33% повільніша за MD4. У 2005 р. був описаний алгоритм знаходження колізій. Не рекомендується до застосування;
- SHA-1, SHA-2, SHA-3. SHA-0 розроблена у 1993 р. Агентством Національної Безпеки США, але у ній була допущена помилка, яка у 1995 р. була виправлена у SHA-1. SHA-2 включає алгоритми SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 й SHA-512/224. SHA-3, яка стала переможницею конкурсу криптографічних алгоритмів, є функцією змінної розрядності.

У розробленій безпровідній сигналізації використовується криптографічна хеш-функція SHA-256, як достатньо безпечна і менш

надмірна, ніж інші алгоритми з сімейства SHA-2. Окрім цього, про високий рівень довіри до алгоритму SHA-256 свідчить його використання у криптовалюті bitcoin.

SHA-256 має довжину блоку 64 байти, довжину дайджесту 32 байти. Функції для розрахунку SHA-256 входять до складу криптографічної бібліотеки від STMicroelectronics.

2.3 Автентичність

Автентичність інформації – повнота, справжність і точність інформації; автентична інформація – та, що надійшла від правомочного суб‟єкта системи.

Автентифікація є засобом протидії зловмисникам. Зловмисник може змінити біт(и) повідомлення, видалити з повідомлення біт(и), додати до повідомлення біт(и), змінити порядок слідування бітів у повідомлення. Автентичність пов‟язана з цілісністю, вона досягається схожим чином.

Автентифікація відправника здійснюється шляхом додавання до повідомлення спеціального набору символів, який має назву код аутентифікації (MAC, message authentication code).

MAC може бути отриманий такими способами:

- шифрування хешу отриманого повідомлення симетричним алгоритмом;
- використання останнього блоку повідомлення, зашифрованого блоковим алгоритмом в режимах CBC або CFB, у якості MAC.

Отже з використанням зазначених способів отримання MAC для його вирахування необхідно, щоб з секретний ключ був як в отримувача, так і у відправника.

У розробці використаний код автентифікації на основі хеш-функції (HMAC, hash-based message authentication code). Результатом розрахунку HMAC-SHA-256 є 32-байтовий хеш – функція від ключа і незашифрованого повідомлення.

Алгоритм HMAC записується формулою:

$$HMAC_k(text) = H[(k_0 \hat{} opad)||H([k_0 \hat{} ipad]||text)], \text{ де}$$

^ - викл. або;

|| - конкатенація;

opad – блок виду {0x5c, 0x5c ... 0x5c}, де байт 0x5c повторюється число разів, рівне числу байтів у блоці;

ipad – блок виду {0x36, 0x36... 0x36}, де байт 0x36 повторюється число разів, рівне числу байтів у блоці.

Функції для розрахунку HMAC-SHA-256 входять до складу криптографічної бібліотеки від STMicroelectronics.

2.4 Огляд криптографічної бібліотеки STMicroelectronics

Криптографічна бібліотека STM32 Cryptographic Library є набором скомпільованих файлів для різних сімейств мікроконтролерів і середовищ розробки. При цьому кожен скомпільований варіант реалізації будується за модульним принципом. Така структура дозволяє компілятору використовувати тільки ті модулі, які потрібні користувачеві (AES-CTR, AES-CCM, HASH-SHA тощо), а інші, для економії пам'яті, не включати в проект. Це також дозволяє при необхідності додавати модулі в будь-який момент часу, як тільки це буде потрібно.

Оскільки криптографічна бібліотека представлена у вигляді скомпільованих бібліотечних файлів, то користувачі можуть включати їх в свої проекти, але не можуть вносити в зміни в вихідний текст бібліотеки. З цієї причини кожна бібліотека поставляється в декількох екземплярах: для кожного компілятора (IAR, ARMCC, GCC) і з різними можливостями, такими як оптимізація по швидкості, оптимізація за обсягом пам'яті.

Бібліотека розподіляє мікроконтролери на групи у відповідності до двох своїх версій:

- апаратно-незалежна версія (firmware implementation) – версія, призначена для використання на мікроконтролерах, які не

мають у своєму складі апаратних криптографічних засобів, версія здатна працювати з усіма мікроконтролерами STM32: від STM32F0 до STM32F7;

- апаратно-залежна версія (hardware acceleration library) – заснована на доповненні до програми STM32CubeMX і включає набір крипто-алгоритмів, заснованих на реалізації апаратного прискорення, призначених для використання у всіх серіях STM32, які підтримують апаратну крипто-периферію.

Окрім файлів заголовків і скомпільованих файлів з прототипами функцій, STMicroelectronics постачає шаблони та приклади програм, написані на мові Сі. Для отримання готових криптографічних функцій, оптимізованих для роботи на мікроконтролерах STM32, необхідно завантажити з сайту st.com одну з двох бібліотек:

- STM32 cryptographic library (описана у UM0586), що підтримує 2 компілятори IAR і ARMCC;
- STM32 cryptographic firmware library software expansion for STM32Cube (описана у UM1924), що підтримує IAR, ARMCC, GCC.

Перша версія займає менше пам‘яті, але містить менше прикладів програм для комбінацій середовищ розробки з різними мікроконтролерами і налагоджувальними платами (Discovery, Nucleo, Evaluation).

При скачуванні бібліотеки з сайту st.com користувач отримує архів, при розпакуванні якого створюється складна мережа папок і вкладених директорій. У зазначених двох бібліотеках різна структура розташування файлів: в першій вона простіша – файли бібліотеки згруповані за компіляторами, приклади і шаблони – окремо; в другій файли бібліотеки, шаблони та приклади згруповані за наявністю апаратної підтримки криптографії у мікроконтролерах, а також за сімействами мікроконтролерів.

Всі файли бібліотеки, які стосуються апаратно-залежної частини,

знаходяться в папці AccHw_Crypto (для другої), або мають у складі HW (для першої), а апаратно незалежні - в папці Fw_Crypto, або мають у назві FW. Структура «STM32 cryptographic library» наведена на рис.2.3 зліва. Структура «STM32 expansion for STM32Cube» – на рис.2.3 посередині та справа.

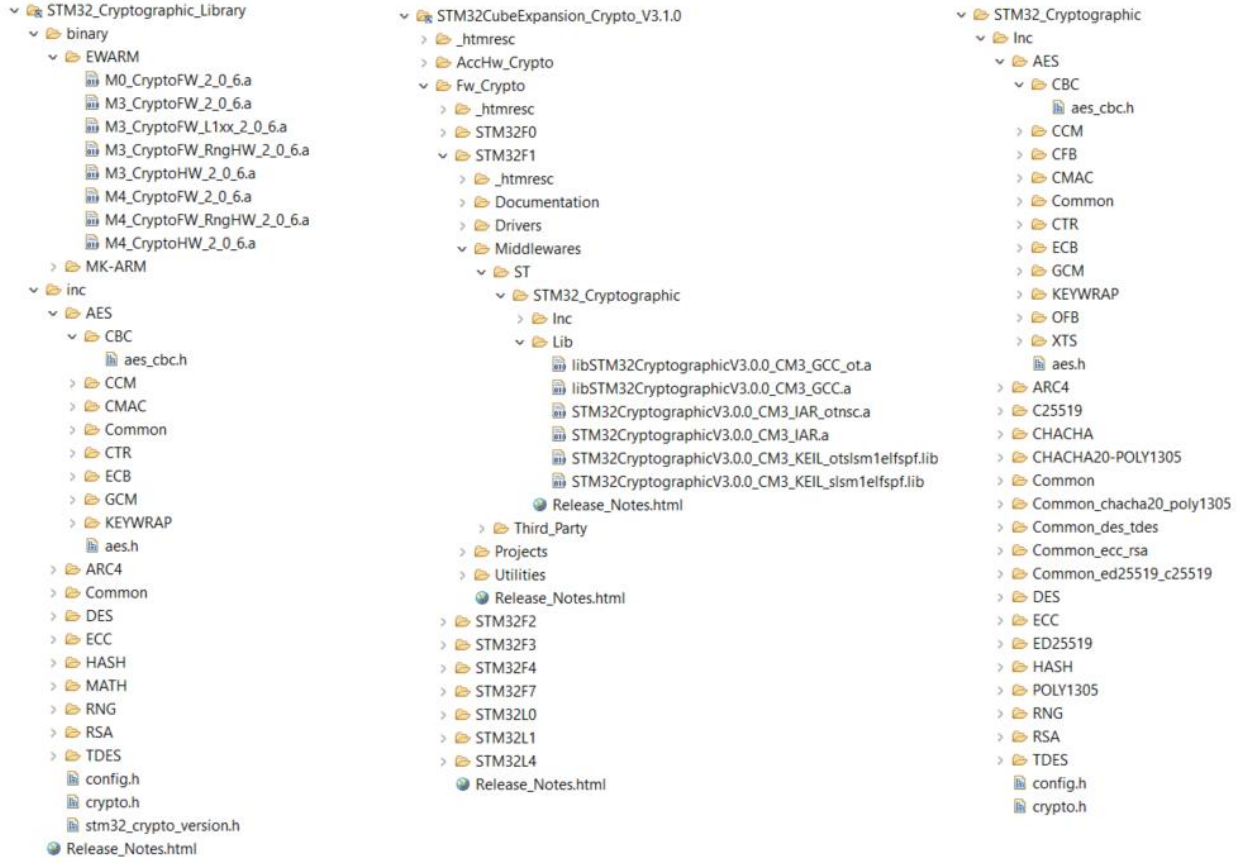


Рис.2.3. Структура криптографічних бібліотек ST.

Назву файлу *M0_CryptoFW_2_0_6_.a* можна зрозуміти так: скомпільовані прототипи функцій криптографічної бібліотеки для роботи з мікроконтролерами на ядрі Cortex-M0 без апаратної підтримки криптографії.

Бібліотека підтримує [7]:

- AES-128, AES-192, AES-256 bits. Supported modes are:
  – ECB (Electronic Codebook Mode)
  – CBC (Cipher-Block Chaining) with support for ciphertext stealing
  – CTR (CounTer Mode)
  – CCM (Counter with CBC-MAC)
  – GCM (Galois Counter Mode)
  – CMAC

– KEY WRAP

- ARC4
- DES, TripleDES. Supported modes are:

– ECB (Electronic Codebook Mode)

– CBC (Cipher-Block Chaining)

- HASH functions with HMAC support:

– MD5

– SHA-1

– SHA-224

– SHA-256

- Random engine based on DRBG-AES-128
- RSA signature functions with PKCS#1v1.5
- ECC (Elliptic Curve Cryptography):

– Key generation

– Scalar multiplication (the base for ECDH)

– ECDSA

У розробці застосовані такі криптографічні алгоритми у складі бібліотеки:

- AES-128-ECB;
- HMAC-SHA-256.

Шифр AES-128 у різних режимах шифрування (AAA у назві функції замінюється на абревіатуру режиму) застосовується шляхом виклику функцій з табл.2.2.

Табл.2.2. Функції шифру AES.

Назва	Опис
AES_AAA_Encrypt_Init	Завантажує ключ і вектор ініціалізації, розділяє ключ на окремі раундові ключі
AES_AAA_Encrypt_Append	Запускає криптографічне перетворення, функцію можна викликати декілька разів

AES_AAA_Encrypt_Finish	Завершує шифрування у режимі AAA
AES_AAA_Decrypt_Init	Завантажує ключ і вектор ініціалізації, розділяє ключ на окремі раундові ключі
AES_AAA_Decrypt_Append	Запускає криптографічне перетворення, функцію можна викликати декілька разів
AES_AAA_Decrypt_Finish	Завершує розшифрування у режимі AAA

Послідовність роботи функцій для виконання шифрування і розшифрування наведена на рис.2.4.

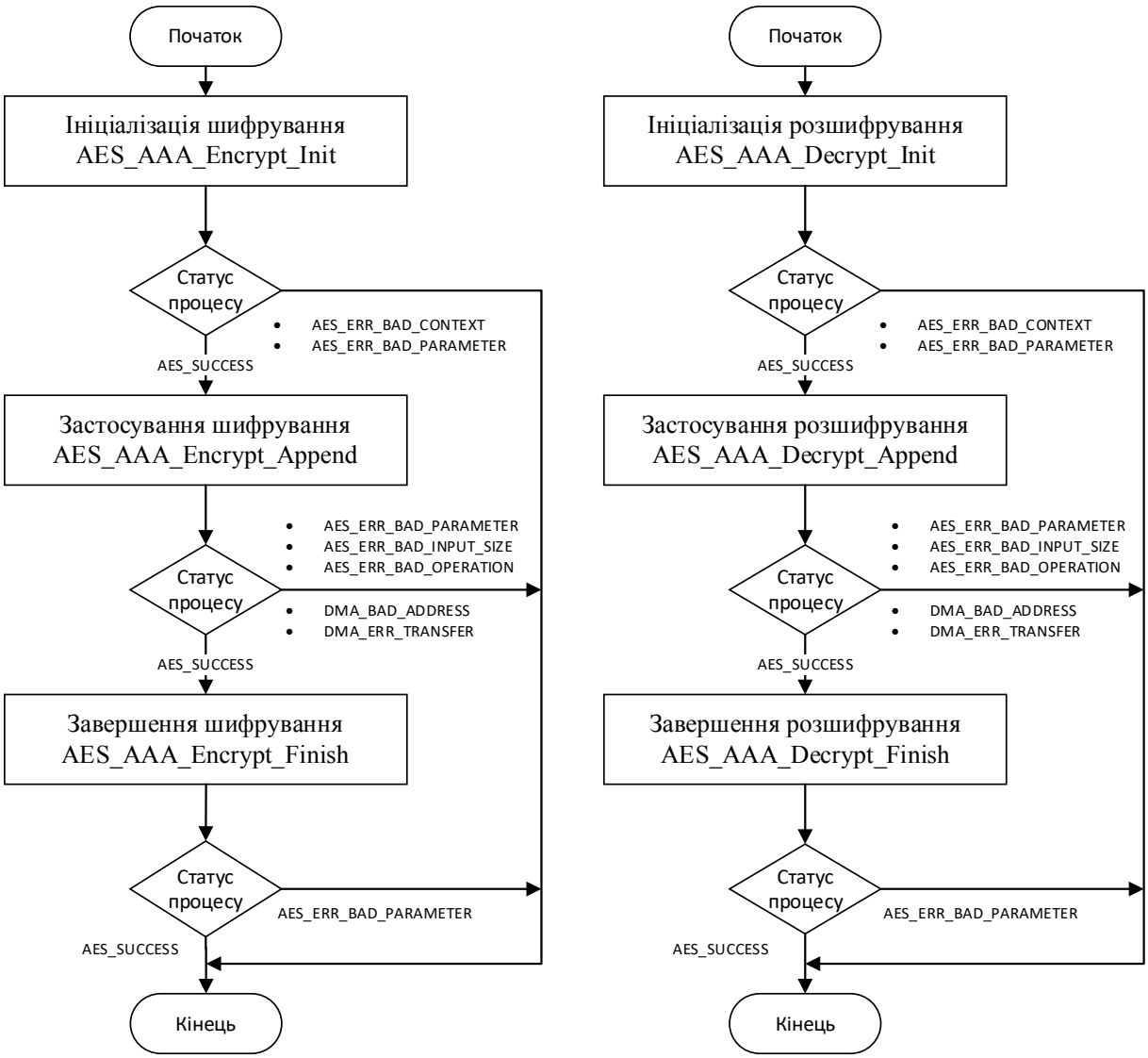


Рис.2.4. Послідовність виклику функцій для шифрування і розшифрування.

