Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
Факультет Комп'ютерної інженерії та управління
(повна назва)
Кафедра Автоматизації проектування обчислювальної техніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Система пошуку прихованих каналів в діапазоні 2.4 ГГц

(тема)

Виконав: здобувач 4 курсу,
групи КІУКІ-21-9
Сасько А.О.
(прізвище, ініціали)

спеціальності 123 – Комп'ютерна інженерія
(шифр і назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерна інженерія
(повна назва освітньої програми)

Керівник ст.викл. Шевченко О.Ю.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Чумаченко С.В.
(підпис) (прізвище, ініціали)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління

Кафедра Автоматизації проектування обчислювальної техніки

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 Комп'ютерна інженерія

Тип програми Освітньо-професійна

Освітня програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ:
Зав. кафедри
_____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Сасько Артему Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи _Система пошуку прихованих каналів в діапазоні 2.4 ГГц
затверджена наказом університету від __21___ _____05_____2025 р. № _403Ст__
2. Термін подання здобувачем роботи до екзаменаційної комісії _09_ ___06____ 2025 р.
3. Вихідні дані до роботи
бездротові мережі
nRF24L01
сканування спектру

4. Перелік питань, що потрібно опрацювати в роботі
Аналіз та огляд існуючих систем.
Постановка задачі.
Розробка структурної схеми пристрою.
Розробка функціональної схеми програми.
Розробка алгоритму роботи пристрою.
Тестування

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
13 слайдів

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Видача теми проекту, узгодження і затвердження теми	06.05.2025 – 09.05.2025	
2	Аналіз проблемної галузі, постановка задачі, вибір інструментальних засобів	09.05.2025 – 14.05.2025	
3	Розробка структурної схеми пристрою, вибір апаратної платформи	14.05.2025 – 16.05.2025	
4	Розробка функціональної схеми програми	16.05.2025 – 17.05.2025	
5	Розробка програмних модулів. Проведення тестування	17.05.2025 – 23.05.2025	
6	Оформлення пояснювальної записки	23.05.2025 – 25.05.2025	
7	Перевірка виконаного проекту керівником, допуск до захисту	25.05.2025 – 10.06.2025	

Дата видачі завдання _____06.05.2025 р.

Здобувач _____ _____
(підпис)

Керівник роботи _____ _____ ст.викл Шевченко О.Ю.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи містить: 49 сторінок, 14 рисунків, 2 додатки, 11 джерел за переліком посилань.

МІКРОКОНТРОЛЕР, СПЕКТРОАНАЛІЗАТОР, БЕЗДРОТОВІ МЕРЕЖІ, WI-FI, СКАНУВАННЯ, STM32.

Метою кваліфікаційної роботи є розробка програмно-апаратного комплексу, що дозволяє проводити сканування радіочастотного спектру у діапазоні 2.4 ГГц та виводити отримані значення рівнів для частотних каналів.

Був проведений аналіз існуючих систем виявлення каналів передачі сигналу та складено технічне завдання на проєктування. Була розроблена структурна схема системи сканування та обрана елементна база для реалізації проєкту. Керує системою мікроконтролер STM32F103C8T6, радіоприймачем виступає модуль nRF24L01. Здійснюється вивід результатів сканування на дисплей SSD1306 та на моніторі комп'ютера з використанням програмного додатку. Усі елементи були зібрані на макетній платі, мікроконтролер запрограмовано, та було протестовано роботу пристрою.

ABSTRACT

The explanatory note of the qualification work contains: 49 pages, 14 pictures, 2 appendices, 11 sources according to the list of links.

MICROCONTROLLER, SPECTRUM ANALYZER, WIRELESS NETWORKS, WI-FI, SCANNING, STM32.

The objective of the qualification work is the development of a hardware-software complex capable of scanning the radio frequency spectrum within the 2.4 GHz range and displaying the measured signal levels for individual frequency channels.

An analysis of existing signal transmission channel detection systems was conducted, followed by the formulation of a technical specification for the system design. A structural diagram of the scanning system was developed, and an appropriate set of components was selected for implementation.

The system is controlled by an STM32F103C8T6 microcontroller, with the nRF24L01 module serving as the radio receiver. The scanning results are displayed on an SSD1306-based screen as well as on a computer monitor through the use of a custom software application. All components were assembled on a breadboard, the microcontroller was programmed, and the device was successfully tested to validate its functionality.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

МК – мікроконтролер

ПК – персональний комп’ютер

ЦП – центральний процесор

ICP – Інтегроване середовище розробки – комплексне програмне рішення для розробки програмного забезпечення

COM-порт – двонаправлений послідовний інтерфейс

CMSIS – стандарт загального програмного інтерфейсу мікроконтролера від компанії ARM

GFSK – Gaussian Frequency-Shift Keying – Гаусівська частотна маніпуляція

HAL – Hardware Abstraction Layer – набір програмних бібліотек та інтерфейсів для високорівневої взаємодії з периферією мікроконтролера STM32

IDE – Integrated Development Environment – див. ICP

I^2C – послідовна двопровідна шина для зв'язку інтегральних схем

ISM – Industrial, Scientific and Medical – частина радіочастотного спектра загального призначення

LL – Low Layer – драйвери низького рівня, які ближче до апаратного забезпечення, на відміну від HAL

OLED – Organic Light-Emitting Diode – світлодіод, у якому електролюмінесценція відбувається в тонкому пласті органічного напівпровідника, розташованому між двома електродами; на його основі створюються дисплеї

RSSI – Received Signal Strength Indication – відносна отримана інтенсивність сигналу у безпровідних технологіях передачі

SDR – Software-Defined Radio – програмно-кероване радіо

SPI – Serial Peripheral Interface – послідовний периферійний інтерфейс

SSID – Service Set Identifier – унікальне найменування бездротової мережі, що відрізняє одну мережу Wi-Fi від іншої

SWD – Serial Wire Debug

WPA – Wi-Fi Protected Access – один з протоколів безпеки для захисту бездротових мереж

WEP – Wired Equivalent Privacy – стандарт захисту бездротового трафіку, заснований на RC4

Wi-Fi – від англ. Wireless Fidelity – загальновживана назва для стандарту IEEE 802.11 передавання цифрових потоків даних по радіоканалах

VCP – Virtual COM Port

VSCode – Microsoft Visual Studio Code

ZigBee – бездротовий стандарт передачі даних

USB — Universal Serial Bus – універсальна послідовна шина

ВСТУП

Технології бездротової передачі даних стали невід'ємною частиною сучасної цифрової інфраструктури. Вони відіграють ключову роль у формуванні інформаційно-комунікаційного простору сучасного суспільства, забезпечуючи мобільний доступ до даних, гнучкість мережевої інфраструктури та інтеграцію великої кількості пристроїв у єдину цифрову екосистему. Завдяки використанню радіочастотного спектру, технології бездротового зв’язку (Wi-Fi, Bluetooth, LTE, 5G, ZigBee тощо) забезпечують передачу інформації без фізичного з’єднання, що особливо важливо для динамічних сценаріїв використання – мобільного зв’язку, логістики, телеметрії та розумного міського середовища (Smart City). Їхнє широке впровадження зумовило еволюцію архітектури телекомунікаційних мереж, зокрема – перехід від централізованих моделей до децентралізованих і розподілених систем, здатних до самоорганізації та адаптації до змін середовища.

У технічному контексті бездротові технології виступають основою для розвитку концепцій Інтернету речей (IoT), кіберфізичних систем (КФС), автономних сенсорних мереж і мобільних роботизованих платформ. Їх використання дозволяє реалізовувати масштабовані, енергоефективні та економічно доцільні рішення в промисловості, медицині, енергетиці та оборонній сфері. Зокрема, стандарти 5G забезпечують наднизьку затримку та високу щільність підключень, що критично важливо для задач реального часу та автоматизованого управління. Таким чином, бездротові технології не лише забезпечують функціонування сучасних сервісів, а й виступають рушієм інноваційних трансформацій в умовах цифровізації всіх сфер життєдіяльності.

Завдяки цьому технологія Wi-Fi набула широкого поширення як у домашніх умовах, так і в громадських місцях, офісах та промислових

об'єктах. Основою роботи Wi-Fi є використання радіохвиль для передачі інформації між пристроями і точками доступу. Незважаючи на очевидні переваги, технологія Wi-Fi стикається з низкою викликів, пов'язаних із безпекою, радіо-перешкодами та обмеженням по дальності сигналу. Однак постійні інновації та розвиток стандартів сприяють усуненню цих проблем, роблячи бездротовий зв'язок дедалі надійнішим і доступнішим. Тому цей стандарт залишається ключовим елементом сучасного комунікаційного середовища та продовжує активно розвиватися.

Приховані канали та перешкоди – одні з ключових факторів, що впливають на якість та стабільність Wi-Fi з'єднання. Незважаючи на зовнішню простоту технології, бездротова передача даних схильна до безлічі впливів з боку навколишнього середовища та інших пристроїв, що працюють на тих же діапазонах частот. Проблема прихованих каналів виникає, коли пристрої знаходяться поза зоною прямої видимості один одного, але при цьому використовують ту саму точку доступу або канал зв'язку. В результаті вони можуть заважати один одному на рівні радіосигналів, не розпізнаючи присутність інших учасників мережі. Це призводить до конфліктів при передачі даних, зниження пропускної здатності каналу та збільшення кількості помилок, особливо за високої щільності клієнтів в одній мережі.

Радіоперешкоди є також поширеною причиною погіршення сигналу. У частині радіочастотного спектра загального призначення ISM на діапазоні 2.4 ГГц, який широко використовується для Wi-Fi, працюють багато інших пристроїв: мікрохвильові печі, бездротові телефони, Bluetooth-пристрої. Їхні сигнали можуть накладатися один на одного, викликаючи згасання чи спотворення корисного сигналу. У діапазоні 5 ГГц таких перешкод менше, але й зона покриття у нього більш обмежена, а сигнал гірше проходить крізь стіни та інші перешкоди. Також в умовах щільної міської забудови виникає проблема однакових каналів у сусідніх точок доступу, що призводить до перенасичення спектру сигналами та погіршення якості з'єднання.

Автоматичний вибір каналу не завжди справляється з цим завданням, особливо якщо в одній зоні працюють мережі різних провайдерів або власників.

Для боротьби з цими явищами застосовуються різні методи: вибір менш завантажених каналів, використання діапазону 5 ГГц або Wi-Fi 6 (стандарт IEEE 802.11ax), технології багатокористувацького доступу (MU-MIMO), а також ретельне планування розташування точок доступу. Однак повністю виключити вплив прихованих каналів та перешкод практично неможливо, особливо в умовах великої кількості користувачів.

Застосування радіомоніторингу та попереднього виявлення радіосигналів є критично важливим чинником для забезпечення стабільної роботи бездротових мереж у середовищі з високою щільністю радіочастотного трафіку. Ці методи дозволяють своєчасно ідентифікувати джерела радіозавад, нелегітимні передавачі, конфлікти частот та інші аномалії, які можуть негативно впливати на параметри зв’язку, зокрема – рівень сигналу, співвідношення сигнал/шум (SNR) та пропускну здатність каналів. Аналіз спектру в реальному часі забезпечує динамічну оптимізацію частотного ресурсу та зменшення ймовірності колізій, що особливо актуально для мереж з адаптивною модуляцією та багатокористувацьким доступом.

Крім того, виявлення та класифікація сигналів на ранніх етапах функціонування бездротової мережі дозволяє автоматизованим системам керування здійснювати вибір оптимальних параметрів зв’язку, включно з частотою, шириною смуги та типом модуляції, з урахуванням спектральної обстановки. Це сприяє покращенню енергоефективності пристроїв, зниженню затримок і втрат пакетів, а також підвищенню рівня кібербезпеки завдяки здатності виявляти потенційно шкідливі або аномальні сигнали. Таким чином, радіомоніторинг виступає не лише інструментом контролю, а й засобом адаптивного підвищення загальної якості та надійності бездротової комунікаційної інфраструктури.

1 АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Огляд існуючих систем виявлення каналів передачі сигналу

Для моніторингу прихованих радіоканалів передачі даних, які можуть заважати роботі обладнання у частотному діапазоні ISM, застосовуються різні методи виявлення сигналу. Сучасні системи виявлення каналів передачі радіосигналу класифікуються за рівнем складності, функціонального призначення та принципами обробки сигналу. Найбільш поширені варіанти включають: спектроаналізатори (у тому числі із смуговою та радіочастотною розгорткою), програмно-керовані радіоприймачі (SDR-системи), портативні частотоміри й сканери, а також стаціонарні комплекси пасивного моніторингу спектру. Спектроаналізатори дозволяють точно вимірювати амплітудно-частотні характеристики сигналів у широкому діапазоні частот, тоді як SDR-системи забезпечують гнучке програмне керування прийомом і обробкою сигналу, що робить їх придатними для виявлення та класифікації цифрових і адаптивно-модульованих каналів. Портативні пристрої використовуються переважно для польових задач в умовах обмеженого доступу, де критичними є автономність і швидкість реагування.

Більш складні системи, зокрема багатоканальні моніторингові комплекси та розвідсистеми електронної боротьби, поєднують широкосмуговий аналіз, розгалужену багатоточкову радіопеленгацію, машинне навчання для автоматичної класифікації сигналів, а також можливість геолокації джерел випромінювання. Такі системи, як CRFS RFeye, Narda SignalShark, або TCI Spectrum Monitoring Systems, забезпечують постійне сканування у реальному часі, реєстрацію порушень спектру, та динамічну ідентифікацію джерел радіосигналу. У військовому сегменті застосовуються замкнені комплекси з інтеграцією в мережеві

системи управління, що дозволяє не лише виявляти, а й оперативно протидіяти функціонуванню ворожих РЧ-каналів. Таким чином, спектр наявних рішень охоплює як мобільні аналізатори загального призначення, так і стратегічні платформи для безперервного контролю радіочастотного середовища.

Для спектрального аналізу використовується спектроаналізатор – пристрій, який вимірює рівень сигналу в широкому діапазоні частот. Дозволяє побачити, які частоти активні, виявити передавачі, завади та характер модуляції. Якщо вимірювана смуга частот виходить за межі одномоментної смуги пропускання приймача, то використовується радіочастотна розгортка (frequency sweep). Для цього послідовно знімаються спектри для кожного частотного відрізку на вимірювальному діапазоні, що потім об’єднуються в один суцільний спектр. Це можливо при використанні радіоприймача з регульованою частотою прийому.

Використання SDR (програмно-керованого радіо) дозволяє в реальному часі моніторити і записувати широкі смуги частот, проводити аналіз сигналів та декодування протоколів. Його перевагами є гнучкість та висока ефективність в обробці сигналів.

Також сучасним методом є системи виявлення на основі штучного інтелекту, що використовують алгоритми машинного навчання у завантаженому сигналами радіочастотному середовищі. Вони аналізують трафік, класифікують типи сигналів і визначають нові або несанкціоновані передавачі.

З усіх перелічених способів найбільш оптимальним буде використання спектроаналізатору з радіочастотною розгорткою. Він дозволяє сканувати радіочастотні канали з обраною шириною смуги пропускання, а кероване підлаштування частоти дає змогу безперервно охопити весь необхідний частотний спектр. Та, на відміну від SDR, не потребує додаткового високопродуктивного устаткування і використання ресурсоємних математичних обчислень (таких як перетворення Фур'є).

1.2 Обчислювальна платформа системи

Існує декілька варіантів придатних для використання в якості керуючого ядра системи, що розробляється. Порівняння мікроконтролерів, одноплатних комп'ютерів (ОПК), смартфонів та персональних комп'ютерів (ПК) ґрунтується на відмінностях в обчислювальній потужності, енергоспоживанні, рівні абстракції програмного забезпечення, апаратних ресурсах і призначенні. Мікроконтролери є системами на кристалі з жорстко обмеженими ресурсами (обсяг пам'яті в межах десятків/сотень КБайт, відсутність операційної системи), що призначені для детермінованого керування апаратними процесами в реальному часі. ОПК (наприклад, Raspberry Pi) реалізують повнофункціональну обчислювальну платформу із багатоядерними процесорами, графічними інтерфейсами, мережевими стеками та підтримкою ОС Linux. При цьому вони зберігають доступ до низькорівневих інтерфейсів (GPIO, I^2C, SPI), що дозволяє використовувати їх як мости між фізичним і програмним середовищем.

Смартфони і ПК характеризуються вищим рівнем інтеграції апаратного і програмного забезпечення, орієнтованим на користувача. Смартфони базуються на енергоефективних ARM-процесорах з оптимізованими мобільними ОС (Android, iOS) і містять широкий набір сенсорів, засобів зв'язку (Wi-Fi, LTE, BLE) і мультимедійних систем. ПК, у свою чергу, працюють на процесорах x86-архітектури, мають масштабовану оперативну пам'ять (до десятків ГБайт), високопродуктивні GPU, багаторівневі ОС (Windows, Linux) і слугують платформою для виконання ресурсоємних задач: обробки даних, візуалізації, розробки ПЗ тощо. Таким чином, мікроконтролери забезпечують мінімальні ресурси для чітко визначених задач керування, а ПК – максимально універсальні для широкого класу інформаційних обчислень. Тоді як смартфони й ОПК виступають як мобільні компроміси між функціональністю та ресурсами. Отже,

використання енергоефективних мікроконтролерів та одноплатних комп’ютерів дозволяє вбудовувати їх як частину фізичного пристрою для радіомоніторингу, значно поліпшуючи їхні характеристики з мобільності та часу автономної роботи.

Серед портативних спектроаналізаторів для радіомоніторингу поширення набули як комерційні пристрої, так і відкриті проєкти з використанням SDR. Вибір портативного спектроаналізатора пов’язаний з компромісом між автономністю, роздільною здатністю, шириною спектру, можливостями програмної обробки та вартістю. Комерційні пристрої переважають у простоті використання, тоді як SDR-рішення пропонують широку функціональність, але інколи ціною складнішої інтеграції.

Одним з таких відкритих проєктів є HackRF One у зв'язці з PortaPack H2, що дозволяє здійснювати базовий спектральний аналіз, прийом та передачу радіосигналів у широкому діапазоні без потреби у зовнішньому комп’ютері. Його функціональність значною мірою залежить від завантаженого мікропрограмного забезпечення, яке розширює можливості пристрою до сканування спектру, зчитування ідентифікаторів, ведення простого радіомоніторингу, перегляду аналогового телебачення тощо. З переваг цього пристрою ще можна виділити портативність, вбудований екран та елементи керування, що забезпечують автономність у дослідженні радіосередовища. Основними недоліками є значне енергоспоживання та не досить зручний інтерфейс для роботи у режимі радіомоніторингу. Інші портативні аналізатори спектру, наприклад, RF Explorer та TinySA, мають здебільшого такі самі переваги та недоліки.

Окремим класом пристроїв слід виділити портативні детектори радіосигналів, які призначені для виявлення активності в радіочастотному спектрі, зокрема пошук джерел сигналів у діапазонах VHF/UHF, GSM, Wi-Fi, Bluetooth та інших. Серед поширених моделей можна виділити K18 RF, iProtect 1216, JMDHKK M8000, а також більш спеціалізовані пристрої типу Protect 1207i або Hero009. Вони є ефективними для швидкого виявлення та

протидії несанкціонованому спостереженню, однак мають обмежену функціональність у порівнянні з пристроями класу SDR та спектроаналізаторами, і призначені переважно для побутового та прикладного використання. Детектори дозволяють лише виявити загальну присутність сигналу на широкому частотному діапазоні, та ніяк не розрізняють окремі частотні канали на передачу.

Переглянувши існуючі аналоги пристроїв, можна зробити висновок, що пріоритетом у розробці сканера радіочастотних каналів має бути низьке енергоспоживання та простий і зручний інтерфейс користувача. Також використання мікроконтролера в портативному спектроаналізаторі радіосигналів забезпечує автономну обробку та керування даними в умовах обмежених ресурсів і живлення. Мікроконтролер виконує функції конфігурування радіомодуля, збору та попередньої обробки спектральної інформації, взаємодії з дисплеєм та елементами керування, а також організації збереження та передачі даних. Завдяки низькому енергоспоживанню, компактним розмірам і наявності периферійних інтерфейсів (SPI, I^2C, UART), мікроконтролер є оптимальним ядром для побудови ефективного та стабільного пристрою. Крім того, мікроконтролери дозволяють реалізувати алгоритми цифрової обробки сигналів у режимі реального часу та можливість оновлення прошивки, що забезпечує гнучкість у модернізації пристрою. Таким чином, мікроконтролер виступає ключовим елементом у досягненні портативності, функціональності та енергоефективності такого приладу як спектроаналізатор.

Якість вимірювань залежить від чутливості використовуваного приймача і власних шумів мікросхеми. При проектуванні такого приладу необхідно враховувати перешкоди від мікроконтролера, блоку живлення та периферійних пристроїв. Особливо це актуально при використанні недорогих модулів, де екранування та розв'язка часто відсутні. Хорошою практикою є фізичне відділення радіомодуля від мікроконтролера, використання екрануючих корпусів та мінімізація шумів на лініях живлення.

1.3 Технічне завдання на проєктування

Виходячи з проведеного аналізу було сформовано технічне завдання на розробляємий пристрій, а саме:

- пристрій повинен виконувати сканування радіочастотного діапазону у межах 2400 - 2500 МГц;
- результати моделювання виводити на екран розробляємого пристрою;
- дозволяти користувачу оцінити ступінь завантеженності частотного радіоканалу;
- більш детальні результати виводити додатково на моніторі комп’ютера;
- повинен складатися з доступних компонентів, що завжди є в наявності у виробника;
- мати низьке енергоспоживання, якщо планується мобільне використання пристрою.

2 ВИБІР АПАРАТНОЇ ПЛАТФОРМИ

2.1 Структурна схема проєкту

Для забезпечення функціонування системи сканування радіочастотних каналів та виконання технічного завдання було розроблено структурну схему, яка наведена на рисунку 2.1.

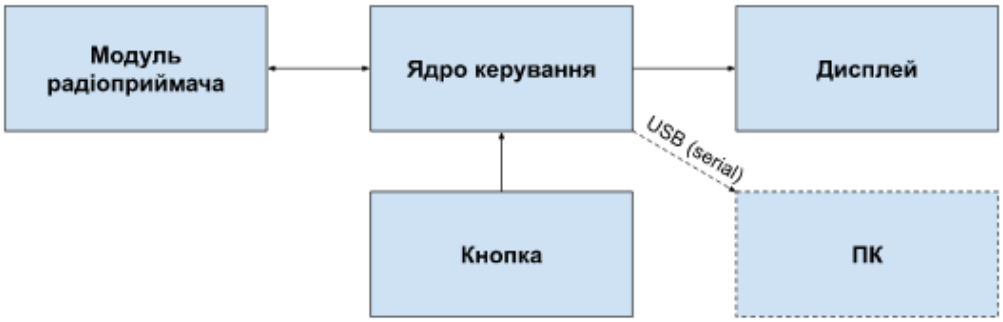


Рисунок 2.1 – Структурна схема системи сканування

Запропонована структурна схема позначає окремі фізичні компоненти системи, що відповідають вимогам до проєкту. Модуль радіоприймача здійснює прийом радіочастотного сигналу в заданому діапазоні частот, вимірювання його рівня і присутності на заданому частотному каналі, та передачу цифрових даних до керуючого ядра. Реалізується зазвичай на базі спеціалізованих чипів або модулів, що підтримують протокол зв’язку SPI або I^2C для інтеграції з ядром керування.

Ядро керування виконує роль центрального процесора системи, реалізуючи програмну логіку пристрою. Здійснює ініціалізацію периферійних модулів, обробку даних із радіомодуля, реакцію на вхідні події (натискання кнопок), а також керування відображенням інформації на дисплеї. Зазвичай базується на мікроконтролері, який забезпечує обчислювальні ресурси та фізичні інтерфейси.

Кнопка є засобом ручного введення, який дозволяє користувачеві ініціювати певні дії: зміну режиму, запуск сканування, оновлення даних тощо. Підключається до мікроконтролера через цифровий вхід, з використанням періодичного опитування його стану або зовнішнього переривання.

Дисплей виконує функцію візуалізації інформації, зокрема графічного представлення спектру, текстових повідомлень або параметрів системи. Залежно від вимог до роздільної здатності та споживання енергії, може бути реалізований на базі графічного дисплея з інтерфейсом I^2C або SPI.

Зв’язок з ПК є опціональним та дозволяє передавати більш деталізовані результати сканування для виводу на моніторі ПК. Підключення встановлюється за допомогою кабеля або через інший доступний інтерфейс. Обробкою прийнятих даних займається спеціалізований додаток на комп’ютері.