Розрахунок коду автентифікації повідомлень з використанням різних хеш-функцій (HHH замінюється на абревіатуру хеш-функції) застосовується

шляхом виклику функцій з табл.2.4. Послідовність роботи функцій для розрахунку коду автентифікації наведена на рис.2.5.

Табл.2.4. Функції коду автентифікації HMAC.

Назва	Опис
HMAC_HHH_Init	Виконує ініціалізацію нового HMAC з вибраною хеш-функцією
HMAC_HHH_Append	Обробляє вхідні дані і оновлює вміст алгоритму HMAC, який підлягає оновленню
HMAC_HHH_Finish	Завершає розрахунок, створює дайджест

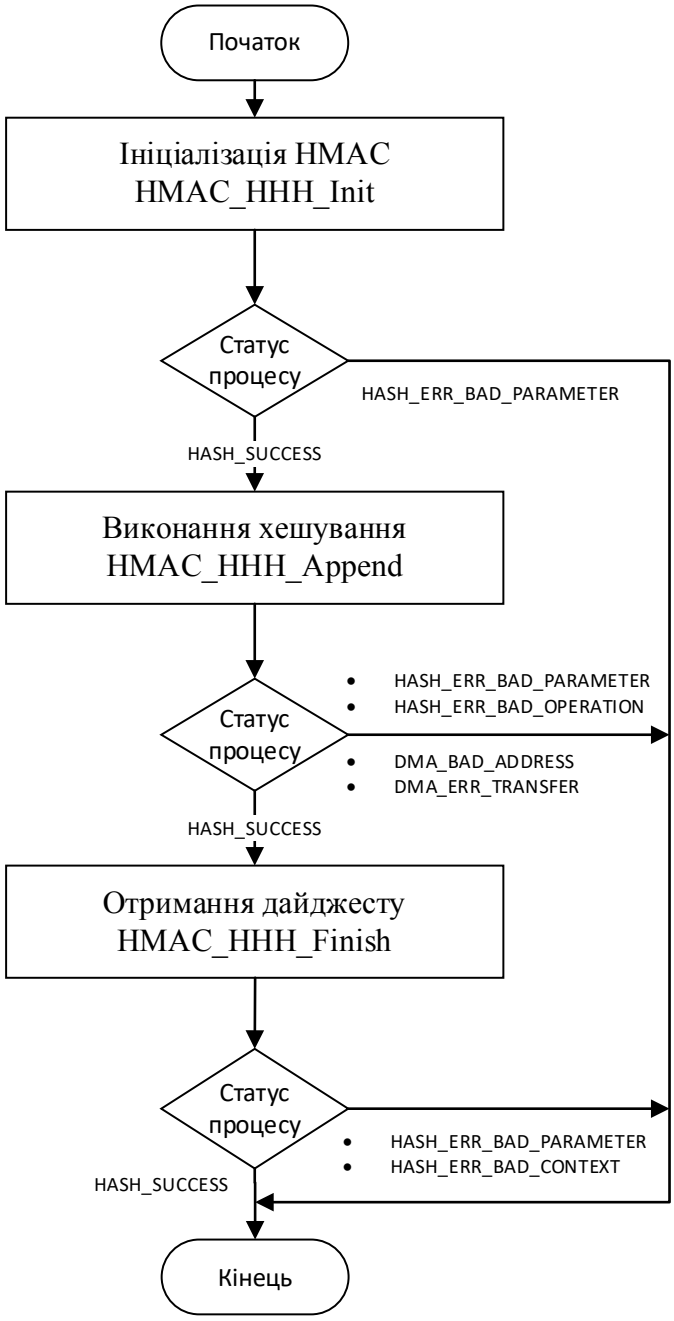


Рис.2.5. Послідовність виклику функцій для розрахунку HMAC.

2.5 Генерація випадкових чисел

Для отримання ключів шифрування, а також для деяких інших цілей, що не пов‟язані з криптографією, має бути згенерована послідовність випадкових чисел.

Генерація випадкових чисел – це процес, який за допомогою пристрою (генератора) створює послідовність чисел або символів, яку неможливо розумно передбачити краще, ніж за допомогою випадкового

шансу. Генератор (псевдо)випадкових чисел може бути програмним і апаратним.

Генератор псевдовипадкових чисел (ГПВЧ) – програмний алгоритм, який породжує послідовність, елементи якої майже не залежать один від одного.

Генерація псевдовипадкових чисел може бути швидкою, але вона не позбавлена недоліків, а саме:

- короткий період;
- значення послідовності не є незалежними;
- деякі біти не настільки випадкові, як інші;
- оборотність.

Хоча й існують криптографічно стійкі генератори псевдовипадкових чисел (придатні до використання у криптографії), ідеального результату з точки зору випадковості і рівномірності розподілу можна досягти з використанням апаратного генератора випадкових чисел.

Апаратний генератор випадкових чисел (АГВЧ) – пристрій, який створює випадкову послідовність з результатів вимірювання фізичних величин у межах випадкового процесу. Саме АГВЧ використаний у розробці.

2.5.1 Випробування різних АГВЧ

Випробувані декілька схем генерації випадкових чисел – різних за надійністю, складністю реалізації, ціною елементної бази та швидкістю.

На рис.2.6 наведена схема генератора випадкового аналогового сигналу і осцилограма сигналу на виході. У моделі шуми замінені джерелом синусоїдної напруги. Шуми стабілітрона мають бути підсилені за напругою операційним підсилювачем і оброблені мікроконтролером.

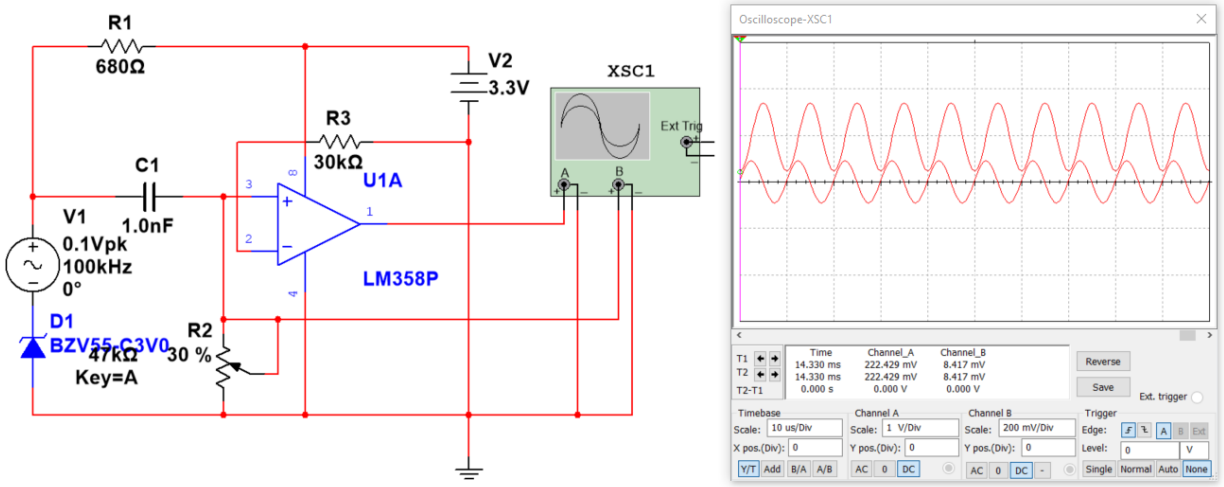


Рис.2.6. Невдалий генератор.

Планувалося подати сигнал з виходу генератора на цифровий вхід мікроконтролера, у якому міститься компаратор; з'ясовувати логічний рівень сигналу, опитуючи періодично цей вхід (з невеликою частотою).

Генератор був зібраний, та при перевірці виявилося, що він не функціонує: на виході незмінно тримається високий рівень або нуль. При виборі великого номіналу для опору R2 (1МОм) – на виході лог.1, при виборі малого номіналу R2 (100кОм) на виході – 0. У результаті експериментів з номіналами R1 і R2, при R2 = 147кОм, отримана генерація прямокутного сигналу частотою 50Гц, хоча використовувалося акумуляторне живлення. Це свідчить про те, що амплітуда наводок більша за амплітуду шуму стабілітрона.

Вважаю, що причинами невдачі були:

- завищені очікування щодо амплітуди шуму на стабілітроні;
- відсутність ОП з великим коефіцієнтом підсилення, задовільними частотними властивостями і малою напругою зміщення;

Інша зібрана схема була схожою на першу, але мала у своєму складі 2 стабілітрона, 2 підсилювача і компаратор, до входів якого були підключені виходи підсилювачів. На практиці ця схема не працювала коректно, як і перша.

Третій генератор також використовував тепловий шум стабілітрона у якості джерела випадковості: напруга на стабілітроні зчитувалася АЦП напряму, використовувався найменш значущий біт, але результати таких вимірювань візуально не відрізнялися від вимірювання «напруги повітря» непідключеним входом АЦП.

2.5.2 Використані у розробці АГВЧ

Існує необхідність формування вектору ініціалізації в підпорядкованому пристрої, вектор не обов‟язково має бути істинно випадковим, але не повинен повторюватися. Тому вимоги до випадкових чисел такі:

- відсутність «скупчень» одиниць і нулів;
- рівномірний розподіл;
- висока швидкість їх отримання.

У підпорядкованому пристрої у якості ГВЧ використовується АЦП, який виконує серію перетворень напруги на непідключеному вході, попутно «збирає» число з молодших розрядів результату перетворення.

Для зменшення впливу невипадкових процесів апаратний генератор підпорядкованого пристрою використовується у зв‟язці з методом Фібоначчі з запізнюванням. У генераторі Фібоначчі використовується формула:

$Y_i = X_{-a} - X_{-b}$, де $a = 17$ і $b = 5$ – магічні числа.

Оскільки у головному пристрої використовується мікроконтролер серії STM32F4, який має апаратний ГВЧ (RNG), він і виступає в ролі криптографічно стійкого ГВЧ для отримання ключів шифрування. Модуль RNG використовує тепловий шум резистора як джерело випадковості.

Функції генерації випадкових чисел наведені у додатку В.

2.5.3 Графічна оцінка використаних АГВЧ

Існують різні математичні методи оцінки випадковості чисел, але я вирішив скористатися простим графічним. На цьому етапі модифікована програма для мікроконтролера: додана команда генерації послідовності і її

друку в USART, отримані дані записуються у файл відповідною функцією термінальної програми; на мові Сі++ з використанням бібліотеки Qt написана призначена для тестів комп'ютерна програма. Програма виконує графічне відображення отриманої послідовності і її гістограми. Код програми наведений у додатку Б. Результати роботи програми при довжині послідовності у 1280 байт на рис.2.7, при довжині у 3200 байт – на рис.2.8. Синім відображається згенерована послідовність (її перші 256 байт), а зеленим – гістограма (масштабована).

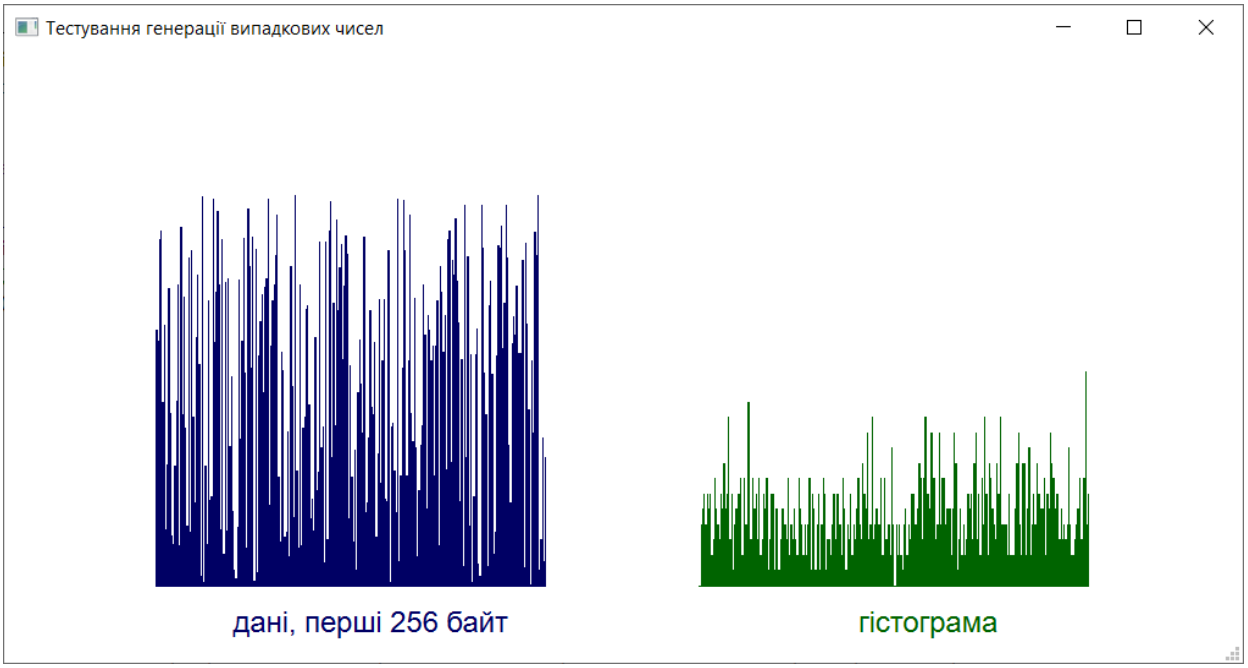


Рис.2.7. «Перевірка випадковості» послідовності з 1280 байт.