2.2 Вибір бездротового інтерфейсу

До класу радіомодулів, здатних приймати сигнали в діапазоні 2.4 ГГц, належать апаратні засоби, що використовують відповідні протоколи бездротового зв’язку, зокрема IEEE 802.15.4, Bluetooth, ZigBee, Wi-Fi та пропрієтарні протоколи на основі модуляцій GFSK або QPSK. Нижче подано перелік найбільш поширених мікроелектронних радіомодулів, які підтримують прийом у зазначеному частотному діапазоні:

- nRF24L01 – модуль від Nordic Semiconductor, що працює в діапазоні 2400-2525 МГц, підтримує модуляцію GFSK та пропрієтарні протоколи, широко використовується в IoT-системах;
- ESP8266 та серія ESP32 – модулі з інтегрованим Wi-Fi (802.11 b/g/n) у діапазоні 2.4 ГГц, ESP32 додатково підтримує BLE та має вбудований 32-розрядний мікропроцесор;

- nRF52 (наприклад, nRF52832, nRF52840) – мультипротокольні чипи з підтримкою Bluetooth Low Energy (BLE), NFC, ANT+ та ZigBee;
- CC2500 та CC2530 – модулі від Texas Instruments; CC2500 – для пропрієтарного зв'язку, підтримує декілька модуляцій сигналу та псевдовипадкове перелаштування робочої частоти, CC2530 – із вбудованою підтримкою IEEE 802.15.4 / ZigBee;
- RFM75 та RFM73 – модулі від HopeRF для передачі та прийому в ISM-діапазоні 2.4 ГГц з підтримкою різних типів модуляції;
- XBee Series 2 (ZigBee Mesh) – модулі, що реалізують стек ZigBee і працюють на частоті 2.4 ГГц;
- Cypress CYW43438 – комбіновані модулі Wi-Fi + Bluetooth, що інтегруються, зокрема, в Raspberry Pi.

Усі вказані модулі призначені для різних класів застосування – від сенсорних мереж до повнофункціональних бездротових вузлів, та характеризуються різним рівнем інтеграції, енергоспоживання та пропускної здатності.

Використання модуля nRF24L01 для сканування радіочастотного ефіру в діапазоні 2.4 ГГц є доцільним завдяки доступності в його архітектурі внутрішніх регістрів фізичного рівня, що забезпечує можливість безпосереднього аналізу рівня сигналу у кожному з 126 доступних каналів із кроком 1 МГц. Завдяки режиму сканування несучої частоти (carrier detect) користувач може виконати швидке виявлення зайнятих частот, що дозволяє сформувати спектральну картину активності в ISM-діапазоні без потреби в складному аналоговому фронтенді чи зовнішньому спектроаналізаторі. Крім того, низьке енергоспоживання, компактні розміри та широка підтримка бібліотек для різних платформ та мікроконтролерів (зокрема для Arduino, STM32, ESP32) роблять nRF24L01 оптимальним вибором для побудови простих, мобільних та автономних систем моніторингу спектру. На відміну від повноцінних SDR систем, nRF24L01 не потребує високопродуктивного процесора, а можливість швидкої конфігурації приймача через інтерфейс SPI

дозволяє реалізувати адаптивне сканування ефіру у режимі реального часу. Це особливо важливо для попереднього аналізу спектру в умовах обмежених ресурсів, наприклад, в сенсорних мережах або під час налагодження бездротових систем.

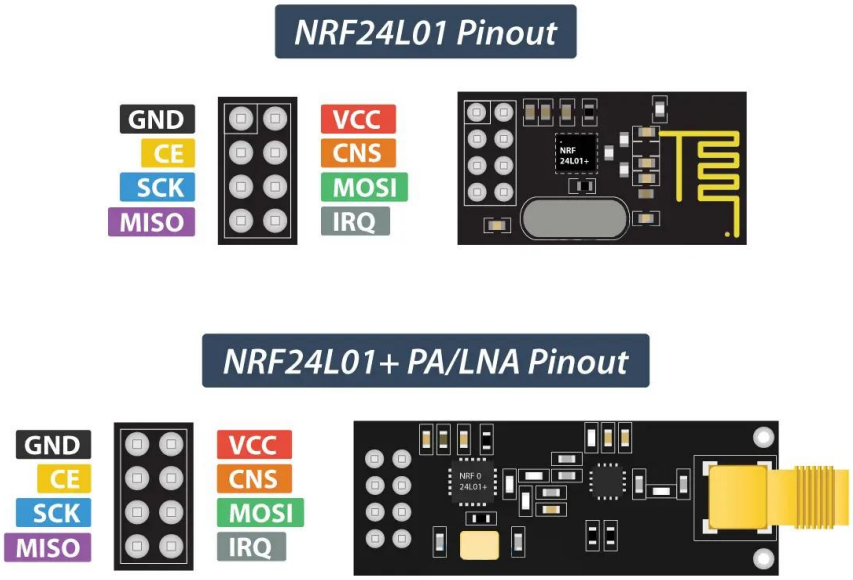


Рисунок 2.2 – Різновидності модуля nRF24L01

Модуль nRF24L01 є інтегрованим низькопотужним трансивером, розробленим компанією Nordic Semiconductor для роботи в безліцензійному ISM-діапазоні на частотах 2.4–2.525 ГГц. Його основні технічні характеристики визначають високу ефективність у задачах бездротової передачі даних на короткі та середні відстані з низьким енергоспоживанням. Модуль підтримує передачу даних зі швидкістю 250 кбіт/с, 1 Мбіт/с або 2 Мбіт/с з використанням модуляції GFSK (Гаусівської частотної маніпуляції). Модуль виробляється у декількох варіантах та може мати малошумний підсилювач (LNA) та підсилювач вихідної потужності (PA) одразу на його друкованій платі. Інші ключові характеристики включають:

- напруга живлення: 1.9–3.6 В (типово 3.3 вольта);
- максимальна вихідна потужність: +0 дБм (зовнішній підсилювач дозволяє збільшити до +20 дБм у версіях nRF24L01+PA+LNA);

- чутливість радіоприймача: до -85 дБм (на 2 Мбіт/с);
- кількість доступних каналів: 126 (з кроком 1 МГц);
- послідовний інтерфейс управління SPI (з частотою до 8 МГц);
- максимальна довжина пакета: 32 байти;
- наявні механізми виявлення колізій: автоматичне підтвердження прийому (ACK) та ретрансляція;

Завдяки вбудованій підтримці автоматичного узгодження адрес, керування чергами передачі, CRC-контролю та енергоефективним режимам сну, модуль є придатним для використання в бездротових сенсорних мережах, IoT-системах та системах моніторингу.

Якщо порівнювати характеристики модуля nRF24L01 з ESP8266, то він матиме наступні переваги:

- дозволяє детектувати радіосигнали, які передаються за іншими протоколами, а не тільки за стандартом Wi-Fi;
- більш широкий частотний діапазон та відсутність прив'язки до фіксованої кількості каналів Wi-Fi;
- порівняно більша швидкість сканування, завдяки відсутності потреби у декодуванні кожного прийнятого сигналу та очікуванні завершення прийому пакетів із даними.

Тому виходячи з усіх вищеперелічених факторів, використання цього модуля є оптимальним для потреб проєкту, що розробляється.

2.3 Вибір мікроконтролера

У сучасній практиці розробки вбудованих систем широке застосування знаходять мікроконтролери (МК), що характеризуються низьким енергоспоживанням, гнучкістю периферійних інтерфейсів та наявністю розвинутого програмного забезпечення. Серед найпоширеніших мікроконтролерів можна виділити наступні:

- STM32 (STMicroelectronics) – мікроконтролери на основі ядра ARM Cortex-M (від M0 до M7), що мають широкий спектр застосування завдяки високій тактовій частоті, великій кількості периферій (ADC, UART, SPI, I^2C, DMA), підтримці режимів низького енергоспоживання та наявності багатофункціонального програмного середовища STM32CubeMX / HAL / LL;
- RISC-V мікроконтролери – відкрита ліцензована архітектура, що орієнтована на високий ступінь програмної гнучкості, апаратну мінімізацію та використання в системах із відкритим апаратним кодом. RISC-V активно використовується в навчальних цілях, наукових дослідженнях та проєктах з потребою у повній архітектурній прозорості;
- ATmega/ATtiny (Microchip/Atmel) – 8-бітні мікроконтролери, які широко використовуються в навчальних цілях (Arduino Uno), простих IoT-проєктах та пристроях з невисокими вимогами до обчислювальних ресурсів;
- ESP8266 / ESP32 (Espressif Systems) – мікроконтролери з інтегрованими Wi-Fi та Bluetooth, що поєднують доступність, багатофункціональність і потужні засоби розробки (IDF фреймворк) та використовуються у бездротових мережах, смарт-пристроях та IoT;
- PIC (Microchip) – 8- та 16-бітні мікроконтролери, які застосовуються в промисловій автоматизації, системах керування та навчальних платформах, завдяки стабільності, широкому вибору моделей і підтримці розробників;
- MSP430 (Texas Instruments) – 16-бітні МК з ультранизьким енергоспоживанням, що використовуються у пристроях тривалого автономного функціонування, зокрема в сенсорних мережах та біомедичних системах;
- Raspberry Pi та подібні одноплатні комп’ютери – є мікропроцесорними платформами із підтримкою повноцінної ОС. Вони не є класичними

мікроконтролерами, однак часто застосовуються для обробки великих обсягів даних, управління периферією через GPIO та реалізації протоколів високого рівня.

Проаналізувавши цей перелік, модуль “Blue Pill” з мікроконтролером STM32F103C8T6 є оптимальним вибором для побудови аналізатора спектру завдяки ефективному балансу між продуктивністю та доступністю апаратної периферії. Він забезпечує достатній рівень обчислювальних ресурсів для реалізації алгоритмів обробки сигналів у реальному часі, сканування частотних діапазонів та візуалізації даних. Наявність апаратного SPI дозволяє швидко зчитувати дані з радіочастотних модулів типу nRF24L01, а підтримка DMA та таймерів – оптимізувати передачу та обробку даних без навантаження на центральне ядро. Крім того, інтерфейси USB та UART дозволяють виводити розширену спектральну інформацію на комп’ютер або інші пристрої візуалізації. Під’єднання до ПК можна здійснювати за допомогою фізичного USB інтерфейсу або через конвертер інтерфейсів, наприклад, FTDI FT232RL. Додатковими перевагами є наявність великої спільноти розробників, підтримка таких інструментів, як STM32CubeIDE, PlatformIO, Arduino IDE та сумісність з додатком OpenOCD для налагодження через SWD.

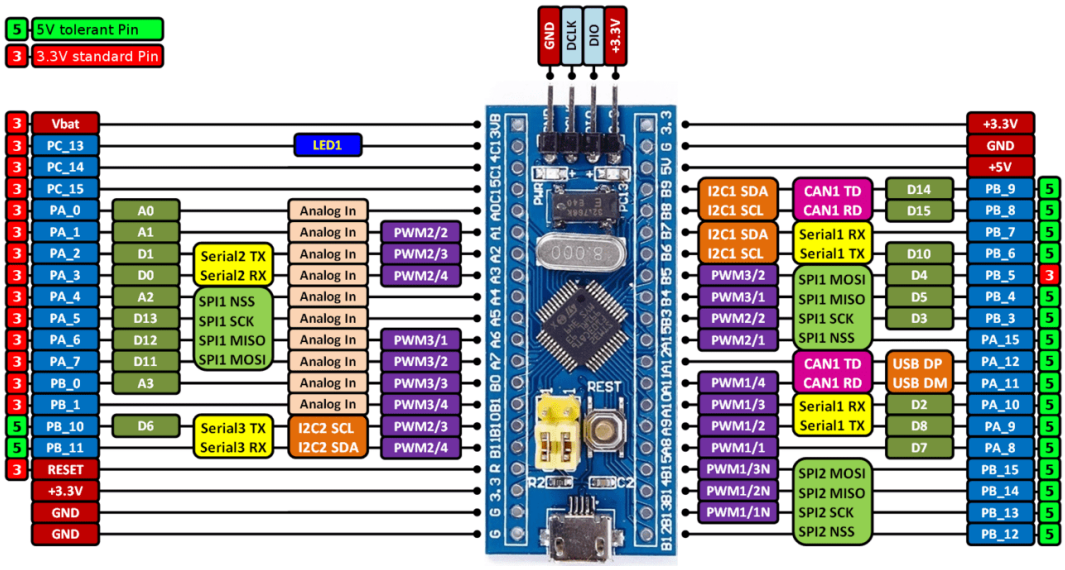


Рисунок 2.3 – Позначення пінів на модулі BluePill

Також використання готового модуля “Blue Pill” має низку конструктивних і функціональних переваг, що роблять його зручним для швидкої розробки електронних систем. Модуль постачається з уже виведеними контактами GPIO, що забезпечує пряме підключення до макетної плати або зовнішніх пристроїв без потреби у додатковому розведенні та виготовленні друкованої плати. Ще він містить перетворювач напруги в 3.3 вольта, схему скидання та інтегровані кварцові резонатори (8 МГц тактовий та 32.768 кГц для RTC), що забезпечують стабільну генерацію тактових сигналів та роботу МК. Також “Blue Pill” має попередньо встановлений мікро-USB роз’єм для живлення або програмування, що спрощує інтеграцію з комп’ютером, а також виведені контакти для програмного налагодження через SWD. Плата сумісна з різними програмними середовищами розробки, що дозволяє обирати зручний стек інструментів. Завдяки невеликим розмірам, низькій вартості й високій сумісності з екосистемою STM32, цей модуль оптимально підходить для прототипування даного проєкту.