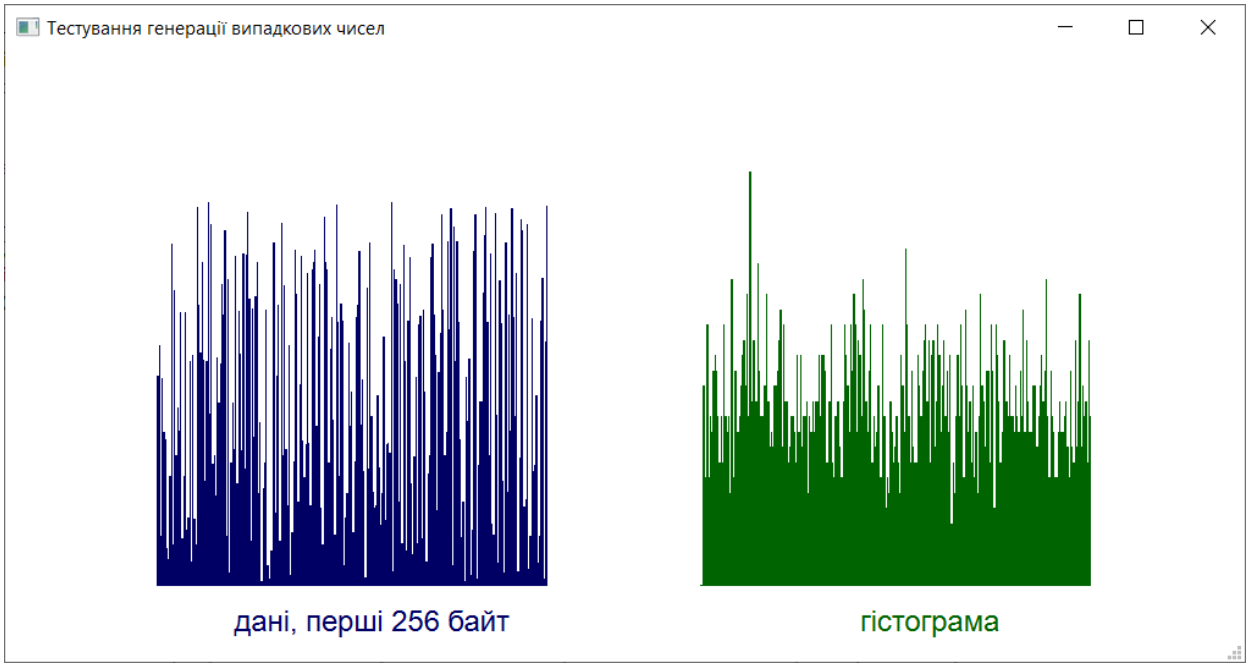


Рис.2.8. «Перевірка випадковості» послідовності з 3200 байт.

Результат перевірки модуля RNG у STM32F4 наведений на рис.2.9.

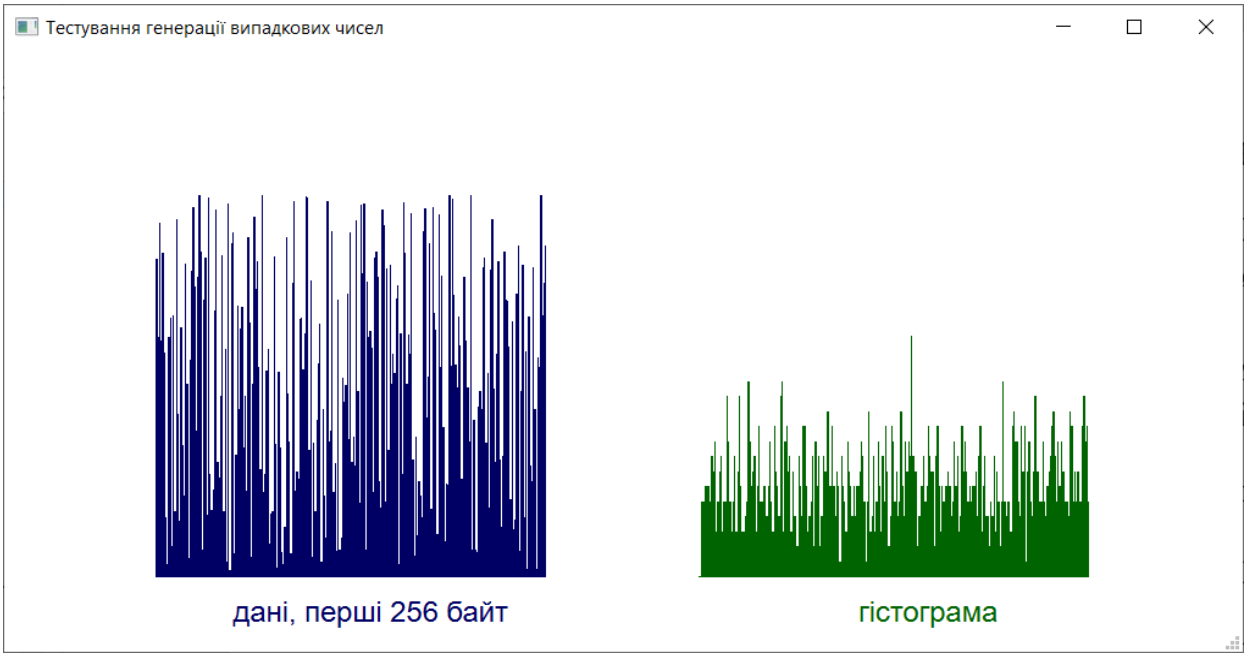


Рис.2.9. «Перевірка випадковості» згенерованої RNG STM32F4 послідовності з 1600 байт.

2.6 Вибір мови програмування і бібліотеки

Додавання нових об‟єктів у систему, зміна каналу радіозв‟язку, запис історії спрацювань сигналізації та багато інших операцій у розробці виконуються комп‟ютерною програмою. Взаємодія пристроїв на базі мікроконтролерів, що входять до складу системи, з користувачем відбувається у графічному інтерфейсі користувача.

Графічний інтерфейс користувача (ГІК) (Graphical user interface, GUI) – система засобів для взаємодії користувача з комп'ютером, заснована на представленні всіх доступних користувачеві об'єктів і функцій у вигляді графічних компонентів екрану (вікон, значків, меню, кнопок, списків тощо).

ГІК у складі комп‟ютерної програми, якщо порівнювати з ГІК на мікроконтролері, є кращим способом відображення інформації, зміни налаштувань і керування роботою розробленої сигналізації. Переваги від його використання:

- зручність користування;
- дешевизна при високій функціональності (мікроконтролеру не потрібен дисплей, не обов‟язкове використання дорогого мікроконтролера);
- гнучкість (можливе використання різних мов програмування, безлічі готових бібліотек та середовищ розробки);
- легкість налагоджування;
- швидкість розробки.

Я розглядаю дві мови програмування, якими я вмію користуватися і вони дозволяють реалізувати графічний інтерфейс користувача під Windows: Сі++ і графічна мова G від National Instruments.

Перевагами графічної МП є простота використання і швидкість розробки, проте вона має обмежене застосування: розробниками передбачене її використання науковцями для збору даних чи управління приладами.

Графічна мова не дозволяє досягнути тих же рівня оптимізації, гнучкості і складності, що властиві програмам, написаним на традиційних МП.

Отже у розробці комп‟ютерної програми з ГІК використана мова Сі++.

Розглянуті дві бібліотеки на Сі++, які дозволяють створювати ГІК:

- Microsoft Foundation Class (MFC) – об‟єктно-орієнтована бібліотека для розробки програм під Windows;
- Qt – об‟єктно-орієнтована бібліотека для розробки ГІК і кросплатформних програм; бібліотека віджетів.

MFC є надбудовою над Windows API, який зорієнтований в основному на мову Сі [8], тож при розробці з використанням MFC часто доводиться заповнювати надмірні структури, де більшість параметрів є не важливими, а також передавати у функції застарілі параметри з неінтуїтивними назвами. Натомість Qt має узгоджене іменування, якісну організацію класів і методів; значення, що повертають функції, логічні; при цьому зберігається функціональність і простота. Після першого використання якогось класу бібліотеки Qt, легко використати й інші, оскільки вони працюють схожим чином.

Враховані переваги Qt, прийняте рішення про використання Qt у розробці. Перелік переваг Qt:

- Qt кросплатформна, тобто дозволяє створювати програми з ГІК для операційних систем Windows, Linux, Android, macOS, iOS, а також для мікроконтролерів STM32 без зміни (або з мінімальними змінами) вихідного коду;
- Qt використовує механізм сигналів і слотів замість функцій зворотного виклику;
- будь-які властивості елементів керування можуть бути редаговані в простому у використанні і зручному Qt Designer; в бібліотеці Qt присутній менеджер компонування;

- Qt має гарно структуровану зрозумілу документацію, що містить приклади коду;

Використання механізму сигналів і слотів дає розробнику такі переваги [8]:

- кожен клас, успадкований від QObject може мати будь-яке число сигналів і слотів;
- повідомлення, що посилаються за допомогою сигналу, можуть мати багато аргументів будь-яких типів;
- сигнал можна з‟єднати з багатьма слотами;
- слот може отримувати повідомлення від багатьох сигналів різних об‟єктів;
- з‟єднувати слот із сигналом можна у будь-якій точці програми;
- при знищенні об‟єкту відбувається автоматичне роз‟єднання сигнально-слотових зв‟язків.

2.7 Огляд графічного інтерфейсу користувача

2.7.1 Головне вікно

Головне вікно програми виконує такі функції:

- підключення до головного пристрою, отримання від нього інформації про наявні ключі шифрування для об‟єктів, повідомлення користувачу стану сигналізації на об‟єктах;
- відкриття і створення файлу зі списком об‟єктів, що відображаються;
- відображення інформаціє про усі об‟єкти з файлу;
- отримання апаратно згенерованих ключів шифрування від головного пристрою, запис ключів у енергонезалежну пам‟ять головного пристрою;
- стирання усіх ключів з пам‟яті головного пристрою;
- відкриття інших вікон програми по запиту користувача, чи при отриманні даних від головного пристрою.

Головне вікно за відсутності підключення до головного пристрою наведене на рис.2.10.

Рис.2.10. Головне вікно програми при відсутності підключення.

Вікно містить:

1. Меню «File», що дозволяє створити, відкрити чи закрити файл зі списком об‘єктів, що відображаються (рис.2.11).

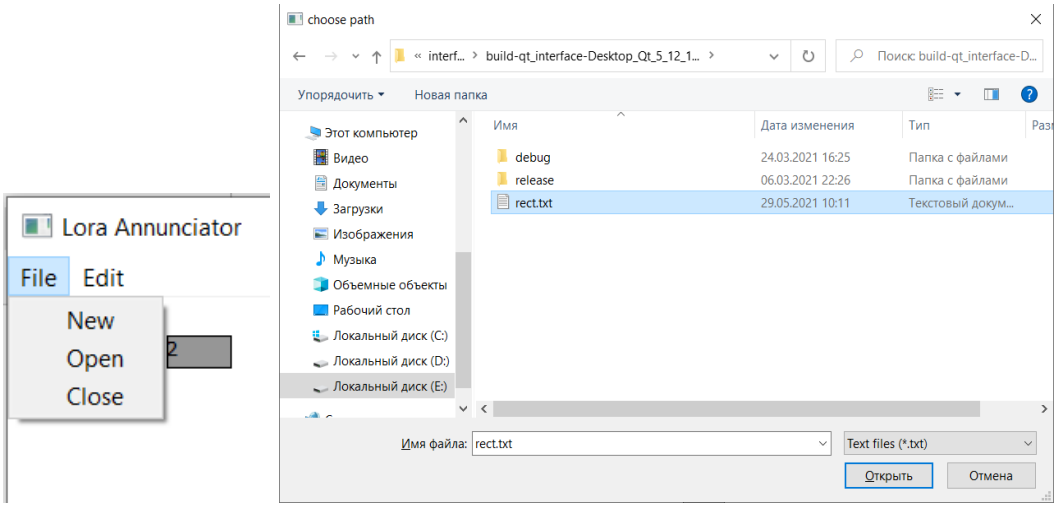


Рис.2.11. Функціонал меню «Файл».

2. Меню «Edit», що дозволяє відкрити вікна, у яких відбувається редагування (рис. 2.12).

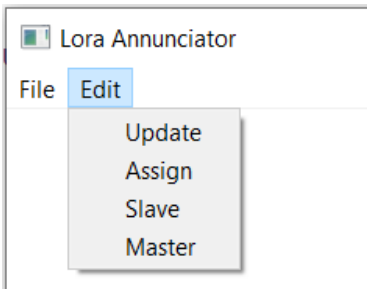


Рис.2.12. Меню «Редагувати».

Кнопка «update» виконує оновлення інтерфейсу – завантажує об‟єкти з файлу, оновлює список доступних для підключення портів, виконує запит списку об‟єктів, для яких вказані ключі шифрування, у головного пристрою (якщо виконане підключення).

3. Поле зі списком, у якому наявні доступні порти; кнопка connect, що дозволяє виконати підключення до активного (вибраного) порту. Елементи поля зі списком оновлюються автоматично за настання певних подій. Користувач може оновити список кнопкою «update».
4. Поле зі списком, у якому наявні усі ID, завантажені з файлу; кнопка «get key», що дозволяє створити запит ключа шифрування; запит здійснюється для активного ID.
5. Кнопка «erase all keys», що виконує видалення усіх ключів і енергонезалежної пам‟яті головного пристрою;
6. Елементи статичного тексту, що позначають сутність елементів контролю;
7. Власне об‟єкти, список яких завантажено з файлу.

Колір об‟єкту свідчить про його поточний стан. В ГІК наявні такі кольори об‟єктів:

- Зелений – нормальний (останнє повідомлення від об‟єкту свідчило про відсутність тривоги);

- Червоний – сигналізація на об‘єкті спрацювала;
- Сірий – для об‘єкта відсутній ключ шифрування.

2.7.2 Вікно додавання нових об’єктів

Вікно на рис.3.4 призначене для додавання на головне вікно нових об‘єктів, які мають бути відображені у головному вікні, охорона яких виконується; має таку ж назву, як і у створеного класу «assign dialog».

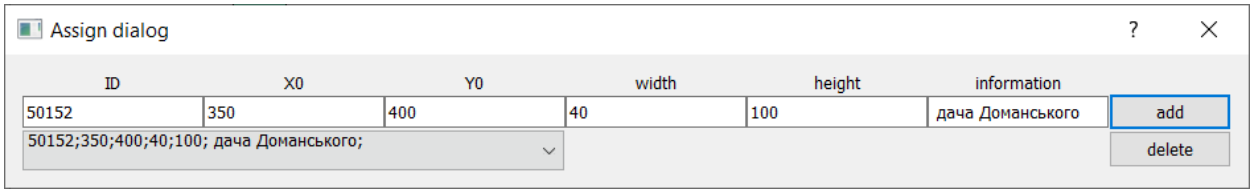


Рис.3.4. Вікно додавання нових об‘єктів

Вікно «Assign dialog» відкривається шляхом натиснення кнопки Assign у меню Edit головного вікна (рис. 2.13).

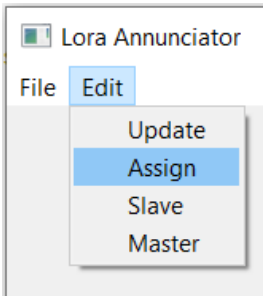


Рис.2.13. Відкриття вікна «Assign dialog».

Вікно відкривається лише у випадку, якщо у головному вікні був відкритий чи створений файл, інакше програма повідомляє про помилку (рис. 2.14).

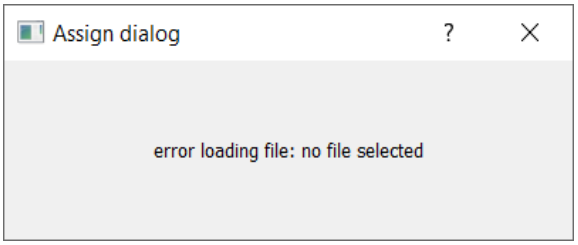


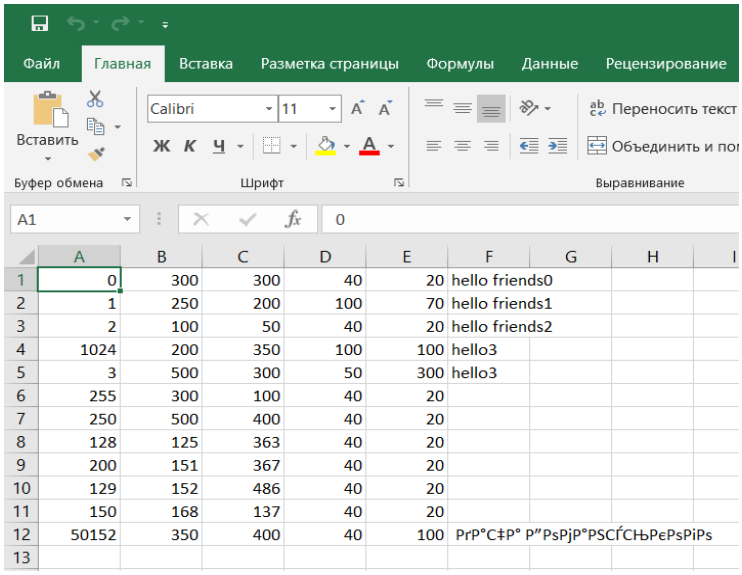
Рис.2.14. Файл не вибраний.

Вікно «Assign dialog» містить елементи статичного тексту, які позначають сутність полів для вводу, що розташовані нижче під текстом. Поле ID означає ідентифікатор об‘єкту, що додається, ID може приймати

значення від 0 до 65535. Чотири наступні поля (x0, y0, width, height) задають позицію та розмір відображуваного на головному вікні прямокутного елементу, що позначає об‟єкт. Поле information дозволяє додавати будь-яку текстову інформацію про об‟єкт, але ця інформації не має містити знак ; .

У вікні (рис.3.4) присутні 2 кнопки: додати (add) і видалити (delete). Кнопка «add» додає у файл нову строку даних, складену з введених у поля значень, розділених знаком ;. При натисканні «add» відбувається призначення об‟єкту з вибраним ID позиції на головному вікні програми. «delete» видаляє з файлу поточну (вибрану полем зі списком) строку. Оновлення головного вікна відбувається одразу після додавання чи видалення об‟єкту.

Усі введені дані записуються у вибраний у головному вікні .txt файл у текстовому вигляді (придатному для редагування і перегляду людиною). Цей файл можна відкрити у блокноті і редагувати, а можна змінити його розширення з .txt на .csv і відкрити у програмі Excel (рис. 2.15), хоча Excel без виконання додаткових дій некоректно відображає українські символи.



	A	B	C	D	E	F	G	H
1	0	300	300	40	20	hello friends0		
2	1	250	200	100	70	hello friends1		
3	2	100	50	40	20	hello friends2		
4	1024	200	350	100	100	hello3		
5	3	500	300	50	300	hello3		
6	255	300	100	40	20			
7	250	500	400	40	20			
8	128	125	363	40	20			
9	200	151	367	40	20			
10	129	152	486	40	20			
11	150	168	137	40	20			
12	50152	350	400	40	100	PrP°C‡P° P”PsPjP°PSCЃCЊPєPsPiPs		
13								

Рис.2.15. Вміст файлу objects.csv.

2.7.3 Вікно налаштування підпорядкованого пристрою

Зовнішній вигляд вікна налаштування підпорядкованого пристрою на об‟єкті «Slave dialog» наведений на рис.2.16.

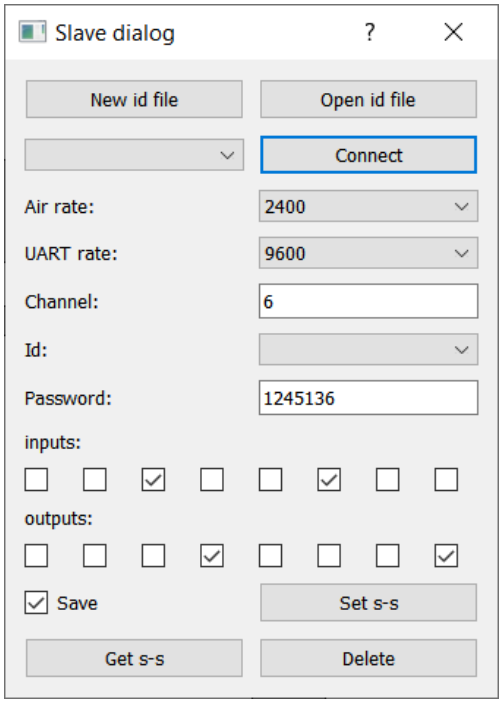


Рис.2.16. Зовнішній вигляд вікна «Slave dialog».

Вікно «Slave dialog» відкривається при натисненні кнопки «slave» у меню головного вікна програми (рис.2.17).

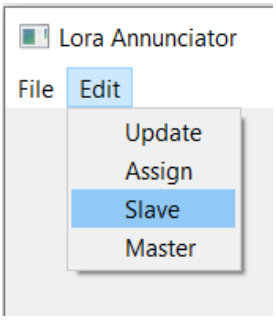


Рис.2.17. Відкриття вікна «Slave dialog».

Вікно дозволяє налаштовувати підпорядковані пристрої перед їх розміщенням на об'єктах, що охороняються. У вікні наявні:

- кнопки для створення і відкриття файлів із розширенням .midf;
- поле зі списком, у якому відображаються наявні послідовні порти, а також кнопку «connect» підключення до вибраного порту;
- два поля зі списком. «air rate» дозволяє задати швидкість передачі даних радіоканалом у бітах/секунду, «UART rate» –

швидкість USART між модулем радіозв‘язку і мікроконтролером;

- поле «channel», що задає канал радіозв‘язку;
- поле зі списком «id», яке дозволяє вибрати ідентифікатор об‘єкту, на якому буде розташовано пристрій, налаштування якого відбувається;
- поле «password», яке містить пароль зняття з сигналізації;
- прапорець «save» для збереження налаштувань;
- кнопки «set settings», «get settings», «delete», які призначені для встановлення налаштувань (передачі їх по послідовному порту і запис у файл), отримання актуальних налаштувань, видалення отриманих налаштувань з відкритого файлу.

Файл з розширенням .midf (microcontroller identifier file) не призначений для редагування і перегляду користувачем у іншому ПЗ, окрім розробленої програми. Введення даних у файл і видалення їх звідти виконуються лише при отриманні відповіді «успіх» від налаштовуваного пристрою.

Після відкриття вікна поле зі списком «id» наповнюється елементами не одразу, послідовність цього процесу показана на рис.2.18.

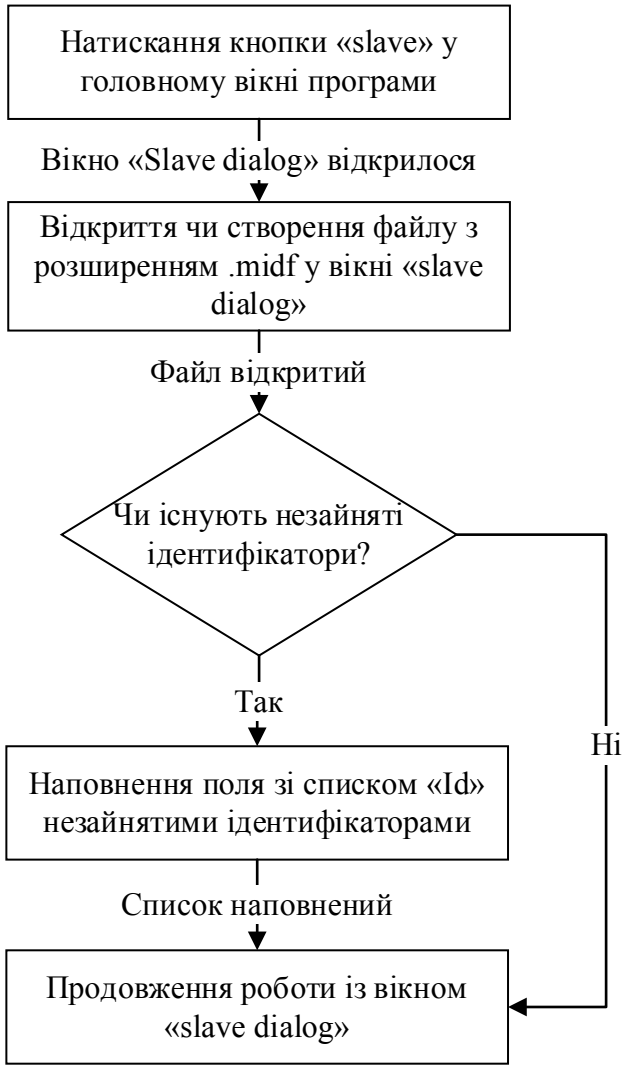


Рис.2.18. Послідовність наповнення поля зі списком «id».

Під умовою «чи існують незайняті ідентифікатори?» розумію зіставлення умісту файлу головного вікна з розширенням .txt із умістом файлу з розширенням .midf і виявлення ідентифікаторів, які наявні у файлі .txt, але відсутні у .midf.

2.7.4 Вікно перевірки стану об'єкту/тривога на об'єкті

Вікно перевірки стану об‟єкту/тривога на об‟єкті призначене для інформування про стан датчиків на об‟єкті, вікно «site check» може бути викликане шляхом натискання на умовне графічне зображення об‟єкту на головному вікні програми. На рис.2.19 наведений зовнішній вигляд вікна при виявленні спрацювання датчиків руху, диму, розриву струмопровідної стрічки, а також перевищення температурою порогового значення.

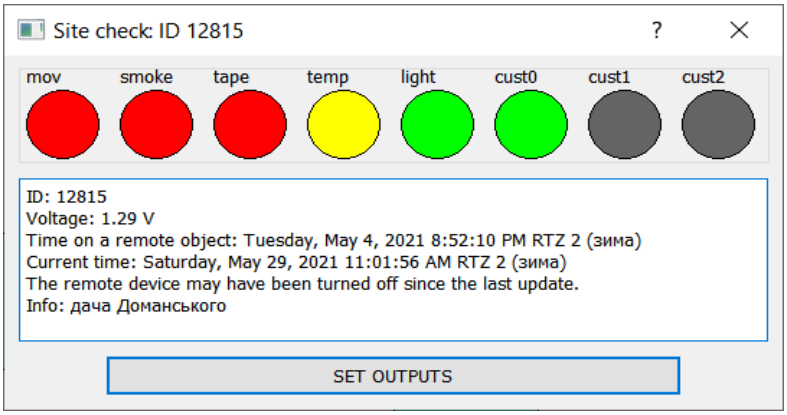


Рис.2.19. Вікно «site check».

Вікно «site alarm» має такий же вигляд, але викликається програмою автоматично при приході повідомлення про спрацювання сигналізації і має обмежений термін життя (закривається автоматично, якщо нових спрацювань датчиків не відбувається впродовж терміну життя вікна). Запис про спрацювання зберігається у відповідному файлі.

Червоний колір датчиків означає, що датчик зараз в стані спрацювання. Жовтий – що датчик спрацьовував нещодавно, але наразі повернувся до нормального стану (тривога відсутня). Зелений – датчик не спрацьовував давно. Сірий – датчик відімкнений (вхід не підтримується).

Окрім станів датчиків, вікно відображає ще таку інформацію:

- ідентифікатор;
- напругу акумулятору;
- час на віддаленому об‘єкті (на момент отримання відповіді);
- поточний час;
- інформацію про об‘єкт.

Якщо час на відділеному об‘єкті менший за поточний час, пристрій міг бути відключений зловмисником.

У вікні присутня кнопка «set outputs», вона дозволяє викликати вікно встановлення виходів.

2.7.5 Вікно встановлення виходів

Вікно встановлення виходів (рис.2.20) викликається з вікна «site check»/«site alarm».

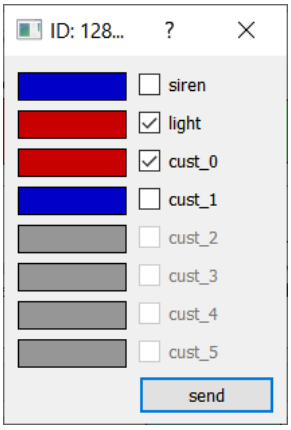


Рис.2.20. Вікно встановлення виходів.

Вікно містить:

- ідентифікатор пристрою, виходами якого здійснюється управління;
- назви виходів;
- стани виходів;
- прапорці, якими здійснюється вибір стану кожного з виходів;
- кнопка відправки команди на управління виходами «send».

Червоним кольором виділені активні виходи, синім – не активні, сірим – виходи, що не підтримуються.

2.7.6 Вікно налаштування головного пристрою

Вікно налаштування головного пристрою (рис.2.21) викликається з меню edit головного вікна.

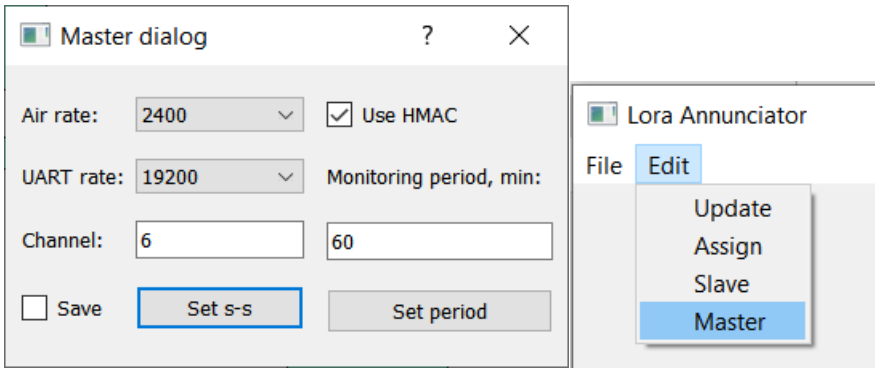


Рис.2.21. Вікно «Master dialog» і його відкриття.

Вікно «Master dialog» має у своєму складі такі ж п‘ять елементів керування, що є у «Slave dialog»: поля зі списком для задання швидкості

радіозв‘язку і швидкості УСАПП, поле для каналу, прапорець збереження налаштувань і кнопка встановлення налаштувань.

Вікно також містить поле «monitoring period», у яке записується період моніторингу підпорядкованих пристроїв. Період моніторингу встановлюється кнопкою «set period». Прапорець «use HMAC» визначає, чи буде використаний HMAC для верифікації і перевірки цілісності.