Мікроконтролер STM32F103C8T6 має ядро ARM Cortex-M3, що тактується до 72 МГц, 20 КБ оперативної пам’яті та 64 КБ для зберігання даних та вбудованої програми.

2.4 Вибір дисплея

Спочатку необхідно з’ясувати, який тип та характер інформації потрібно відображати для користувача даного приладу. Результатом роботи будуть періодичні виміри спектру для наявних частотних каналів, що будуть змінюватися з плином часу. Базуючись на обраному модулі для радіоінтерфейсу, основними вимогами до засобу відображення є:

1) здатність відображати рівень для усіх 126 частотних каналів;
2) можливість зафіксувати максимальний рівень для кожного з каналів;

3) зобразити умовні позначення для частотних каналів за номером або частотою, а також умовну шкалу для рівня сигналу.

Таким чином, з’являється необхідність у виводі комбінованої графічної та текстової інформації.

Існує декілька основних методів відображення графічної інформації, що використовуються в сучасній електроніці. До них належать: LCD (Liquid Crystal Display) – рідкокристалічні дисплеї з підсвіткою, які широко застосовуються завдяки своїй доступності та низькому енергоспоживанню; TFT (Thin-Film Transistor LCD) – покращена версія LCD з можливістю відображення кольорової графіки та кращою швидкодією; E-Ink (електронне чорнило) – використовується здебільшого в електронних книгах завдяки наднизькому енергоспоживанню та відмінній читабельності при яскравому освітленні; LED-матриці – призначені переважно для відображення простої інформації або анімацій у зовнішніх інформаційних табло; OLED (Organic Light-Emitting Diode) – технологія з високою контрастністю та автономною світністю пікселів. Також можливо використовувати зовнішній інтерфейс (наприклад, HDMI або VGA) для виводу зображення на монітор, телевізор або проектор. Кожна з цих технологій має свої переваги у застосуванні, що залежать від вимог проєкту.

Для реалізації проєкту достатньо монохромної графіки з відносно невеликою роздільною здатністю, тому немає потреби у використанні кольорового TFT дисплею. З причин низької швидкодії та великої затримки на оновлення зображення не підійдуть й LCD та E-Ink дисплеї, а LED-матриці матимуть завеликі габарити для даного проєкту. Замість зовнішнього інтерфейсу виступатиме додаток на ПК.

Підсумовуючи усі зазначені вимоги, для виводу графічної інформації було обрано монохромний OLED-дисплей на базі контролера SSD1306 з роздільною здатністю 128 на 64 пікселів. Має наступні характеристики: робоча напруга від 3.3 до 5 вольт, діагональ 0.96 дюйма, великий кут огляду 160 градусів, енергоспоживання до 50 мВт. Контролер дисплею підтримує

два інтерфейси для обміну інформацією – SPI та I^2C, – вибір якого здійснюється за допомогою запаювання перемички на самому дисплеї.

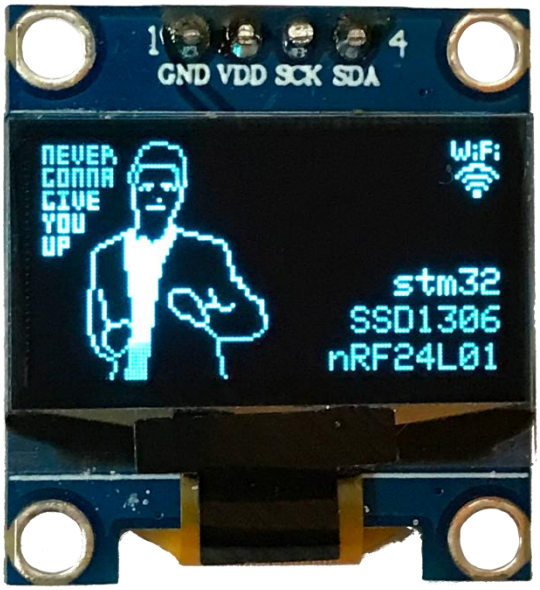


Рисунок 2.4 – Зовнішній вигляд дисплею на основі SSD1306

Його роздільна здатність дозволяє відобразити всю вищеперелічену графічну інформацію для частотного спектру. Також важливим фактором є низьке енергоспоживання, невелика ціна за модуль та наявність готових програмних бібліотек для роботи з модулем.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ ПРОЄКТУ

3.1 Структурно-функціональна схема пристрою

Згідно до складеної специфікації, спроєктований пристрій повинен мати бездротовий інтерфейс для сканування радіоефіру, інтерфейс для відображення даних та інтерфейс комунікації з ПК. Також опціональним є інтерфейс керування режимом сканування, що дозволить користувачу вибрати режим роботи пристрою. Ґрунтуючись на цих вимогах була створена функціональна схема пристрою, що зображена на рисунку 3.1. Вона визначає загальну архітектуру програмно-апаратного комплексу, де кожен блок позначає окрему функціональну одиницю та виконує визначену роль у забезпеченні процесу сканування радіочастотного спектру та виведення результатів.

Рисунок 3.1 – Функціональна схема пристрою

Взаємодія між кожним блоком відбувається через фізичні інтерфейси, що позначені стрілками на функціональній схемі. Кожен блок використовує свій окремий інтерфейс для зв’язку з іншим, що забезпечує передачу необхідної інформації або фізичних величин.

Центральним вузлом для взаємодії з іншими блоками виступає блок керування та аналізу даних. Він відповідальний за налаштування правильної роботи для кожного з блоків, обмін даними і зчитування вхідних сигналів, а також обробку отриманої інформації і формування видачі готових результатів у вигляді зображення або текстових повідомлень. Фізично реалізований на базі мікроконтроллера STM32 серії F103, що має в наявності усі необхідні фізичні шини обміну даними.

Блок прийому даних на комп'ютері займає роль посередника, що забезпечує передачу даних у програмний додаток. Реалізований у вигляді шини USB, послідовного протоколу передачі даних та набору необхідних драйверів для його роботи. Підключення до ПК відбувається через роз'єм USB Micro-B, що присутній на модулі "Blue Pill". Вивід даних на моніторі комп'ютера здійснюється за допомогою програмного додатку, що обробляє одержану інформацію та формує її графічну репрезентацію.

Блок вибору частотного каналу та вимірювання є найважливішим з точки зору функціональності пристрою, бо саме він відповідає за прийом радіосигналу з ефіру та детектування його рівня. Його роль виконує модуль nRF24L01 з антеною, що під'єднується до його роз'єму. Використовується шина SPI для обміну даними з МК.

Дисплей на базі контролера SSD1306 здійснює функцію блоку виводу інформації та виводить отримані дані у графічному вигляді. Отримання даних відбувається через двопровідну послідовну шину I^2C. Блок вибору режиму роботи являє собою сенсорну або тактову кнопку, що під'єднана до одного з цифрових входів мікроконтролера. Вона надає користувачу єдиний доступний інтерфейс керування пристроєм.

Для початку роботи з пристроєм необхідно забезпечити окреме живлення 5 вольт постійного струму. Це здійснюється за допомогою зовнішнього блоку живлення, що приєднується до терміналу "+5V" та загального потенціалу "GND" (землі); або підключенням комп'ютера чи портативної акумуляторної батареї (повербанка) до роз'єму USB Micro-B на

модулі “Blue Pill”, використовуючи USB-кабель. Після подачі напруги пристрій автоматично вмикається та проводить самодіагностику. Якщо усі модулі пристрою під’єднані правильно, у справному стані та ініціалізовані, то на дисплеї відобразиться шкала та почнеться сканування у режимі спектру по усім доступним радіочастотним каналам. В іншому випадку, при виникненні помилки, повідомлення про неї буде відправлено на комп’ютер та виведено на дисплей, якщо вони доступні.

3.2 Принципова електрична схема пристрою

Ґрунтуючись на структурно-функціональній схемі та використовуючи обрані електронні компоненти, була побудована принципова електрична схема пристрою сканування радіочастот, що зображена на рисунку 3.2. Зазначена схема відповідає вимогам, що зазначені в документації на використані компоненти та готові модулі.

При проєктуванні принципової схеми необхідно забезпечити стабільну та безперебійну подачу живлення для кожного компонента. Повинні бути відсутні коливання напруги та високочастотні пульсації, або знаходитися у межах 5% від номінального значення напруги для цифрових схем, а для чутливих радіочастотних елементів – не більше 1-2%. Використання додаткових конденсаторів та індуктивностей в якості фільтруючих елементів дозволяє забезпечити ці вимоги. Якщо готовий модуль не має у своєму складі фільтруючих конденсаторів, їх необхідно додати на схему окремо, якнайближче до його виводів живлення.

Спочатку було розроблено організацію подачі живлення та обрані необхідні рівні напруг для усіх компонентів пристрою. Для стабільної роботи модуля “Blue Pill” необхідно подати напругу, не більшу за +5.5 вольт відносно “землі”. Типове значення напруги складатиме +5 вольт постійного струму, що подається на контакт 38 даного модуля, позначений символом “5V”. При живленні модуля від USB, немає потреби у використанні

додаткового джерела живлення. Модуль nRF24L01 потребує додаткового стабілізованого джерела напруги на +3.3 вольта. Для цього використовується окремий лінійний стабілізатор напруги, на вхід якого подається +5 вольт. Він забезпечує компенсацію короткочасних сплесків напруги та фільтрацію шумів на лінії живлення модуля. Для живлення дисплею на базі контролера SSD1306 достатньо подачі напруги +3.3 вольта від модуля “Blue Pill”, підключившись до контакту 18 або 40, що позначений символом “3V3”. Вбудований лінійний стабілізатор модуля забезпечує необхідний струм для роботи дисплею.

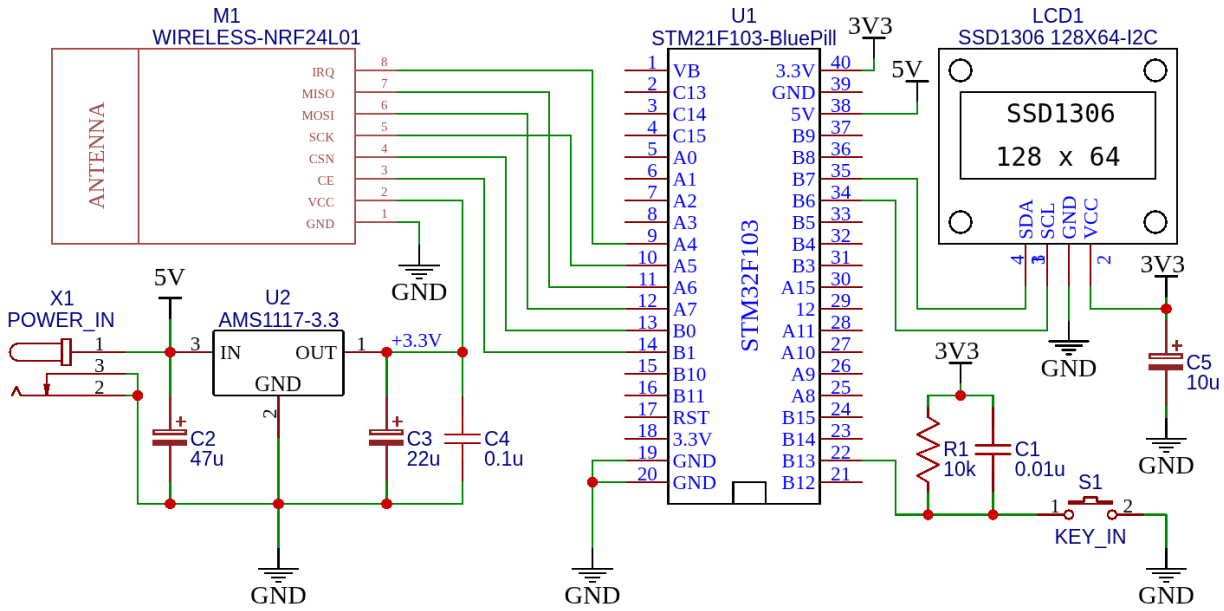


Рисунок 3.2 – Принципова електрична схема пристрою

Для підключення радіомодуля nRF24L01 була використана послідовна шина SPI. У використаному мікроконтролері доступно два апаратних інтерфейси SPI, але підключення до них можливе лише через фіксовані піни вводу-виводу (контакти на МК). Було обрано шину SPI1 з відповідними пінами “PA5”, “PA6” і “PA7”. Керування входами “CE” і “CSN” на радіомодулі здійснюється програмно, тому виходи на МК були обрані довільно. Потреби в додаткових елементах на шині SPI немає. Дисплей SSD1306 отримує дані по двопроводній шині I^2C. Цей інтерфейс також є

фіксованим та під’єднується до виводів “PB6” для тактування і “PB7” для передачі даних. Шина I^2C потребує додаткової підтяжки ліній до напруги живлення через резистори номіналом 4.7-10 кОм, але дисплейний модуль вже має їх на друкованій платі. Згідно документації на МК STM32F103C8T6 сигнальні лінії I^2C та SPI підтримують напругу не більшу за 3.3 вольта, що було враховано при узгоджені підключення між модулями.