Параметри періоду моніторингу і використання HMAC не зберігаються, оскільки вони не впливають на налаштування модулю радіозв‘язку. При натисненні кнопки «set settings», якщо встановлений прапорець «save», відбувається запис налаштувань у файл «master_info.txt»; файл розміщується у тій же папці, де розміщений виконуваний файл програми.

Перед відкриттям «Master dialog» має бути виконане підключення до послідовного порту у головному вікні програми.

Висновки до розділу 2

У розробленій системі використані сучасні засоби захисту інформації.

Блоковий шифр AES-128 у режимі CBC забезпечує конфіденційність даних і приховання структури даних, що передаються.

Код аутентифікації HMAC на основі криптографічної хеш-функції SHA-256 забезпечує цілісність та аутентифікацію.

AES-128 і HMAC-SHA-256 вважаються безпечними і широко використовуються.

Досліджені апаратні генератори випадкових чисел, використані лише реально робочі. Для генерації ключів шифрування у головному пристрої використаний RNG у STM32F4, що пройшов тест на випадковість. Міра випадковості не призначеного для криптографії генератора підпорядкованого пристрою збільшена використанням методу Фібоначчі з запізненням.

Використання усіх зазначених засобів дозволяє захистити систему від втручання зловмисників.

Розроблена на Сі++ комп‘ютерна програма використовує найкращу і широко відому бібліотеку Qt. Інтерфейс програми мінімалістичний, красивий і зручний, користувачеві буде просто розібратися в усіх функціях ГІК.

Програма записує важливі дії користувача у файли, фіксує спрацювання сигналізації; зберігає адреси файлів у реєстрі операційної системи. У файлів, призначених для зберігання інформації про підключені підпорядковані пристрої, різні розширення – таким чином позначені файли, редагування яких передбачено користувачем, і ті, редагування яких може відбуватися лише у розробленій програмі.

Передбачений захист від випадкових натиснень (кнопки стирання ключів шифрування у головному вікні програми), від помилкових дій користувача. Програма сповіщає користувача про важливі події інформативними повідомленнями у вікнах повідомлення і у рядку стану головного вікна.

Обмін даними по послідовному порту реалізований асинхронно (програма для ПК не очікує у циклах, не зависає).

					172.4391.КР.ПЗ.Р3			
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*				
Розробник		Бецько І.О.			Підпорядкований і головний пристрої	*Літ.*	*Арк.*	*Аркушів*
Консультант							55	
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова		
Керівник		Жук О. К.						
Зав. каф.		Рябенький В. М.						

РОЗДІЛ 3. ПІДПОРЯДКОВАНИЙ І ГОЛОВНИЙ ПРИСТРОЇ

Підпорядкований пристрій розміщується на підохоронному об‟єкті. Слово «підпорядкований» означає, що при відсутності тривоги ініціювати обмін даними може лише головний пристрій, розміщений на пункті охорони. Але у стані сигналізації ініціює передачу даних підпорядкований пристрій

3.1 Вибір і огляд мікроконтролера підпорядкованого пристрою

3.1.1 Вибір мікроконтролера підпорядкованого пристрою

Вимогами до мікроконтролера підпорядкованого пристрою є:

- достатнє, але не надмірне число виводів;
- наявність трьох УАПП/УСАПП;
- наявність годинника реального часу;
- наявність мікроконтролера на ринку при невисокій вартості;
- достатня продуктивність (розрядність і тактова частота);
- робота від 3.3 В, енергоефективність;
- швидкий з 12-розрядним АЦП;
- наявність якісної документації.

Потреба у наявності трьох УАПП зумовлена пристроями, що підключаються до мікроконтролера, а саме:

- USB-TTL перетворювач;
- модуль радіозв‟язку;
- Bluetooth модуль.

Однією з найважливіших вимог, хоча і суб‟єктивною, є наявність у мене як розробника теоретичних знань і досвіду програмування мікроконтролерів певного виробника.

Розглянуті мікроконтролери таких відомих виробників та їх сімейства (8-бітні не розглядаються):

- STMicroelectronics, STM32;
- Espressif Systems, ESP32;

- Microchip, PIC32MX;
- Microchip, AT32UC (ядро AVR32);
- Texas Instruments, MSP430.
- Texas Instruments на ядрах ARM.

Мікроконтролери PIC32MX задовольняють технічним вимогам, але не є доступними і поширеними, а також мають середньо-високу ціну. До того ж я не маю досвіду програмування PIC мікроконтролерів.

Мікроконтролери на AVR32 також задовольняють технічним вимогам, але є недешевими і мало розповсюдженими.

Розповсюджені мікроконтролери MSP430 мають низьку ціну, але задовольняють не всім технічним критеріям. «Потужні» MSP430, як і мікроконтролери Texas Instruments на ядрах ARM, не є розповсюдженими і мають зависоку ціну.

Головними конкурентами є STM32 і ESP32. Існують недорогі плати з мікроконтролерами STM32 і ESP32: STM32 Blue Pill і ESP32-WROOM-32. Плати є доступними, а використані у них мікроконтролери задовольняють технічним критеріям, тому порівнювати їх слід за якісними, у деякій мірі суб‟єктивними показниками (табл.3.1).

Показник	ESP32-D0WDQ6	STM32F103C8
Наявність Bluetooth	Наявний	Не наявний
Виробник,	Espressif Systems, Китай	STMicroelectronics, Європа
Гарантія	12 років	10 років
Документація	Наявна	Відмінної якості
Розповсюдженість навчальних матеріалів, прикладів коду	Середня	Дуже висока
Програмне забезпечення для розробки	Arduino IDE, PlatformIO	EWARM, uVision, TrueSTUDIO, SW4STM32, CoIDE, CubeIDE, CubeMX.

Найнижча поточна ціна (з доставкою)	6,17 $	4,39 $

Табл.3.1. Порівняння мікроконтролерів.

Хоча вибрана плата ESP32 дорожча від плати на STM32, але використаний у ній мікроконтролер має модуль Bluetooth, який використовується у розробці. Переваги ESP32 у продуктивності не враховуються, оскільки обидва мікроконтролери мають відмінну продуктивність. Натомість враховується всесвітнє ім'я бренду ST, велике число середовищ розробки і наявність якісних бібліотек різного рівня абстракції.

Важливою перевагою мікроконтролера від ST є можливість перенесення програми у майбутньому на більш відповідні до вимог проекту мікроконтролери ST, які наразі в Україні не доступні або дуже дорогі.

4.1.2 Огляд мікроконтролера підпорядкованого пристрою

У роботі використаний мікроконтролер STM32F103C8T6 на платі Blue Pill. STM32F103C8T6 має такі особливості:

- 32-розрядне ядро ARM Cortex-M3, максимальну частоту 72 МГц, продуктивність 1,25 DMIPS / МГц, апаратне ділення;
- 64 Кбайт пам'яті flash, 20 Кбайт SRAM;
- 37 виводів загального призначення, усі можуть бути налаштовані в режимі зовнішніх переривань (16 векторів);
- 7 таймерів;
- 3 УСАПП, 2 SPI, 2 I2C;
- годинник реального часу і 2 режими пониженого енергоспоживання;
- 12-розрядний АЦП (до 16 каналів);
- корпус LQFP-48.

На платі містяться також зовнішні кварцові резонатори на 8МГц і 32.768 кГц, кнопка скидання та інші обов'язкові елементи.

3.2 Опис роботи програми підпорядкованого пристрою

Програма для STM32F103C8 написана з використанням МП Ci, бібліотек CMSIS, HAL, STM32 cryptographic library, а також програми CubeMX, у якій виконувалася ініціалізація.

CMSIS – рівень апаратної абстракції ядра ARM Cortex-M.

HAL – рівень апаратної абстракції регістрів мікроконтролера.

Бібліотека HAL потребує більше ресурсів і працює повільніше, ніж запис в регістри, тому застосовується лише там, де її використання дозволяє зекономити час.

3.2.1 Функції програми підпорядкованого пристрою

Функціями програми підпорядкованого пристрою є:

- перевірка стану цифрових і аналогових датчиків, виявлення проникнення й інших подій;
- передавання інформації про події на пункт охорони;
- надання відповідей на запити головного пристрою;
- перевірка працездатності підпорядкованого пристрою (перевірка заряду акумулятору);
- вимкнення сигналізації користувачем;
- зміна налаштувань (у тому числі паролю) у відповідності до отриманих від користувача команд.

3.2.2 Діаграма станів і переходів підпорядкованого пристрою

Діаграма станів і переходів наведена на рис.3.1.

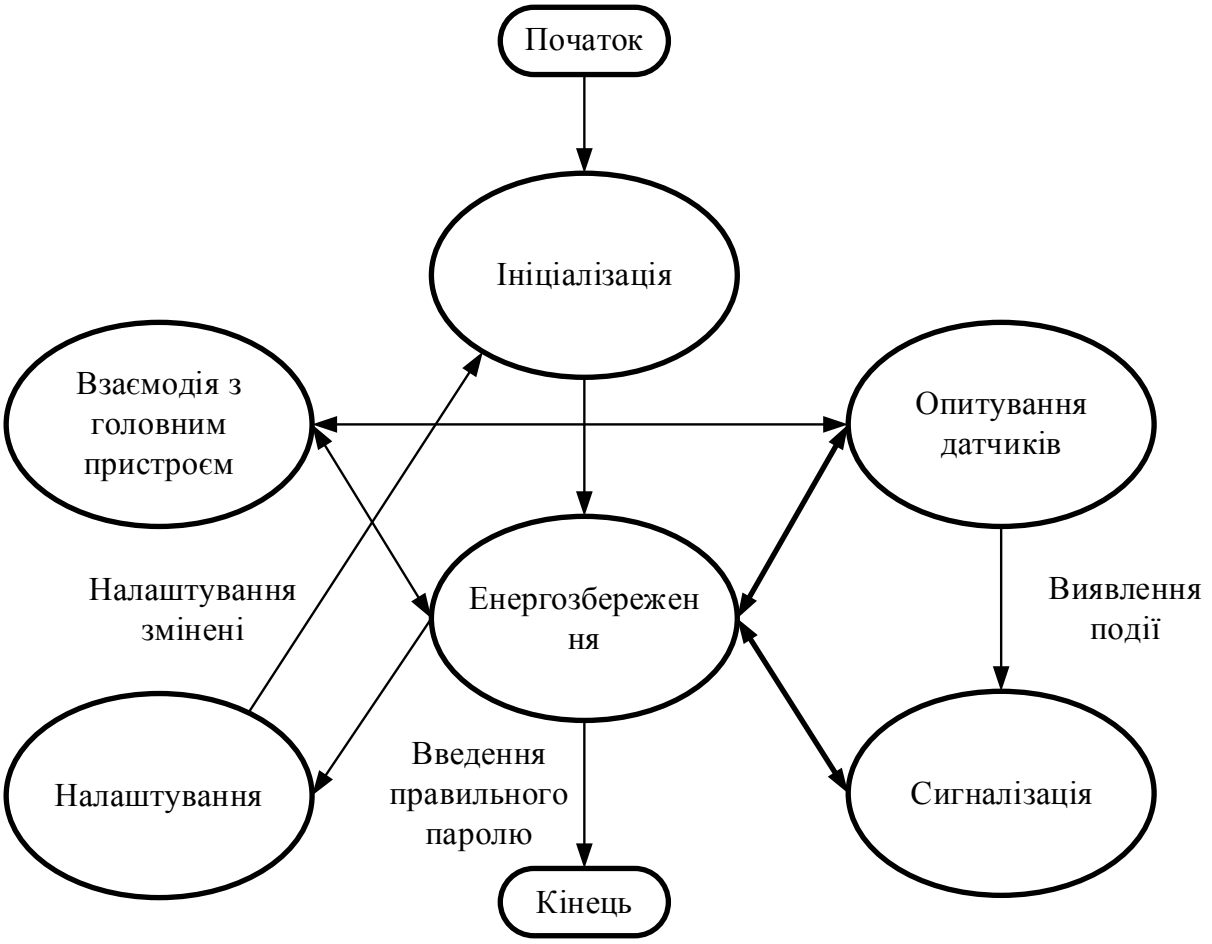


Рис.3.1. Діаграма станів і переходів.

Режимами я називаю такі стани, у які пристрій вводить користувач.

Режим ініціалізації полягає у ввімкненні і налаштуванні периферії. Налаштування периферії у режимі ініціалізації відбувається у відповідності до вмісту flash пам‟яті мікроконтролера.

Режим налаштування може бути викликаний користувачем з ГІК на ПК у перші 60 секунд роботи програми підпорядкованого пристрою. Через 60 с. роботи програми, якщо режим налаштування не був викликаний, програма з метою енергозбереження виконує де-ініціалізацію УАПП1, який відповідає за зв‟язок з комп‟ютером. Режим налаштування передбачає зміну вмісту користувацької області flash; підлягають зміні такі параметри:

- параметри модулю радіозв‟язку і швидкость УСАПП, призначеного для роботи із модулем радіозв‟язку;
- пароль;

- ключ шифрування;
- входи і виходи, що підтримуються;
- поточний час.

Користувач має виконати скидання після зміни налаштувань.

Стан енергозбереження – основний стан програми. У нього мікроконтролер повертається автоматично з інших станів. З метою енергозбереження відключається тактовий сигнал ядра і уся периферія, що не використовується (входи і виходи, таймери, АЦП тощо).

Опитування датчиків – періодичний процес, за якого відбувається зчитування станів цифрових і аналогових входів. Цифрові входи використовуються з перериваннями, тому реакція на зміну стану цифрового входу миттєва; покази АЦП зчитуються та аналізуються з періодом 1 секунда, інтервал відлічується годинником реального часу RTC.

Якщо в результаті опитування датчиків виявлене їх спрацювання чи вихід показів АЦП за визначені межі, відбувається перехід у стан сигналізації, з якого пристрій відправляє дані на пункт охорони.

Взаємодія з головним пристроєм включає отримання від нього запиту на надання даних і відповідь на цей запит, а також дистанційне управління виходами. Підпорядкований пристрій зчитує і опрацьовує стани датчиків негайно при отриманні запиту від головного пристрою.

3.3 Підключення Blue Pill підпорядкованого пристрою

До Blue Pill підключаються зазначені у першому розділі пристрої, а також датчики і виконавчі пристрої.

Перелік датчиків і умови їх спрацювання (активний рівень) наведені в табл.3.2.

№	0	1	2	3	4	5	6	7
Датчик	MOV	SMOKE	TAPE	TEMP	LIGHT	CUST1	CUST2	CUST3
Тип	Цифр.	Цифр.	Цифр.	Аналог.	Аналог.	Цифр.	Цифр.	Цифр.
Активний рівень	1	1	0	> 2V	> 2V	1	1	0

Табл.3.2. Датчики

У табл.3.3. наведений перелік виходів користувача і їх тип.

№	0	1	2	3	4
Вихід	SIREN	LIGHT	CUST1	CUST2	CUST3
Тип цифрового виходу	Двотактний				
Активний рівень	1				

Табл.3.3. Виходи

У табл.3.4 наведене підключення елементів підпорядкованого пристрою до налагоджувальної плати. У дужках позначена периферія мікроконтролеру.

Вивід	Периферія	Вивід	Периферія
B12	MOV	B11	Bluetooth (RX3)
B13	SMOKE	B10	Bluetooth (TX3)
B14	Вхід CUST1	B1	TEMP (ADC)
B15	Вхід CUST2	B0	Вхід LIGHT (ADC)
A8	Вхід CUST3	A7	Батарея (ADC)
A9	До комп. (TX1)	A6	AUX
A10	До комп. (RX1)	A5	M1
A11	TAPE	A4	M0
A12	SIREN	A3	LoRa (RX2)
A15	Вихід LIGHT	A2	LoRa (TX2)
B3	Вихід CUST1	A1	У повітрі (ADC)
B4	Вихід CUST2	A0	NC
B5	NC		
B6	Вихід CUST3		
B7	NC		
B8	NC		
B9	NC		

Табл.3.4. Підключення до Blue Pill.

3.4 Програмна реалізація деяких функцій підпорядкованого пристрою

3.4.1 Емуляція EEPROM

Існує необхідність записувати налаштування периферії, а також пароль і ключ шифрування у постійну пам‘ять мікроконтролера. Використаний у розробці мікроконтролер не має EEPROM; використання мікросхеми пам‘яті є надмірним, оскільки об‘єм даних для запису малий. Можливий запис даних у flash, але стирання flash виконується сторінками місткістю 1 Кбайт (табл.4.5). Якщо часто змінювати налаштування, ресурс пам‘яті може бути вичерпаний.

Block	Name	Base addresses	Size (bytes)
Main memory	Page 0	0x0800 0000 - 0x0800 03FF	1 Kbyte
	Page 1	0x0800 0400 - 0x0800 07FF	1 Kbyte
	Page 2	0x0800 0800 - 0x0800 0BFF	1 Kbyte
	Page 3	0x0800 0C00 - 0x0800 0FFF	1 Kbyte
	Page 4	0x0800 1000 - 0x0800 13FF	1 Kbyte
	. . .	. . .	. . .
	Page 127	0x0801 FC00 - 0x0801 FFFF	1 Kbyte

Табл.3.5. Організація пам‘яті мікроконтролерів середньої продуктивності.

Розробники ST у AN2594 [9], AN3969 пропонують емуляцію EEPROM. Використовуються 2 сторінки flash, які можуть мати 3 статуси:

- ERASED: сторінка порожня;
- RECEIVE_DATA: сторінка отримує дані з іншої повної сторінки;
- VALID_PAGE: сторінка містить корисні дані, і цей стан не змінюється до тих пір, поки корисні дані не будуть повністю перенесені на порожню сторінку.

Кожна змінна визначається віртуальною адресою та значенням, яке зберігається у flash для подальшого пошуку чи оновлення. Коли дані модифікуються, змінені дані асоціюються з попередньою віртуальною адресою і записуються у flash. Пошук даних у flash повертає актуальне значення.

Коли місце на одній сторінці закінчується, усі актуальні дані переносяться на порожню, після цього заповнена сторінка стирається. Для забезпечення надійності зберігання даних і визначення поточної сторінки, на якій містяться корисні дані, зчитуються і за необхідності змінюються їх статуси.

В інтернеті знайдена інша бібліотека «FlashPROM» [10] емуляції EEPROM. Вона простіша: виділяється одна або декілька сторінок пам‘яті, визначається розмірність записуваного масиву і тип даних. Новий масив актуальних даних записується в кінець попереднього.

При старті програми виконується пошук межі розділення даних і незаписаного простору, після чого дані завантажуються в оперативну пам‘ять.

Бібліотека FlashPROM має меншу надійність, але вона простіша у використанні і більш економічно витрачає пам‘ять при записі даних масивами. При використанні підходу ST для досягнення економічності довелося б спочатку перевіряти, чи були змінені дані (кожна їх одиниця визначеного типу), після чого записувати лише нові дані. Це потребує більше часу на реалізацію; простіше, використовуючи бібліотеку FlashPROM, одразу після запису даних виконати їх пошук і завантаження в оперативну пам‘ять, після чого порівняти дані, що були записані, зі зчитаними і зробити висновок про те, чи усі дані були записані коректно.

Бібліотека FlashPROM використовується у розробці.

Дані зберігаються у форматі, наведеному в табл.3.6.

№ байту	0	1	2	3	4	5	6	7	8:15	16:31
Назва	IDH	IDL	SPED	CHAN	OPTION	-	SEN	OUTS	PASS	KEY
За замовчуванням	0x00	0x00	0x1A	0x06	0x44	-	0x01	0x00	-	0xFF…0xFF

Табл.3.6. Розміщення даних у flash.

При відсутності даних у flash, у програму завантажуються значення за замовчуванням.

3.4.2 Запобігання колізій у стані сигналізації

Колізія – накладання двох чи більше повідомлень при одночасній передачі даних. Колізія може виникнути, якщо одночасно спрацювали сигналізації на різних об'єктах. Використаний у розробці спосіб запобігання колізій наведений на рис.3.2.

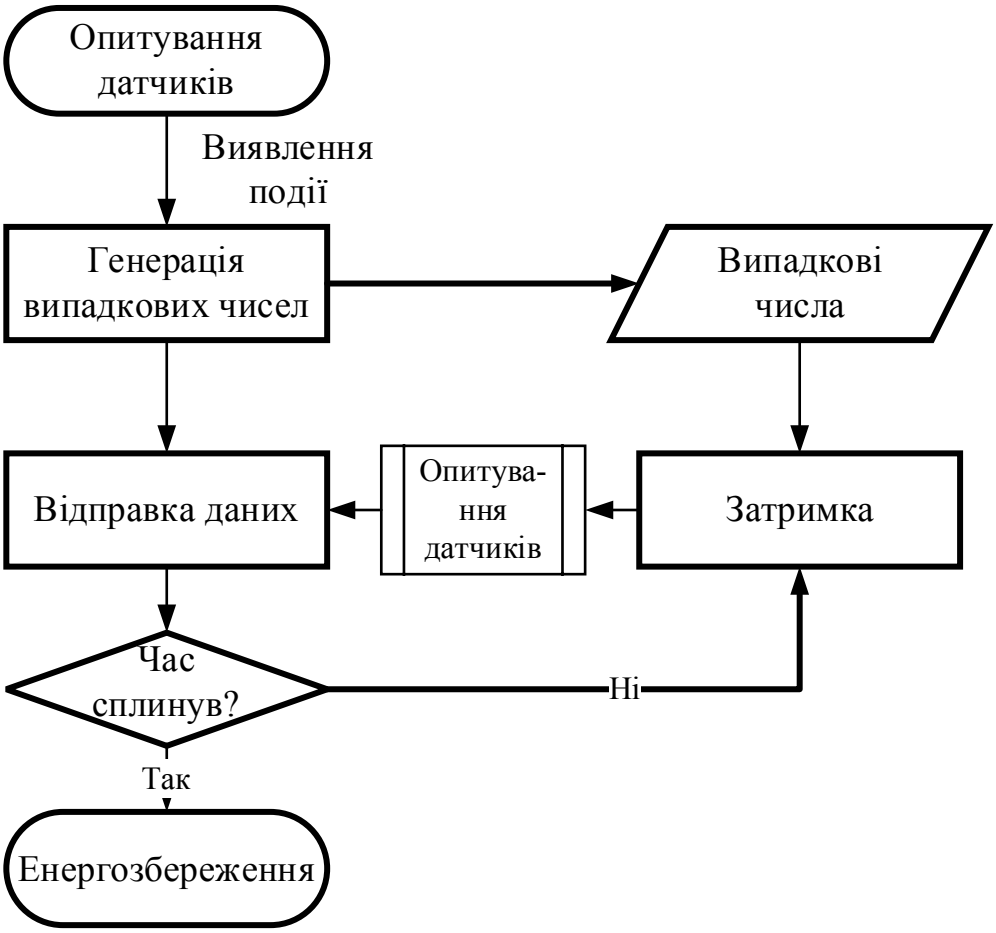


Рис.3.2. Алгоритм запобігання колізій.

При спрацюванні сигналізації відбувається одноразова відправка даних, генеруються випадкові числа, що мають зміст інтервалів часу між сусідніми відправками даних. Оскільки для розділення сусідніх двох повідомлень використовується тайм-аут, згенеровані випадкові числа змінюються так, щоб вони не містили значень, менших за тайм-аут. Дані відправляються декілька разів, доки не сплинув час сигналізації. Перед кожною відправкою відбувається опитування датчиків.

3.5 Вибір і огляд мікроконтролера головного пристрою

Головний пристрій розміщується на пункті охорони. Слово «головний» означає, що при відсутності тривоги ініціювати обмін даними може лише він. Але у стані сигналізації підпорядкованого пристрою ініціює передачу даних підпорядкований пристрій.

3.5.1 Вибір мікроконтролера головного пристрою

—Головний пристрій проводить обмін даними з багатьма підпорядкованими пристроями, отже він повинен мати більшу продуктивність, а також мати можливість апаратної генерації випадкових чисел та достатньо пам‟яті для зберігання ключів шифрування для 2^{16} підпорядкованих пристроїв. Інші вимоги до мікроконтролера головного пристрою не відрізняються від вимог до підпорядкованого.

3.5.2 Огляд мікроконтролера головного пристрою

Вибраний мікроконтролер STM32F407VE на налагоджувальній платі (рис.3.3).

Рис.3.3. Налагоджувальна плата на STM32F407VET6.

Плата містить:

- мікроконтролер STM32F407VET6;

- мікросхему flash пам‟яті W25Q16BV на 2Мбайти;
- кварцові резонатори на 8МГц і 32.768кГц;
- батарейку для підтримання роботи годинника реального часу;
- кнопки користувача;
- лінійний стабілізатор напруги AMS1117, $U_{вих}$ = 3.3В;
- конектори для виводів мікроконтролера, роз‟єм живлення, роз‟єм програмування, роз‟єм для SD-картки, роз‟єм для nRF24, роз‟єм для підключення дисплею.

На момент придбання (2020 р.) ціна на плату була 10$.

Важливі для сигналізації параметри STM32F407VET6 такі:

- 32-розрядне ядро ARM Cortex-M4, максимальна частота 168 МГц, продуктивність 1,25 DMIPS / МГц, FPU;
- 512 Кбайт пам‟яті flash, 192 Кбайт SRAM;
- RNG;
- 82 виводи загального призначення;
- годинник реального часу і 3 режими пониженого енергоспоживання;
- 15 інтерфейсів, серед яких є по декілька USART, UART, SPI, I2C, CAN.

Головною перевагою STM32F4 над багатьма іншими мікроконтролерами ST та інших виробників є наявність АГВЧ (RNG).

Процесор RNG – це генератор випадкових чисел, заснований на безперервному тепловому шумі. RNG забезпечує користувача випадковими 32-бітовими значеннями. RNG пройшов тести FIPS PUB 140-2 (2001, 10 жовтня) із коефіцієнтом успіху 99% [11]. RNG виконує моніторинг ентропії для виявлення ненормальної поведінки (генерації стабільних значень чи періодичної послідовності значень).

3.6. Опис роботи програми головного пристрою

Програма для STM32F103C8 написана з використанням МП Сі, бібліотек CMSIS, HAL, STM32 cryptographic library, а також програми CubeMX, у якій виконувалася ініціалізація.

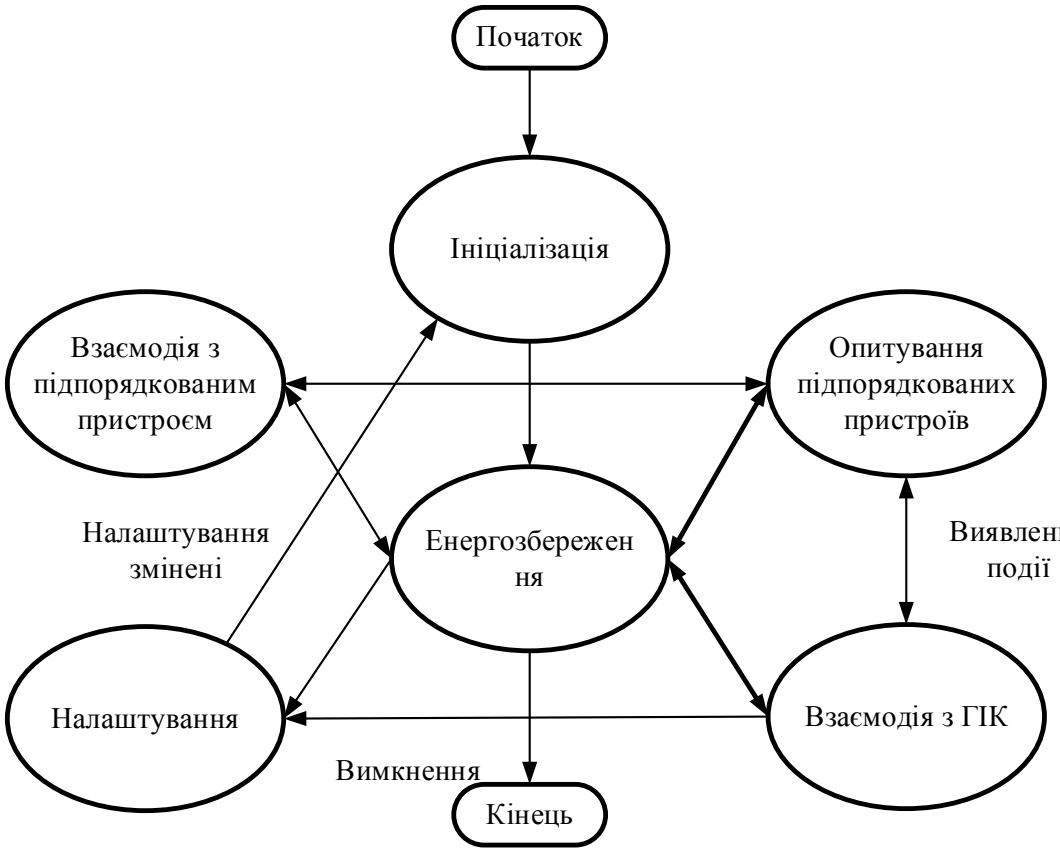
3.6.1 Функції програми

—Функціями програми головного пристрою є:

- отримання інформації про спрацювання сигналізації від багатьох об'єктів та передавання цієї інформації у ГІК;
- періодичне опитування підпорядкованих пристроїв;
- віддалене керування виходами;
- генерація і зберігання ключів шифрування;
- взаємодія з ГІК.

3.6.2 Діаграма станів і переходів

Діаграма станів і переходів наведена на рис.3.4.



— Рис.3.4. Діаграма станів і переходів

Стани ініціалізації, енергозбереження і налаштування головного пристрою мало відрізняються від цих станів підпорядкованого пристрою.

Взаємодія з ГІК передбачає отримання від користувача команд на безпровідне «з‘єднання» з підпорядкованим пристроєм і надання його відповідей користувачу.