Кнопка для керування режимом сканування під’єднується до контакту 22 модуля “Blue Pill”, що відповідає входу “PB13” на мікроконтролері та підтримує генерування зовнішнього переривання. Підключення кнопки зроблено за схемою зовнішньої підтяжки до живлення через резистор R1. Система усунення дребезгу контактів кнопки реалізована також на резисторі R1 та конденсаторі C1, що складають схему фільтру по струму.

Для роботи пристрою необхідно забезпечити живлення, що витримує сумарний струм для всіх модулів принципової схеми і складає не більше 75 мА у піку навантаження. Додатково можна використовувати схеми захисту від напруги неправильної полярності, але при використанні живлення від USB у цьому немає потреби. Також можна удосконалити схему, додавши літієвий акумулятор та модуль контролю заряду на мікросхемі TP4056. Використання тумблера на подачу живлення також полегшить користування пристроєм.

3.3 Підключення модуля приймача

Радіомодуль nRF24L01 підтримує обмін даними та керування через шину SPI та додаткові сигнальні лінії. Послідовна шина SPI – це синхронний інтерфейс обміну даними типу «ведучий-підлеглий», який дозволяє швидку двосторонню передачу інформації між мікроконтролером (ведучим) та периферійними пристроями (підлеглими) через чотири основні сигнальні лінії: SCLK (Serial Clock) – тактовий сигнал, що генерується ведучим; MOSI (Master Out Slave In) – лінія передачі даних від ведучого до підлеглого;

MISO (Master In Slave Out) – лінія передачі від підлеглого до ведучого; та SS/CS (Slave Select/Chip Select) – лінія вибору конкретного підлеглого пристрою.

Принцип роботи SPI полягає у тому, що при активному сигналі CS ведучий синхронізує передавання даних із підлеглим за допомогою SCLK: на кожен тактовий імпульс відбувається передавання біта по лінії MOSI і зчитування біта з MISO. Передача відбувається у фіксованих рамках байтів або слів, а реалізація повного дуплексу дозволяє одночасно передавати та приймати інформацію. Завдяки своїй простоті, високій швидкості (до десятків МГц) і низьким затримкам, SPI широко використовується для підключення дисплеїв, сенсорів, пам’яті, радіомодулів та іншої швидкодіючої периферій.

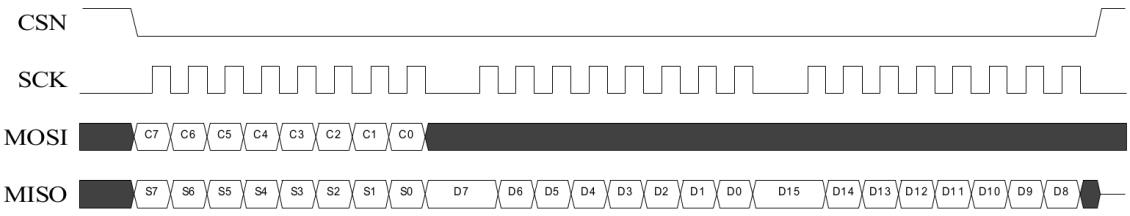


Figure 23. SPI read operation

Рисунок 3.3 – Приклад зчитування даних по шині SPI

Взаємодія по шині SPI приведена у технічній документації на модуль nRF24L01 та показана на рисунку 3.3. Спочатку передаються 8 командних біт, що визначають тип транзакції (читання, запис чи керування режимами роботи) та адресу регістру для доступу (займає 5 молодших бітів). При передачі байту команди SPI під час читання або запису, модуль завжди повертає один байт зі значення регістру статусу, що також доступний за адресою 0x07. Далі приймаються один або більше байт із значенням регістру (адреса якого була вказана) при читанні, або так само передаються при записі. Порядок біт у байті – від старшого до молодшого.

4 ПРОГРАМНА РЕАЛІЗАЦІЯ ПРОЄКТУ

4.1 Алгоритм функціонування пристрою

Запропоновано наступну послідовність роботи пристрою, що наведено на рисунку 4.1. Спочатку відбувається ініціалізація всіх модулів, що під’єднуються до мікроконтролера. Налаштовується тактування ядра та периферії МК, його портів вводу-виводу та робота послідовних інтерфейсів, таких як SPI, I^2C, USB. Далі перевіряється наявність підключеного модулю дисплею та здійснюється його ініціалізація. Та сама процедура виконується для радіомодуля, після чого відбувається його налаштування в режимі сканування за допомогою спеціальної послідовності інструкцій. Якщо в процесі ініціалізації модулів виникне помилка, то користувач буде проінформований про неї, і пристрій перейде в режим очікування перезапуску. Більш детально цей процес описаний у розділі 4.3.

Після успішної ініціалізації пристрій починає працювати в режимі вимірювання спектру. При цьому відбувається налаштування радіомодуля послідовно на усі доступні для нього радіочастотні канали та вимірюється рівень сигналу для кожного з них. Водночас виконується відображення на дисплеї отриманого рівня сигналу для поточного каналу, а також відправка даних на комп’ютер при наявності підключення. Додатково на дисплеї відображається шкала та частотний діапазон для зручності сприйняття інформації користувачем.

Для переходу між режимами сканування використовується тактова або сенсорна кнопка на пристрої. Одноразове натискання на неї перемикає між двома режимами: або сканування усього частотного діапазону, або сканування тільки каналів Wi-Fi. Вибір відповідного режиму та результати сканування виводяться на дисплей. Сканування та відображення інформації відбувається у нескінченному циклі поки пристрій увімкнений.

При підключенні до комп’ютера через USB-кабель та при запущеному додатку на ньому, відображається відповідний спектр радіочастотного ефіру, що був прийнятий радіомодулем пристрою. Також відбувається індикація максимального рівня сигналу, що був отриманий під час сканування для заданого частотного каналу. Він зберігається до наступного перезапуску пристрою або додатку.

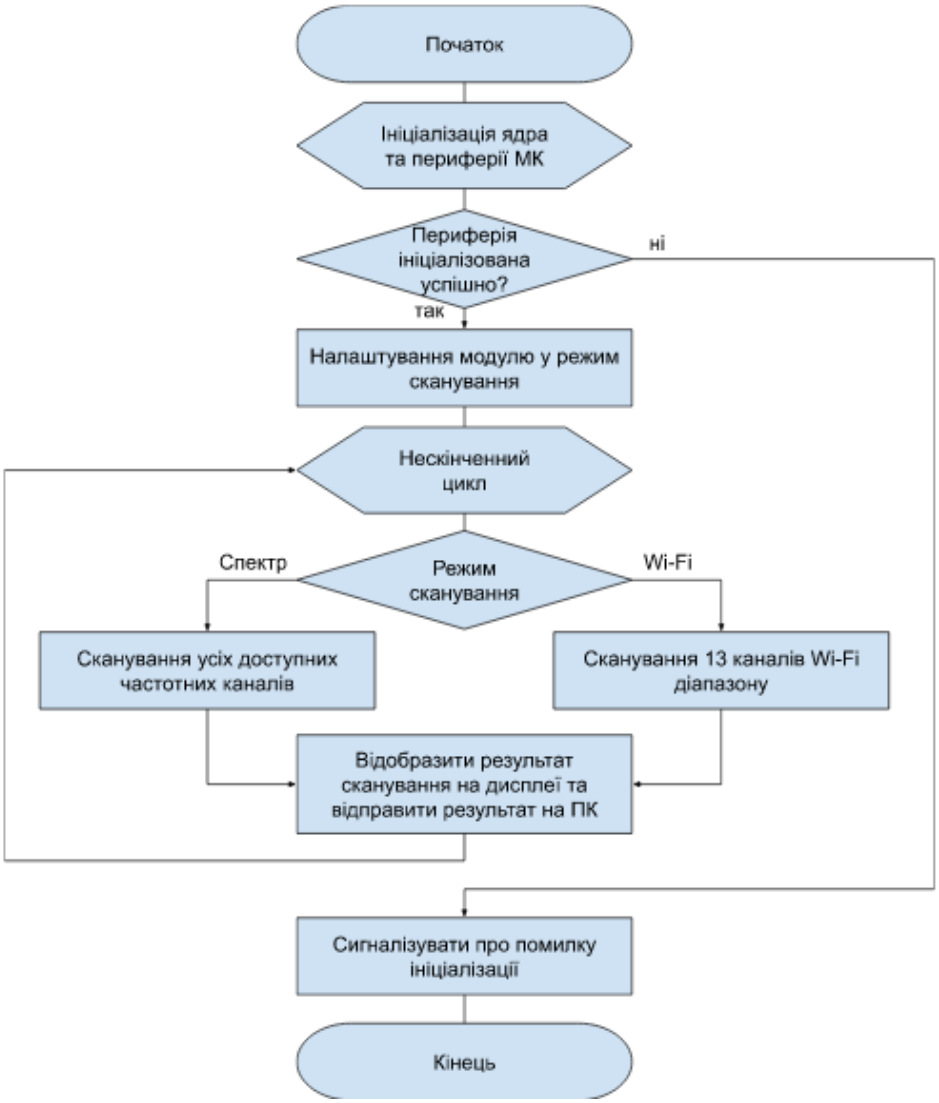


Рисунок 4.1 – Блок-схема алгоритму функціонування пристрою

Вимірювання рівня сигналу відбувається за допомогою методу накопичення кількості успішних випадків детектування на частотному каналі. Отримане значення визначає рівень для заданого каналу відносно кількості спроб вимірювання. На графіку відображається проміжок часу, в

період якого сигнал був присутній на обраній частоті та його задетектований рівень був більшим за -64 дБм під час вимірювань. Далі у розділі 4.3 цей процес розглянутий більш детально.

4.2 Вибір програмних засобів

Програмна частина була розроблена в інтегрованому середовищі розробки Microsoft Visual Studio Code з використанням розширень "PlatformIO" та "STM32 for VSCode". Налаштування проєкту під МК STM32F103 були виконані у додатку "STM32CubeMX".

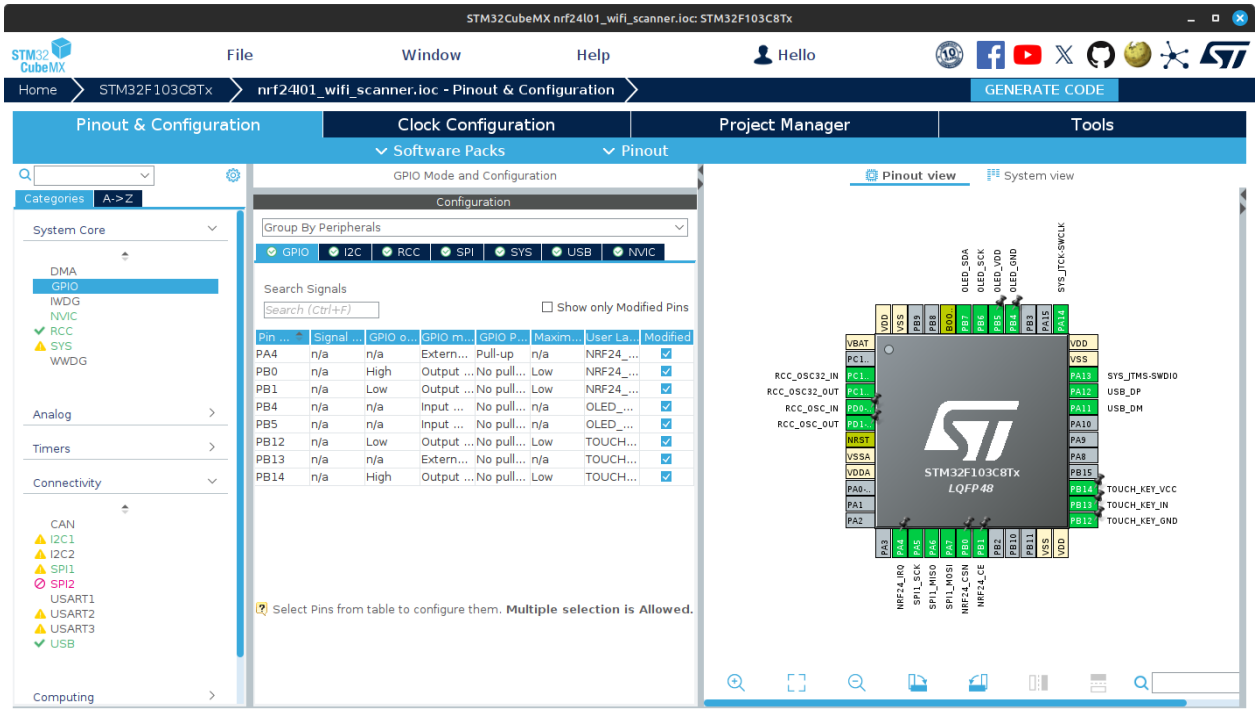


Рисунок 4.2 – Конфігурація проєкту у середовищі STM32CubeMX

Додаток STM32CubeMX від виробника мікроконтролерів STMicroelectronics є зручним і ефективним інструментом для створення проєктів під мікроконтролери STM32, оскільки автоматизує початкове налаштування периферії, тактування та конфігурацію фізичних контактів (пінів) через графічний інтерфейс. Це дає змогу суттєво скоротити час на написання початкової програмної структури проєкта та зробити необхідні

налаштування ядра та периферії мікроконтролера, що допомагає зменшити кількість помилок при ініціалізації МК. Програма генерує чисту та структуровану кодову базу, сумісну з поширеними IDE (наприклад, STM32CubeIDE або Keil), та додає до проєкту всі необхідні бібліотеки для роботи з МК, зокрема ARM CMSIS. Також підтримує інтеграцію з HAL або LL-драйверами, та дозволяє легко оновлювати конфігурацію без втрати користувацького коду.

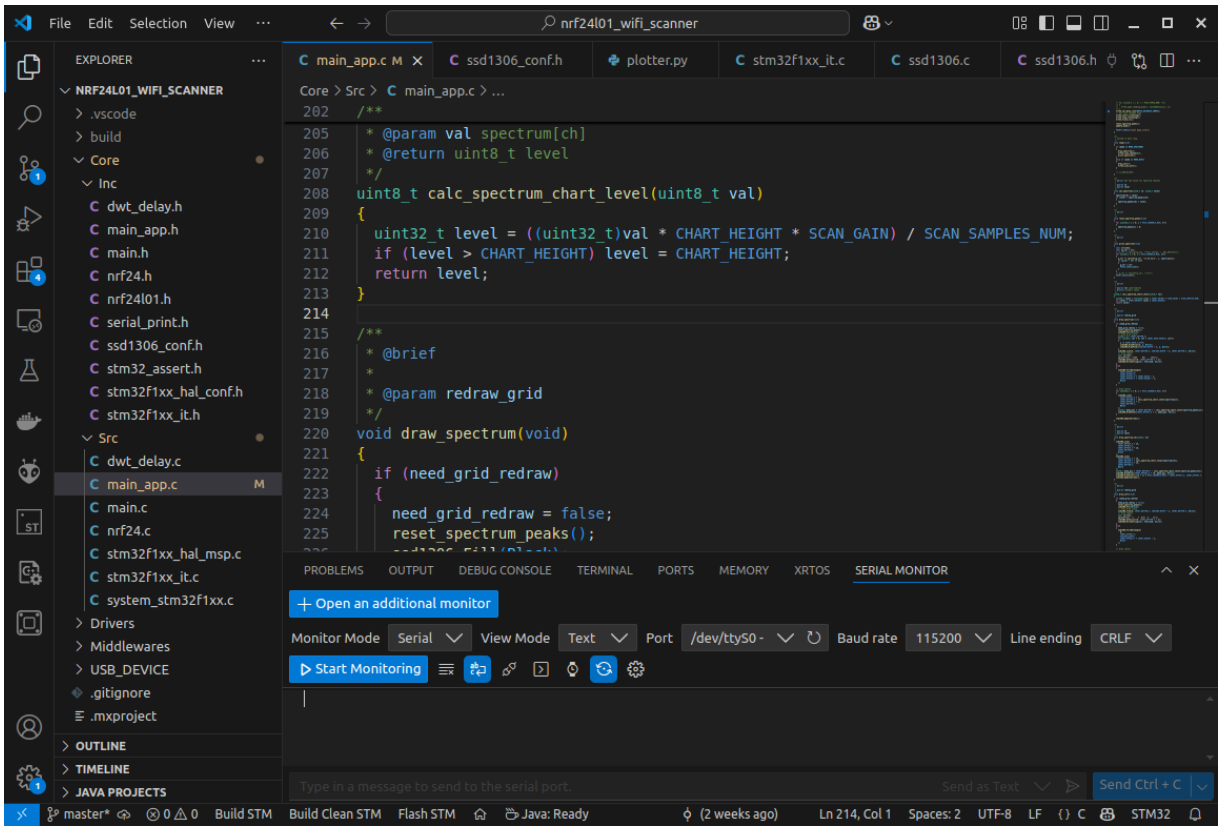


Рисунок 4.3 – Структура проєкту у середовищі розробки VS Code

У додатку STM32CubeMX було налаштовано тактування ядра та периферії на частоті 48 МГц, як найбільш оптимальна для потреб даного проєкту. З периферії було увімкнено послідовні інтерфейси I^2C (на частоті 400 кГц), SPI з тактуванням 6 МГц та USB у режимі віртуального послідовного порта для обміну даними з ПК. Де це було можливим, було ввімкнено використання LL-драйверів для більш оптимального використання ресурсів МК. Аби зробити проєкт універсальним та не мати прив’язки до

конкретного середовища розробки, було обрано метод складання проєкту через файл “Makefile” – спеціальний набір інструкцій для автоматизації побудови проєкту.

Visual Studio Code – зручне та легке кросплатформне середовище розробки з відкритим кодом, яке підтримує велику кількість мов програмування, та розширюється за допомогою гнучкої системи плагінів. Завдяки підтримки зовнішніх модулів, це середовище розробки дозволяє компілювати сирцевий код для обраного мікроконтролера та завантажувати отриманий бінарний файл у МК. Також є можливість використовувати режими покрокового відлагодження для більш детального розуміння роботи програмного коду на мікроконтролері. Ще важливим чинником, чому було обране це середовище розробки, є те, що цей редактор активно розвивається, регулярно оновлюється, має детальну та структуровану документацію, та велику активну спільноту користувачів і розробників. Також VS Code повністю безкоштовний і має відкритий сирцевий код (зберігається на GitHub), що дозволяє розширювати і кастомізувати його відповідно до потреб проєкту.

4.3 Алгоритм вимірювання рівня сигналу в частотних каналах

Вимірювання рівню сигналу в частотному каналі відбувається завдяки незадокументованому режиму роботи радіомодуля nRF24L01. Для використання модуля у режимі сканування спектру, попередньо необхідно встановити спеціальні налаштування. Ініціалізація проводиться одноразово при старті цього модуля. Мета цих налаштувань полягає в тому, щоб перевести модуль у режим невибіркового прослуховування радіоефіру. Для цього вимикається перевірка контрольної суми прийнятого пакету даних та відправка підтвердження прийнятого пакету. Так як сканування відбувається по частотних каналах з кроком 1 МГц, то налаштовується відповідна ширина каналу також в 1 МГц. Модуль має шість каналів на прийом даних, кожен зі

своєю унікальною адресою. Якщо встановити адреси цих каналів максимально подібними до шумового сигналу або преамбули пакета даних, то це дозволить приймати будь-які сигнали, а отже й отримувати їхній рівень. Тому встановлюються адреси каналів, наприклад такі 0x5555, 0xAAAA, 0xAAA0, 0xAAAB, 0xAAAC, та 0xAAAD. Після цього радіомодуль переводиться в режим очікування. Усі ці налаштування наведені у лістингу нижче.

Лістинг 4.1 – Початкове налаштування радіомодуля

```
nrf24_set_auto_ack(0); // вимкнути підтвердження прийому
// приймати будь-який сигнал
nrf24_set_crc_length(NRF24_CRC_DISABLED);
// обирається найкоротша можлива довжина поля адреси
nrf24_set_address_width(2);
for (uint8_t i = 0; i < RF24_PIPES_NUM; ++i)
{
  // дані адреси максимально подібні до шуму
  nrf24_open_reading_pipe(i, noiseAddress[i], 2);
}
// ширина каналу приблизно 1 МГц
nrf24_set_data_rate(NRF24_DATARATE_1MBPS);
// перехід у режим очікування
nrf24_start_listening();
nrf24_stop_listening();
nrf24_flush_rx();
```

Далі у основному циклі роботи МК викликається функція вимірювання сигналу nrf24_get_channel_level() для кожного з 126 доступних частотних каналів, що наведена у лістингу 4.2. Отримані дані зберігаються до масиву та відображаються на дисплеї, а також відправляються у додаток на ПК. Вимірювання рівню відбувається шляхом накопичення вдалих спроб детектування сигналу в частотному каналі із загальної кількості спроб. Кількість спроб attempts буде задавати максимальне значення рівня сигналу, тобто значення, що повертає функція, буде в межах від 0 до attempts включно. Повна версія цього програмного коду наведена у додатку Б.

Лістинг 4.2 – Функція отримання рівня сигналу в частотному каналі

```
uint8_t nrf24_get_channel_level(uint8_t ch, uint8_t attempts)
{
  uint8_t channel_level = 0; // регістр акумулятора
  nrf24_set_channel(ch); // перехід на новий канал
  nrf24_start_listening();
  while (attempts--) // вимірювання сигналу в каналі декілька
                     // разів
  {
    nrf24_set_rx_mode(); // перехід в режим прийому
    DWT_Delay(40); // рекомендована затримка 40 мкс для
                   // встановлення біту RPD
    nrf24_rf_disable(); // в цей момент виставляється біт RPD,
                        // якщо був прийнятий сигнал
    DWT_Delay(2);
    if (nrf24_get_rpd()) // перевірка біту RPD
    {
      ++channel_level; // прийнятий рівень сигналу був більшим
                       // за -64 дБм
    }
    nrf24_flush_rx();
    DWT_Delay(2);
  }
  nrf24_stop_listening();
  return channel_level;
}
```

Перед початком вимірювання виставляється номер каналу для радіомодулю в межах від 0 до 125, що відповідатиме діапазону частот від 2400 МГц до 2525 МГц. За це відповідає функція nrf24_set_channel(), що запише значення каналу у молодші 7 бітів регістру "RF Channel" за адресою 0x05 у радіомодулі. Далі у циклі модуль переводиться у режим прийому, очікує мінімально необхідний час для детектування сигналу, перевіряє перший біт CD регістру "Carrier Detect" за адресою 0x09, та повторює вимірювання знову. На сторінці 21 документації на радіомодуль nRF24L01 вказано, що мінімальний час очікування має бути не меншим за 128 мкс. У реалізованій програмній частині цей час сумарно складає 170 мкс. Наприкінці циклу кожного разу відбувається вимкнення режиму приймання та очищення черг каналів прийому. Дане вимірювання виконується для всіх обраних каналів на сканування в залежності від режиму роботи: від 0 до 125 каналу для усього спектру, та для 12, 17, 22, 27, 32, 37, 42, 47, 52, 57, 62, 67 і 72 каналів для режиму Wi-Fi (що відповідають центру сигналу на каналах).

4.4 Виведення інформації

Відображення інформації на дисплеї відбувається у двох режимах. Перший режим відображає рівень сигналу на безперервному частотному спектрі у діапазоні від 2400 МГц до 2525 МГц з кроком 1 МГц, що відповідає 126 частотним каналам, які доступні на обраному чипі nRF24L01.

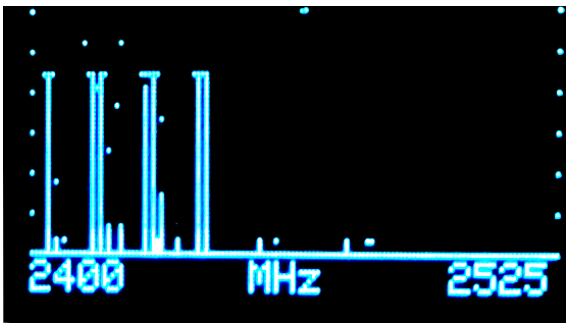


Рисунок 4.4 – Режим відображення спектру

У другому режимі відображається рівень сигналу для кожного з 13 каналів бездротової мережі Wi-Fi на діапазоні 2.4 ГГц, згідно протоколу IEEE 802.11n.