Взаємодія з підпорядкованим пристроєм включає обмін даними як в автоматичному режимі, так і за бажанням користувача; головний пристрій отримує інформацію з будь-яких передавачів, а у ГІК надсилає тільки інформацію, отриману від підключених підпорядкованих пристроїв (ключі шифрування яких наявні).

Опитування підпорядкованих пристроїв – автоматична розсилка запитів підключеним підпорядкованим пристроям. У цьому режимі головний пристрій завантажує ключі шифрування з мікросхеми flash по одному в оперативну пам‘ять. Після завантаження кожного ключа, головний пристрій опитує підпорядкований пристрій з ідентифікатором, який відповідає завантаженому ключу. Якщо підпорядкований пристрій не відповідає, головний повідомляє про це ГКІ.

Висновки до розділу 3

Програма підпорядкованого пристрою є головним елементом системи, оскільки саме підпорядкований пристрій повідомляє про проникнення та інші події; програма забезпечує енергозбереження відключенням невикористовуваної периферії, відключенням тактового сигналу ядра завжди, коли воно не опрацьовує переривання, відключенням USART1 при відсутності команд від програми для ПК впродовж 60с. Реалізоване гнучке налаштування користувачем підпорядкованого пристрою, а саме його входів і виходів.

У програмі підпорядкованого пристрою використані такі корисні прийоми: реалізація апаратного генератору випадкових чисел на шумі

молодшого розряду АЦП з використанням методу Фібоначчі з запізненням, емуляція EEPROM з flash пам‘яті, запобігання колізій.

Головний пристрій є важливим елементом системи: він збирає інформацію з багатьох підпорядкованих пристроїв, забезпечує зв‘язок підпорядкованих пристроїв з користувачем. Головний пристрій виконує шифрування і розшифрування даних, а також «відсіювання» пошкоджених повідомлень та повідомлень від неправомочних суб‘єктів (зловмисників / чужих пристроїв).

Отже головний пристрій дозволяє не навантажувати комп‘ютерну програму опрацюванням даних.

Унікальною властивістю мікроконтролера головного пристрою є можливість генерації істино випадкових чисел для ключів шифрування.

					172.4391.КР.ПЗ.Р4			
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*				
Розробник		Бецько І.О.			Протокол обміну даними	*Літ.*	*Арк.*	*Аркушів*
Консультант							71	
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова		
Керівник		Жук О. К.						
Зав. каф.		Рябенький В. М.						

РОЗДІЛ 4. ПРОТОКОЛ ОБМІНУ ДАНИМИ

У табл. 4.1. наведені способи обміну даними між елементами системи.

Табл. 4.1. Способи обміну даними між елементами системи

Елементи	Спосіб
ГІК <-> Підпорядкований пр.	Провідний
ГІК <-> Головний пр.	Провідний
Підпорядкований <-> Головний	Безпровідний

4.1 Провідний спосіб

Розділення сусідніх посилок відбувається за допомогою тайм-ауту 50 мс.

Посилка складаються з команди (1 байт) і даних (розмір залежить від команди). Інтерпретація даних визначається командою. Перевірка цілісності не передбачена.

Передбачене підключення одного головного і одного підпорядкованого пристрою до одного комп'ютеру одночасно, отже ідентифікатор (адреса) не передається у кожній посилці, а тільки у блоці даних для деяких команд.

На кожну команду передбачена відповідь. Відповіді мають відправлятися тільки у разі успішного виконання команди.

Список команд, що передбачені провідним способом передачі даних, наведений у табл. 4.2.

Табл. 4.2. Спимок команд передбачені провідним способом передачі даних

№	Назва	Опис, формат посилки	Команда	Відповідь (ок/не ок)
Спільні (ГІК -> пристрій)				
1	Запис часу	Передає у пристрій поточний час, *1)	„T“ (0x54)	„T“ (0x54) / „E“
2	Налаштування	Записує налаштування передавача (без збереження), *2)	0xC2	0xC0 / „E“
ГІК -> Підпорядкований пристрій				
1	Запис flash	Оновлює налаштування у flash, *3)	0xC0	0xC0 / „E“
2	Читання flash	Читає налаштування у flash; без даних (тільки команда)	„G“ (0x47)	*4) / „E“
ГІК -> Головний пристрій				
1	Запит ключа	Генерує ключ і повертає його у ГІК, *5)	„K“ (0x4B)	*6) / „E“
2	Період опитування	Встановлює період опитування, *7)	„P“ (0x50)	„P“ / „E“
3	Перевірка	Головний пристрій виконує перевірку підпорядкованого (відправляє запит станів датчиків),*8)	„C“ (0x43)	*9) / „E“
4	Запис виходів	Головний пристрій відправляє підпорядкованому команду на управління виходами, *10)	„o“ (0x6F)	„o“ / „E“
5	Стирання ключів	Стирає усі ключі шифрування головного пристрою; без даних	“Er”	“Er” / „E“
6	Читання наявних ключів	ГІК передає список підтримуваних об‘єктів у головний пристрій, головний пристрій повертає список підпорядкованих пристроїв, для яких наявні ключі (включає пристрої тільки зі списку від ГІК), 11)	„M“	*12)
Головний пристрій -> ГІК				
1	Тривога	Спрацювання сигналізації на об‘єкті, *13)	„A“	-
2	Не відповідає	Підпорядкований пристрій не відповідає при перевірці *14)	„N“	-

Примітки:

*1) Запис часу:

№ байту	0	1	2	3	4	5	6	7
вміст	‘T’	рік	місяць	дата	день т.	години	хвилини	секунди

*2) Налаштування передавача E32-868T20D:

№ байту	0	1	2	3	4	5
вміст	0xC2	IDH	IDL	SPED	CHAN	OPTION

*3) Запис flash:

№ байту	0	1	2	3	4	5	6	7	8:15	16:31	32
вміст	0xC0	IDH	IDL	SPED	CHAN	OPTION	SEN	OUTS	PASS	KEY	KEY_OK

SEN – підтримувані датчики (входи); OUTS – підтримувані виходи;

PASS – пароль; KEY – ключ; KEY_OK– запис ключа;

KEY_OK = 1 – змінити ключ шифрування на KEY;

KEY_OK = 0 – залишити ключ без змін (переписати у пам‟ять старий ключ).

*4) Читання flash, відповідь:

№ байту	0	1	2	3	4	5	6	7	8:15	16:31
вміст	‘G’	IDH	IDL	SPED	CHAN	OPTION	SEN	OUTS	PASS	KEY

*5) Запит ключа:

№ байту	0	1	2
вміст	„K“	IDH	IDL

*6) Запит ключа, відповідь:

№ байту	0	1:16
вміст	„K“	KEY

*7) Встановлення періоду опитування у хв.:

№ байту	0	1	2
вміст	„P“	PH	PL

PL – молодший байт періоду опитування;

PH – старший байт періоду опитування.

*8) Перевірка:

№ байту	0	1	2
вміст	„C“	IDH	IDL

*9) Перевірка, відповідь:

№ байту	0	1	2	3:x
вміст	„C“	IDH	IDL	DATA, *15)

*10) Запис виходів:

№ байту	0	1	2	3
вміст	„o“	IDH	IDL	OUTS_STATES

*11) Читання списку підключених пристроїв:

№ байту	0	1	2	3	4	…	2*n+3	2*n+4
вміст	„M“	QNTH	QNTL	IDH_0	IDL_0	…	IDH_n	IDL_n

N – число об‘єктів у ГІК;

QNT – число байтів (N * 2);

ID_n – ідентифікатор об‘єкту у ГІК;

n = 0...N.

*12) Читання списку підключених пристроїв, відповідь:

№ байту	0	1	2	3	4	…	2*n+3	2*n+4
вміст	„M“	QNTH	QNTL	IDH0	IDL0	…	IDHn	IDLn

N – число об‘єктів зі списку, для яких наявні ключі шифрування;

QNT – число байтів (N * 2);

ID_n – ідентифікатор підпорядкованого пристрою у пам‘яті головного;

n = 0...N.

*13) Тривога:

№ байту	0	1	2	3:x
вміст	„A“	IDH	IDL	DATA, *15)

*14) Не відповідає:

№ байту	0	1	2
вміст	„N“	IDH	IDL

4.2 Безпровідний спосіб

Розділення сусідніх посилок відбувається за допомогою тайм-ауту 50 мс. Формат посилки наведений у табл.6.3.

№ байту	0:1	2:17	18	19:x	x:y
вміст	ID	IV	команда	дані	HMAC

Табл.6.3. Формат посилки при безпровідній передачі.

x - 18 – довжина даних;

y + 1 – довжина посилки; y = x + 32.

Безпровідним способом підтримуються три команди: „o“(без відповіді), „C“, „A“(без відповіді).

За команди „o“ дані мають вигляд:

дані (команда „o“, запит)	
№ байту	19
вміст	Стани виходів

За команди „C“(запит) дані мають вигляд:

дані (команда „C“, запит)			
№ байту	19	20	21
вміст	PH	PL	Стани виходів

За команд „C“(відповідь) і „A“ дані мають вигляд *15).

*15) Дані:

дані (команда „C“, відповідь / команда “A“)						
№ байта	19	20	21	22	23	24:30
вміст	Стани входів	Підключені входи	Доступні виходи	Стани виходів	напруга	Дата і час

Висновки до розділу 4

Розроблені протоколи обміну даними між усіма елементами системи. Розділення двох сусідніх посилок забезпечується тайм-аутом 50мс.

Передбачене виділення головного та підпорядкованого пристроїв, як у Modbus, а також передбачена можливість асинхронної відправки повідомлень підпорядкованим пристроєм у режимі сигналізації. Хоча асинхронний обмін даними зменшує максимальне число підпорядкованих пристроїв у системі, він дозволяє пришвидшити доставлення даних про спрацювання сигналізації у ГКІ.

Провідний та безпровідний способи передачі даних мають відмінності у форматах посилок.

					172..КР.ПЗ.Р5		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Бецько І.О.			Охорона праці	*Літ.*	*Арк.* 78 / *Аркушів*
Консультант		Тубальцев А. М.					
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Жук О. К.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 5. ОХОРОНА ПРАЦІ

Як при роботі на підприємстві, так і в процесі розробки електронного пристрою для дипломного проекту, виконавець роботи завжди зазнає впливу у різній мірі шкідливих і, можливо, навіть небезпечних виробничих факторів, тож в процесі розробки існує необхідність дотримання правил, спрямованих на збереження життя, здоров'я і працездатності, визначених охороною праці.

Метою охорони праці є запобігання дії шкідливих та небезпечних факторів.

Шкідливі виробничі фактори – фактори, які негативно діють на працівника: погіршують стан його здоров'я і знижують працездатність.

Небезпечні виробничі фактори – фактори, що призводять до травми, в тому числі смертельної.

Темою дипломної роботи є розробка охоронної сигналізації; розробка потребує тривалої роботи за комп'ютером і паяння електроніки. Окрім зазначених видів робіт, які потенційно можуть наносити шкоду здоров'ю, існує ще й небезпека загоряння і вибуху акумуляторів, що використовуються для забезпечення автономного живлення сигналізації.

У розділі, присвяченому охороні праці, будуть розглянуті способи протидії таким шкідливим факторам:

- несприятливе освітлення;
- психофізіологічні фактори (зорове та розумове напруження, малорухливість);
- небезпека загоряння і вибуху літій-іонних акумуляторів.

5.1 Несприятливе освітлення

Несприятливе освітлення стає причиною зниження зорової працездатності, але це не єдиний наслідок роботи при несприятливому освітленні. Недостатнє освітлення рухомих частин обладнання, відблиски світла, надмірна яскравість можуть стати причиною травмування.

Освітлення також впливає на психологічні параметри працівника, а саме настрій і емоційний стан.

Для забезпечення якісного освітлення на робочому місці необхідно дотримуватися правил:

- середня освітленість на робочих місцях з постійним перебуванням людей має бути не менше 200 Люкс;
- на робочому місці не повинно бути тіней, різниця у яскравості повинна бути мінімальною;
- настінний світильник має бути розміщений на 30-50 см вище від монітору;
- монітор має бути розміщений так, щоб на нього не потрапляло пряме сонячне світло;
- у полі зору не повинно бути глянцевих та блискучих матеріалів;
- джерело загального світла має розміщуватися високо для досягнення максимальної рівномірності освітлення;
- робоче місце бажано розташувати збоку від вікна; вікно не повинно бути прямо перед обличчям чи за спиною;

5.2 Психофізичні фактори

Психофізичні фактори полягають у зоровому та розумовому напруженні, недостатній руховій активності в процесі роботи. Усі ці фактори пов‘язані з необхідністю виконання відповідальної роботи за комп‘ютером протягом тривалого часу, наприклад: програмування, розрахунки електричної схеми, оформлення дипломної роботи. Зорове напруження може також виникати в під час паяння малих деталей: цей процес потребує уваги і пильності, щоб не допустити помилки і якісно, з першого разу виконати усі з‘єднання.

Зазначені психофізичні фактори можуть викликати захворювання і гарантовано знизять працездатність. Для протидії розумовому та зоровому напруженню необхідно вводити такі правила:

- робочий стіл має бути добре освітлений, а на моніторі не має бути відблисків світла;
- відстань між моніторами має бути більша за 1.2 метри;
- відстань від очей до монітора має бути не менша за 45 см;
- робити паузи у роботі (10 хв. після кожних 50 хв. роботи), під час паузи необхідно забезпечити зоровий і розумовий відпочинок;
- обмежувати загальний час роботи за комп'ютером (за можливості не більше 6 годин на день/зміну) [12];

Якщо не виконувати зазначені рекомендації, може виникати головний біль, біль і різь в очах, з'являється втома, погіршитися зір і порушитися сон.

Окрім перелічених правил, я користуюся монітором з підтримкою технології Eye-care (піклування про очі), до технології входять такі корисні функції:

- відсутність мерехтіння;
- режим читання (слабкого синього світла), що підтримується монітором апаратно;

Правила та заходи профілактики захворювань, пов'язаних з роботою за комп'ютером та малорухомим способом життя взагалі:

- монітор має бути розміщений перед очима чи вище, це дозволить тримати голову прямо;
- стілець має бути зі спинкою, підлокітниками і регулюванням висоти;
- поза не має бути викривленою, важливо змінювати її для зниження статичної напруги м'язів шийно-плечової області і спини;
- клавіатуру слід розташовувати на поверхні столу на відстані 100 - 300 мм від краю, зверненого до користувача, або на спеціальній відокремленій поверхні;

- необхідно періодично виконувати фізичні вправи для здоров‟я шиї та попереку (рис.5.1).