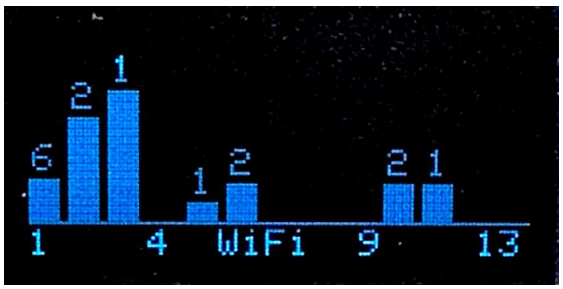


Рисунок 4.5 – Режим відображення Wi-Fi каналів

У кожному з режимів додатково фіксується та відображається максимальний рівень сигналу, що був знайдений під час сканування. Позначається горизонтальною рискою або одиночним пікселем над кожним стовпчиком сигналу на частотному діапазоні. Для перемикання між режимами роботи використовується сенсорна кнопка S1, позначена на схемі.

Бібліотека для роботи з OLED-дисплеєм базується на відкритому початковому коді з ресурсу GitHub, що доступна за посиланням [6]. Вона надає програмний інтерфейс для керування дисплеєм та формування графічного зображення. Підтримує виведення тексту з використанням вбудованого набору шрифтів, а також роботу з графічними примітивами – лінія, прямокутник, коло тощо. Таким чином, цей програмний модуль дозволяє сформувати усю графічну інформацію для відображення користувачу пристрою.

4.5 Взаємодія з користувацьким терміналом

Окрім виведення інформації безпосередньо на дисплеї розробленого апаратного стенду, є можливість відображення цих даних у розробленому додатку на персональному комп’ютері. Додаток являє собою скрипт, що розроблено на інтерпретованій мові програмування високого рівня Python. Це дозволяє запускати його незалежно від типу встановленої операційної системи (за умови встановленого інтерпретатора та наявності графічної оболонки).

Фізичне підключення апаратного стенду до персонального комп’ютера відбувається за допомогою інтерфейса USB через відповідний кабель. В даному випадку, модуль “Bluepill” виконує роль USB-пристрою, а ПК – роль USB-хоста. В якості логічного інтерфейсу використовується протокол USB Communication Device Class, а поверх нього створюється емуляція віртуального COM порта (VCP). Це виявляється можливим завдяки вбудованій функції мікроконтролера STM32 та набору програмних бібліотек HAL до нього. Зазвичай не потребується встановлення додаткових драйверів для роботи віртуального COM-порту, але для ОС Windows їх можна завантажити з сайту виробника мікроконтролерів STM.

Для початку роботи з боку мікроконтролера достатньо налаштувати проєкт у STM32CubeMX та провести ініціалізацію USB периферії

викликавши функцію MX_USB_DEVICE_Init(). Надалі відправка даних відбувається під час виклику функції print_spectrum(), що наведена у наступному лістингу.

Лістинг 4.3 – Функція відправка даних на ПК

```
char str[32];
for (uint8_t i = 0; i < RF24_CHANNELS_MAX; i++) {
  sprintf(str, "ch:%u,%u\n", i, spectrum[i]);
  while(
    (hUsbDeviceFS.dev_state != USBD_STATE_SUSPENDED) &&
    (CDC_Transmit_FS((uint8_t*)str, strlen(str)) == USBD_BUSY)
  ) {;}
}
```

На боці ПК прийом та розбір даних відбувається у скрипті функцією update(), що наведена у лістингу 4.4. Даний метод використовує технологію регулярних виразів для розбору прийнятих даних, та здійснює пошук співпадінь за вказаним патерном і довжиною повідомлення. У результаті обробки номер частотного каналу відкладається на осі абсцис X, а рівень – на осі ординат Y.

Лістинг 4.4 – Функція прийому даних з послідовного порта

```
data_lines = self.ser.readlines(8)
for data_str in data_lines:
    data = re.split(',|:', data_str.decode().strip())
    if (not data) or (data[0] != "ch"): continue
    ch = int(data[1])
    if (ch >= self.ch_num): ch = self.ch_num - 1
    level = int(data[2])
    self.levels[ch] = level
```

Запуск скрипту виконується у терміналі користувача за допомогою наступної команди: “python plotter.py --port /dev/ttyACM0”. В якості значення параметра “--port” необхідно вказати актуальний інтерфейс послідовного порта. Наприклад, для ОС Windows це значення матиме вид “COM13”, для ОС Linux/Mac виглядатиме як “/dev/ttySx”. Також скрипт можна виконати напряму у інтерпретаторі Python.

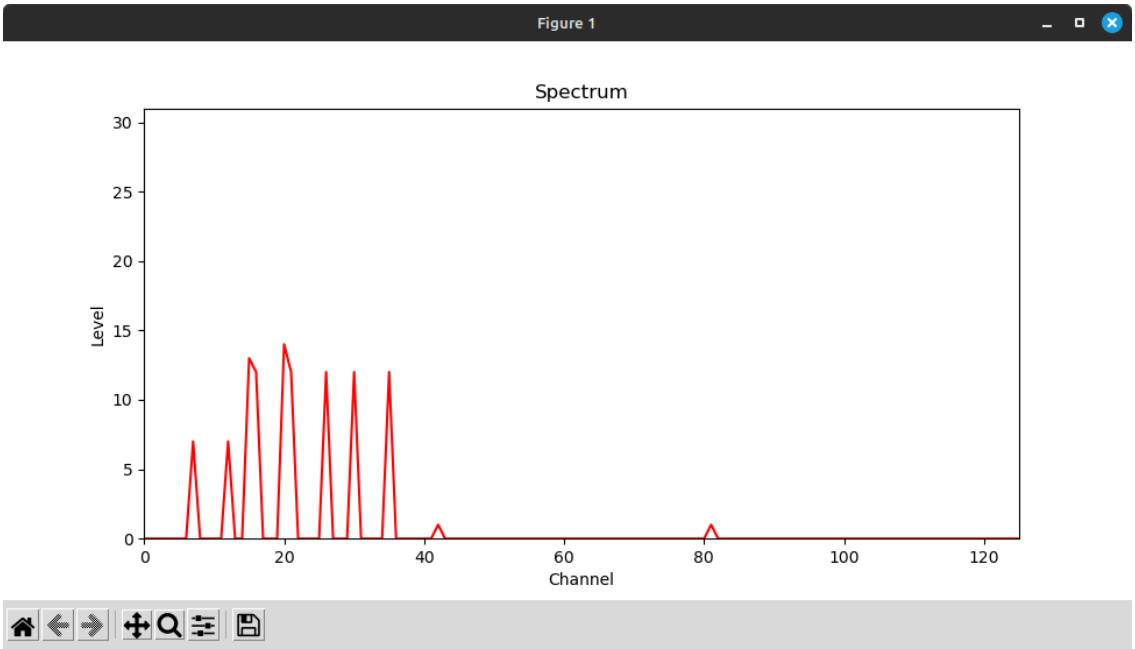


Рисунок 4.6 – Вигляд додатку для відображення прийнятих даних

Під час сканування каналів графік матиме вигляд, аналогічний виводу на вбудований дисплей апаратного стенду. Але завдяки гнучкості даних, котрі надсилаються від мікроконтролера, цей графік можна доповнити та розширити додатковою інформацією. Повний лістінг сирцевого коду скрипта на мові програмування Python приведено у додатку Б.

4.6 Результати роботи розробленого стенду

В ході виконання тестування пристрою було зібрано апаратний стенд, що представлений на рисунку 4.7. Для побудови стенду були використані модулі, що зазначені на принциповій електричній схемі на рисунку 3.2, а саме модуль “Blue Pill” з мікроконтролером STM32F103C8T6, дисплей на основі контролера SSD1306 та радіомодуль nRF24L01 з підсилювачем сигналу і зовнішньою антеною на діапазон 2.4 ГГц. В якості кнопки для керування режимом роботи був використаний сенсорний модуль на основі мікросхеми TTP223. Модулі були зібрані на макетній платі та під’єднані за допомогою проводів-перемичок DuPont. Також був використаний окремий модуль-перетворювач напруги, для забезпечення живленням +5 вольт

зібраної схеми. На його вхід подавалася напруга +12 вольт від мережевого блоку живлення. Програмний код проєкту був скомпільований у бінарний файл, який був завантажений у мікроконтролер за допомогою програматора ST-LINK V2, що під’єднується до відповідних контактів на модулі “Blue Pill”.

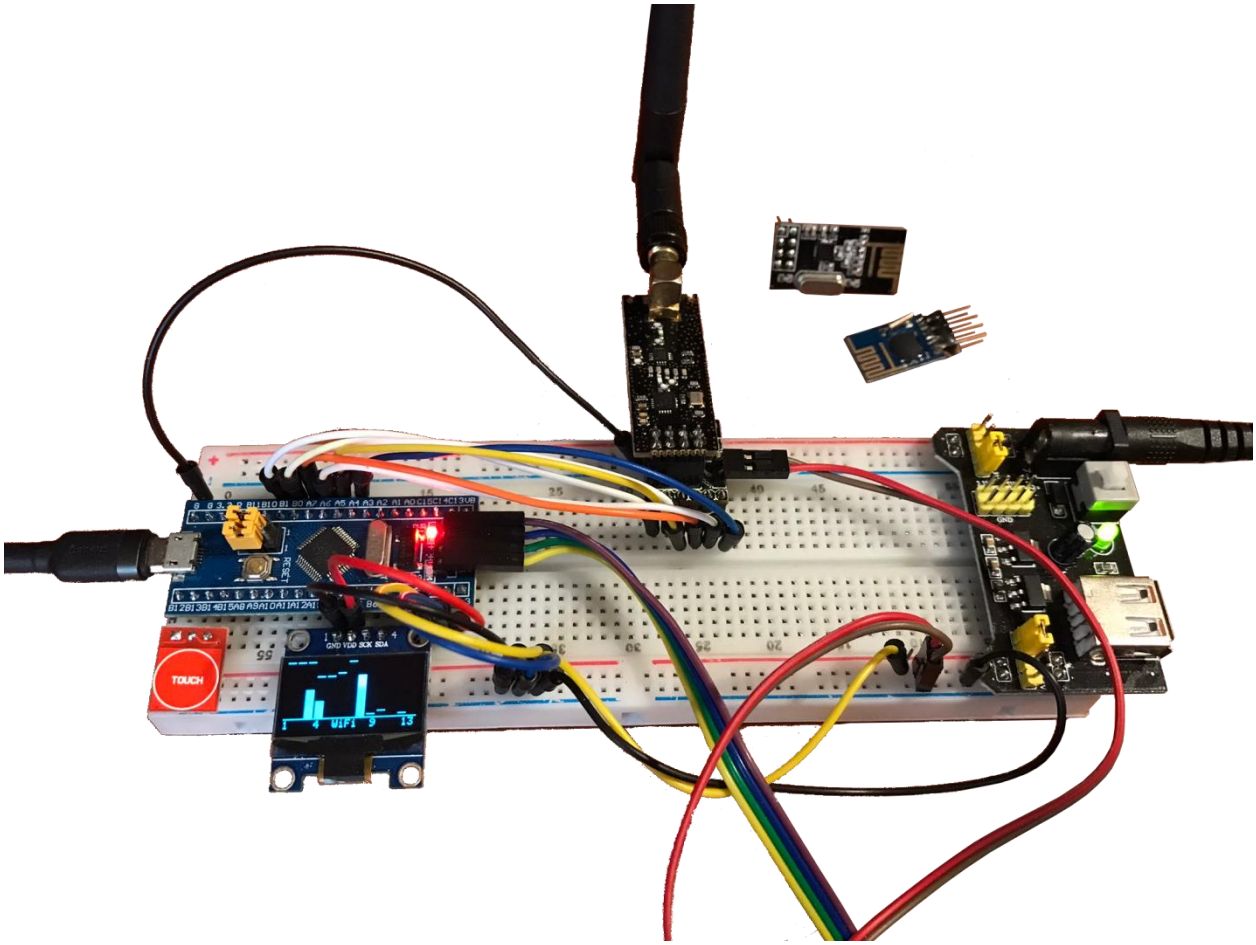


Рисунок 4.7 – Зовнішній вигляд розробленого макету приладу

В результаті роботи перевірочного стенду було виміряно рівні сигналів від навколишніх точок доступу Wi-Fi на відповідних частотних каналах. Було протестовано режим вимірювання спектру з підключенням до комп’ютера, результати якого показані на рисунку 4.6. Також було проведено вимірювання, використовуючи різні версії радіомодуля, та зроблено відповідні висновки щодо чутливості їх антен на прийом сигналу.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи було виконана розробка пристрою для сканування радіочастотного спектру та пошуку прихованих бездротових мереж. Було проведено огляд існуючих систем виявлення каналів передачі сигналу та моніторингу радіоспектру, проаналізовані переваги та недоліки існуючих засобів. На основі проведеного аналізу була сформована структурна схема пристрою та виконано вибір елементної бази. У якості бездротового інтерфейсу обрано радіомодуль nRF24L01, дисплей SSD1306 для відображення даних та мікроконтролер STM32F103C8T6 для керування усім пристроєм.