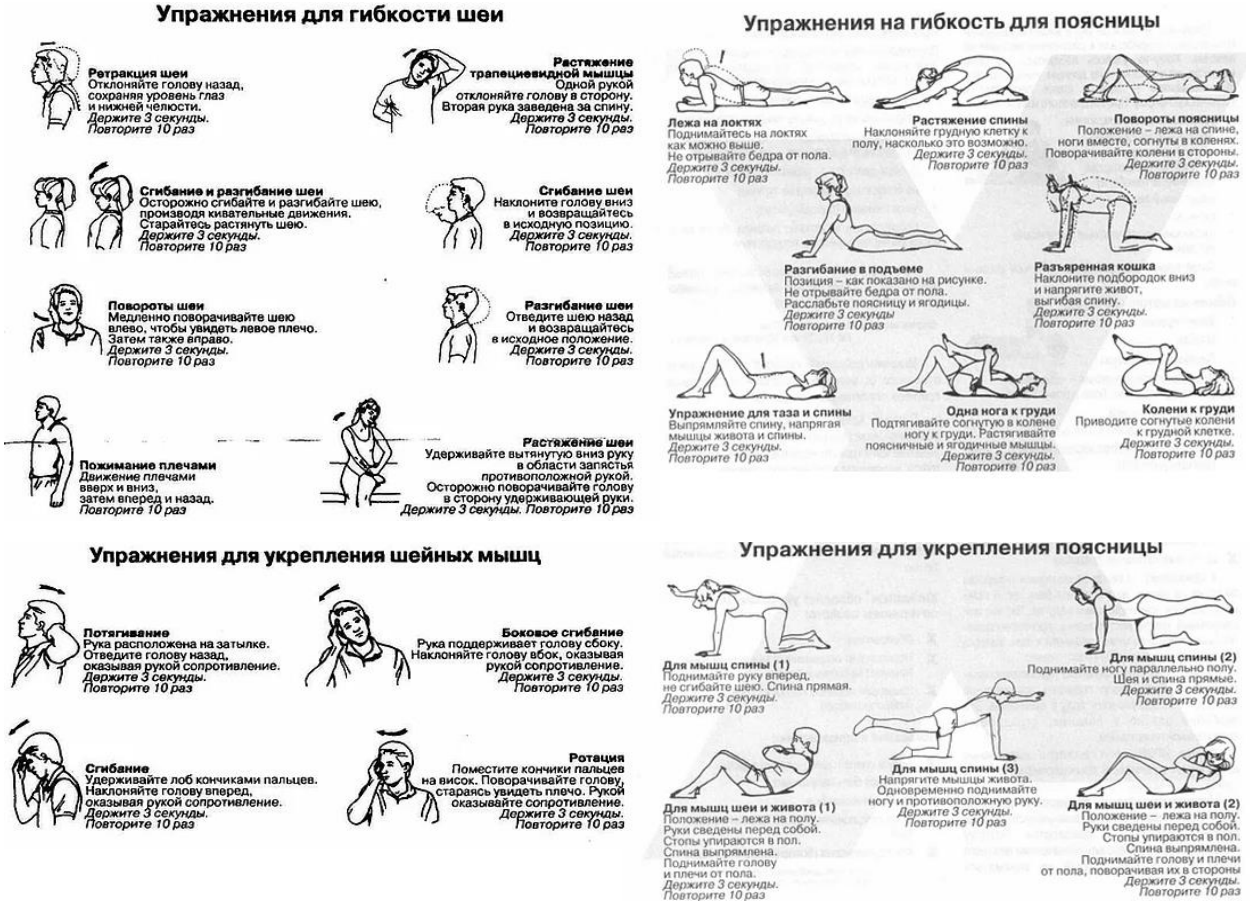


Рис.5.1. Вправи для шиї та попереку

Систематичне нехтування зазначеними правилами роботи за комп‟ютером може призвести до проблем зі здоров‟ям та сприяти розвитку хвороб:

- протрузії шийного відділу хребта;
- головний біль;
- тунельний синдром зап‟ястя;
- сколіоз;
- ослаблення чи підвищений тонус м‟язів.

Хоча своєчасне і якісне харчування не стосується безпосередньо охорони праці, але є важливим фактором впливу на працездатність. Деякі люди, особливо молоді, через неуважне ставлення до харчування та через відчуття сорому від процесу прийому їжі в присутності інших людей під час

роботи не обідають. На мої стан здоров'я і працездатність харчування впливає суттєво, тож я за необхідності перериваю робочий процес для забезпечення вчасного харчування.

5.3 Небезпека загоряння і вибуху літій-іонних акумуляторів

У розробці використовуються літій-іонні акумулятори у якості джерела живлення сигналізації при нетривалому відключенні напруги живлення. Відомі ситуації, коли літій-іонні акумулятори у складі електронного пристрою (телефон, електромобіль) загорялися та вибухали в процесі його експлуатації.

Але якщо неправильно зберігати і використовувати акумулятори в процесі розробки, вони вийдуть з ладу і нанесуть шкоду ще до їх включення до складу пристрою. Тому акумулятори слід сприймати як потенційне джерело небезпеки.

Вибух акумулятору може бути спричинений як діями користувача, так і допущеною при виробництві помилкою.

Найчастіше причиною самозапалення акумуляторів є коротке замикання всередині електрохімічної комірки. Електричний контакт між анодом і катодом може виникнути з багатьох причин. Це може бути, наприклад, механічне пошкодження комірки. Також внутрішнє коротке замикання виникає через порушення технології виробництва при нерівній нарізці електродів або попаданні металевих частинок між анодом і катодом, що веде до пошкодження пористого сепаратора. Також причиною внутрішнього короткого замикання може бути «проростання» ланцюжків металевого літію (дендритів) через сепаратор. Такий ефект виникає, якщо іони літію не встигають вбудуватися в кристал анода при занадто швидкій зарядці або низькій температурі, а також якщо ємність активного матеріалу катода перевищує ємність анода, в результаті чого на поверхні анода з'являються мікроскопічні відкладення, які поступово зростають.

Після того, як відбулося коротке замикання, акумулятор починає нагріватися. При температурі 70-90 °С починається розкладання захисного шару аноду, після цього починається розкладання електроліту на леткі вуглеводні. При досягнення температурою величини 180-200 °С, починає виділятися кисень і відбувається запалення і стрімкий стрибок температури.

Крім внутрішнього короткого замикання існують і інші причини самозаймання: перегрів акумулятора, неправильна зарядка / розрядка (перевищення максимально допустимої напруги, зарядка великим струмом, занадто глибока розрядка) тощо.

Отже, необхідно вводити заходи щодо зменшення вірогідності самозапалення, а також спрямовані на мінімізацію шкоди для здоров‘я унаслідок загоряння та вибуху, а саме:

- застосовувати лише акумулятори надійного виробника;
- використовувати акумулятори тільки за призначенням;
- використовувати у розробці і в процесі роботи спеціальну схему захисту і заряджання літій-іонних акумуляторів;
- не залишати акумулятор на зарядці без нагляду;
- зберігати акумулятори у місцях, де вони не можуть нанести велику шкоду здоров‘ю унаслідок загоряння; температура зберігання має бути 0-40 °С;
- не зберігати багато акумуляторів разом;
- не використовувати пошкоджені акумулятори.

Для захисту акумуляторів від перевищення струму заряду, струму розряду, зовнішнього короткого замикання, перевищення напруги заряду, надмірного розряду використовується схема захисту. Схема захисту (рис.5.2) на мікросхемі TP4056, яка здійснює управління, реалізована на окремій платі. Схема виконує функції:

- обмеження струму заряджання;

- автоматичне завершення процесу заряджання при досягненні напругою на акумуляторі максимального значення, яке відповідає повному заряду;
- відімкнення акумулятору від навантаження при перевищенні струму і при падінні напруги акумулятору нижче допустимої;

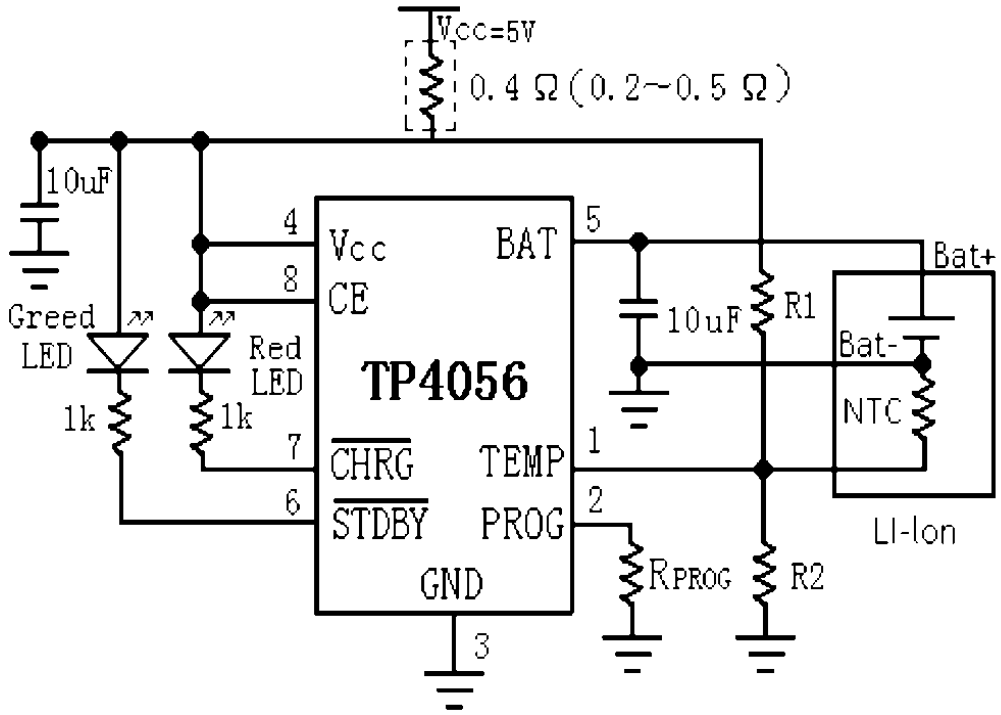


Рис.5.2. Схема захисту і заряджання акумулятору.

Схема використовується в процесі розробки, а також входить до складу кінцевого виробу.

Висновки до розділу 5

У розділі розглянуте питання охорони праці розробника автономної охоронної сигналізації. Виявлені шкідливі і небезпечні виробничі фактори, а саме: несприятливе освітлення, психофізіологічні фактори, небезпека загоряння і вибуху літій-іонних акумуляторів; зазначені механізми їх впливу.

Сформульовані вимоги до освітлення робочого місця і навколишнього простору, вказані правила роботи за комп'ютером, правила безпечного зберігання і використання літій-іонних акумуляторів; наведені можливі наслідки невиконання цих правил.

Розглянута використана у розробці схема захисту і заряджання літій-іонних акумуляторів, однією з цілей застосування якої є забезпечення безпеки в процесі розробки пристрою на акумуляторному живленні і безпечної експлуатації акумуляторів.

ВИСНОВКИ

Розроблена система з трьох елементів:

- головний пристрій;
- підпорядкований пристрій;
- програма для ПК з ГІК.

Розроблена енергоефективна безпровідна сигналізація має низьку вартість і може бути використана у віддалених від міста населених пунктах. Сигналізація не потребує використання додаткової апаратури, а також специфічного ПЗ.

Енергозбереження забезпечене як програмно – ефективним використанням ядра і периферії мікроконтролера (режимом енергозбереження, відключення зайвих входів і виходів, відключенням USART1 при переході в режим енергозбереження), так і апаратно – використанням технології LoRa для передачі сигналу на велику відстань, використанням Bluetooth модулю з низьким енергоспоживанням для зняття об‘єкту з сигналізації.

Автономна робота сигналізації можлива за рахунок літій-іонних акумуляторів, рівень заряду яких контролюється підпорядкованим пристроєм.

Завдяки можливості налаштування входів і виходів підпорядкованого пристрою, наявності як цифрових, так і аналогових входів, сигналізацію можна використовувати не тільки для охорони приватної власності від зловмисників, а й для своєчасного виявлення загоряння (задимлення), затоплення тощо. Виходи підпорядкованого пристрою можуть бути використані як для світло-звукового сповіщення, так і для віддаленого управління навантаженнями (опалювальний котел, зовнішнє освітлення, холодильник тощо).

Сигналізація на об‟єкті може бути вимкнена користувачем зі смартфону шляхом введення паролю.

Використання шифру AES-128, коду ідентифікації на основі криптографічної хеш-функції HMAC-SHA-256, апаратного генератору випадкових чисел, годинника реального часу дозволяє надійно захистити систему від втручання зловмисника в процес обміну даними, а також виявити його фізичне втручання у підпорядкований пристрій. Ключі шифрування генеруються окремо для кожного підпорядкованого пристрою і зберігаються у пам‟яті головного пристрою.

Для зручного користування системою розроблена програма для ПК з ГІК. Інтерфейс мінімалістичний, красивий і зручний. Програма проста у використанні і потребує незначних ресурсів комп‟ютеру (до 40 Мбайт оперативної пам‟яті). Передбачений захист від випадкових натиснень, від неправильних дій користувача, додані інформативні повідомлення у рядку статусу і вікнах з повідомленнями.

Захист від помилок при провідній передачі даних від пристроїв до ГІК та навпаки забезпечений протоколом провідного обміну даними та програмно: після виконання команди відбувається порівняння результату виконаної команди з очікуваним результатом.

В процесі розробки ПЗ деякі рішення приймалися з орієнтацією на подальшу модифікацію системи. Вбачаю такі способи покращення системи:

- відмова від «модульності», розробка друкованих плат;
- перехід на більш відповідні до визначених вимог елементну базу та технології (STM32L0/L4/WB/WL замість STM32F1/F4, SX1276 замість E32-868T20D, NFC замість Bluetooth, мікросхеми пам‟яті ATECCx08A у кожному підпорядкованому пристрої);
- перехід до використання досконалого протоколу LoRaWAN (у зв‟язку зі зміною передавачів);

- використання USB замість UART для з‘єднання пристроїв з комп‘ютером;
- використання баз даних у програмі для ПК
- реалізація криптографічного АГВЧ у підпорядкованому пристрої.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. LoRa application brief. Home security systems. – Semtech, 2017, 2 с.
2. Асиметричні алгоритми шифрування [електронний ресурс]. URL: https://en.wikipedia.org/wiki/Public-key_cryptography.
3. Advanced Encryption Standard [електронний ресурс]. URL: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.
4. National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information. Committee on National Security Systems, 2003.
5. Recommendation for Block Cipher Modes of Operation. NIST Special Publication 800-38A. Technology Administration U.S. Department of Commerce, 2001.
6. Криптографічна хеш-функція [електронний ресурс]. URL: https://en.wikipedia.org/wiki/Cryptographic_hash_function.
7. User manual UM0586, rev.4 – STMicroelectronics, 2013. 131 с.
8. Шлее М. Qt 5.10. Професійне програмування на C++. – СПб.: БХВ-СПБ, 2018. 1072 с.
9. Application note AN2594, rev.3 – STMicroelectronics, 2009. 10 с.
10. STM32 Flash как EEPROM [електронний ресурс], 2020. URL: https://istarik.ru/blog/stm32/142.html. Дата звернення: 10.04.2021.
11. Reference manual RM0090, rev 18 – STMicroelectronics, 2019. 1749 с.