Було запропоновано структурно-функціональну схему пристрою та розроблена принципова електрична схема. Були обрані програмні засоби для розробки проєкту та інструменти для програмування пристрою. Згідно алгоритму функціонування пристрою були написані програмні компоненти вимірювання рівня сигналу, виведення інформації та взаємодії з комп’ютером. Для тестування роботи пристрою був зібраний випробувальний стенд. У результаті роботи було визначено, що пристрій відповідає зазначеним технічним вимогам.

Пристрій можна застосовувати для виявлення наявності сигналу на радіочастотному каналі та відсоток часу, впродовж якого сигнал був присутній. Може бути використаний як частина комплексу РЕР (радіоелектронної розвідки), а також як більш дешевша альтернатива обладнанню для аналізу спектру у радіоефірі. Придатний для детектування стаціонарних пристроїв-джерел радіосигналу, або виявлення дронів, що працюють на заданому частотному діапазоні.

Для подальшого вдосконалення пристрою можна об'єднати модулі ESP8266 з NRF24 та виводити більш детальну інформацію на термінал користувача. Модуль ESP8266 дозволить підвищити швидкість сканування

наявних точок доступу Wi-Fi та отримати більш точний рівень сигналу RSSI. Також він надасть можливість ідентифікації сигналу як того, що відповідає стандарту IEEE 802.11, та його характеристики: назву точки доступу SSID, чи є вона прихованою, тип шифрування, номер каналу тощо. Порівнюючи прийняту інформацію з цих двох модулів, можна більш точніше виявляти та аналізувати наявні радіосигналі в етері частотного діапазону ISM на 2.4 ГГц.

Також можна додати акумулятор та контролер заряду до нього, перенести усі компоненти у пластмасовий корпус, вивівши органи управління та індикації назовні. Це дозволить зробити розроблений пристрій мобільним та енергонезалежним, а компактні розміри та невелика вага дозволять носити його навіть у кишені.

ПЕРЕЛІК ПОСИЛАНЬ

1. Матвієнко М. Комп'ютерна схемотехніка. Навчальний посібник / Матвієнко М., Розен В. – К. : Ліра-К, 2014. – 192 с.

2. Кривуля Г. Ф. Схемотехніка: Навчальний посібник / Кривуля Г. Ф., Рябенький В. М., Буряк В. С. – Харків : ТОВ “Компанія СМІТ”, 2007. – 250 с.

3. Sarah Harris. Digital Design and Computer Architecture: ARM Edition, 1st edition / S. Harris, D. Harris. – Morgan Kaufmann, 2015. – 584 с.

4. ДСТУ ГОСТ 7.1:2006. Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання / Нац. стандарт України. – Вид. офіц. – [Чинний від 2007-07-01]. – К.: Держспоживстандарт України, 2007. – 47 с.

5. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання / Нац. стандарт України. – Вид. офіц. – [Уведено вперше ; чинний від 2016-07-01]. – К.: ДП «УкрНДНЦ», 2016. – 17 с.

6. GitHub.com, програмний код проєкту ssd1306-stm32HAL [Веб-сайт]. – Режим доступу: https://github.com/4ilo/ssd1306-stm32HAL – Назва з екрана. – Дата звернення:03.03.2025.

7. nRF24L01 Single Chip 2.4GHz Transceiver: Product Specification, Revision 2.0 [Електронний ресурс] – Nordic Semiconductor, 2007. – 74 с. – Режим доступу: https://docs.nordicsemi.com/bundle/nRF24L01_PS_v2.0/resource/nRF24L01_PS_v2.0.pdf – Назва з екрана. – Дата звернення: 04.03.2025.

8. STM32F103x8, STM32F103xB Datasheet – production data. Medium-density performance line ARM®-based 32-bit MCU [Електронний ресурс]. – STMicroelectronics, 2023. – 114 с. – Режим доступу: https://www.st.com/resource/en/datasheet/cd00161566.pdf – Назва з екрана. – Дата звернення: 04.03.2025.

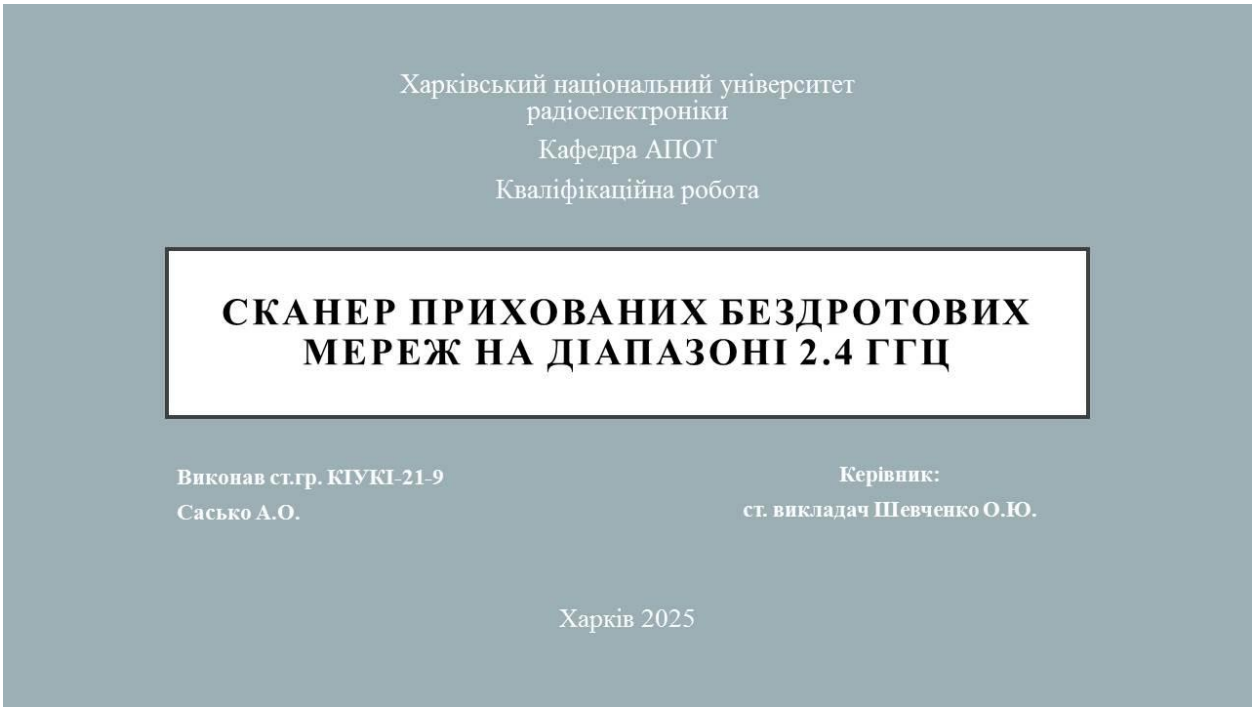
9. Handbook on Spectrum Monitoring / International Telecommunication Union. – Geneva: ITU, 2011. – 492 c.

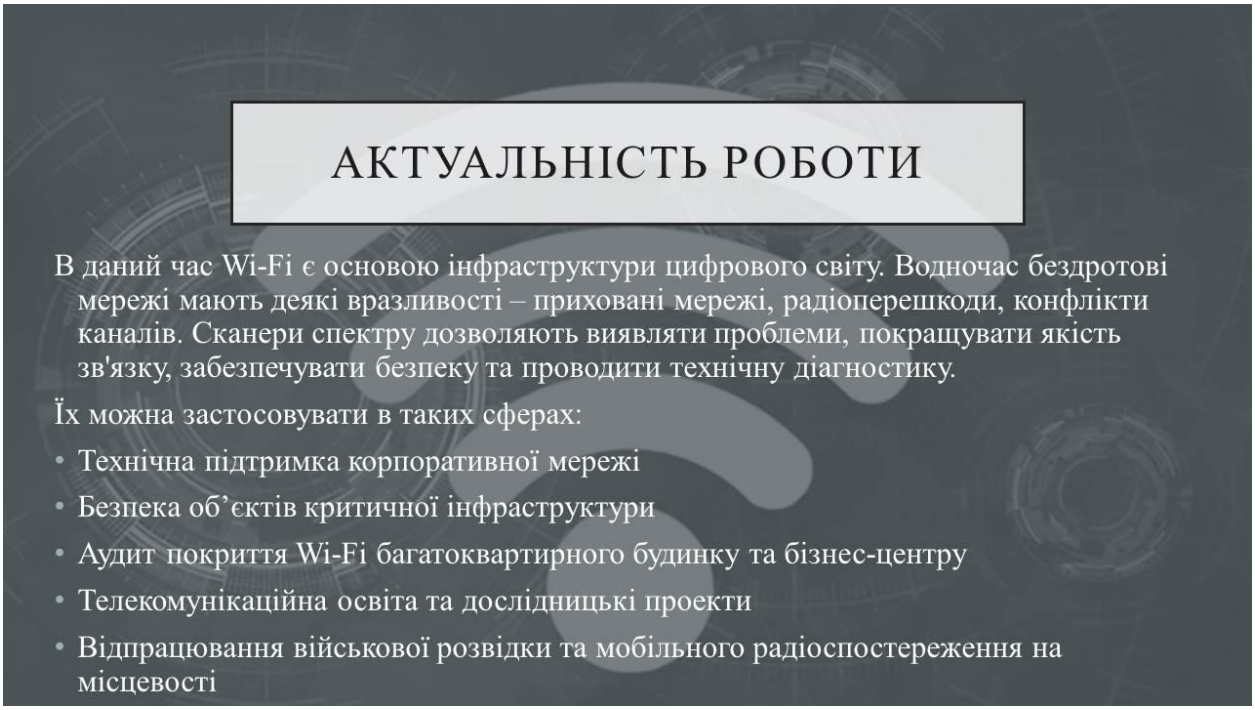
10. Analysis of the implementation efficiency of digital signal processing systems on the technological platform SoC Zynq 7000 / Olexander Shkil, Oleh Filippenko, Dariia Rakhlis, Inna Filippenko, Valentyn Kornienko // Radioelectronic and Computer Systems. – 2024. – No. 4 (112). – P. 168-177.

11. Evaluation of the performance of a computing cluster based on single board raspberry pi 3b+ computer / O. Barkovska, V Korniienko, I Filippenko et al. // 4th KhPI Week on Advanced Technology (KhPIWeek), Kharkiv, Ukraine, 02-06 October, 2023: proceedings. – P. 1–6.

ДОДАТОК А

Графічний матеріал кваліфікаційної роботи





ПОСТАНОВКА ЗАДАЧІ:

- пристрій повинен виконувати сканування радіочастотного діапазону у межах 2400 - 2500 МГц;
- результати моделювання виводити на екран розробляємого пристрою;
- дозволяти користувачу оцінити ступінь завантеженності частотного радіоканалу;
- більш детальні результати виводити додатково на моніторі комп'ютера;
- повинен складатися з доступних компонентів, що завжди є в наявності у виробника;
- мати низьке енергоспоживання, якщо планується мобільне використання пристрою.

АНАЛІЗ ПРЕДМЕТНОЇ ГАЛУЗІ

Для моніторингу прихованих радіоканалів передачі даних, які можуть заважати роботі обладнання у частотному діапазоні ISM, застосовуються різні методи виявлення сигналу:

- **Спектроаналізатори (у тому числі із смуговою та радіочастотною розгорткою)**
- **Програмно-керовані радіоприймачі (SDR-системи)**
- **Портативні частотоміри й сканери**
- **Стаціонарні комплекси пасивного моніторингу спектру**

ОСНОВНІ ТИПИ МІКРОКОНТРОЛЕРІВ У ВБУДОВАНИХ СИСТЕМАХ

STM32 (ARM Cortex-M)

RISC-V

ATmega / ATtiny (Microchip/Atmel)

ESP8266 / ESP32 (Espressif Systems)

PIC (Microchip)

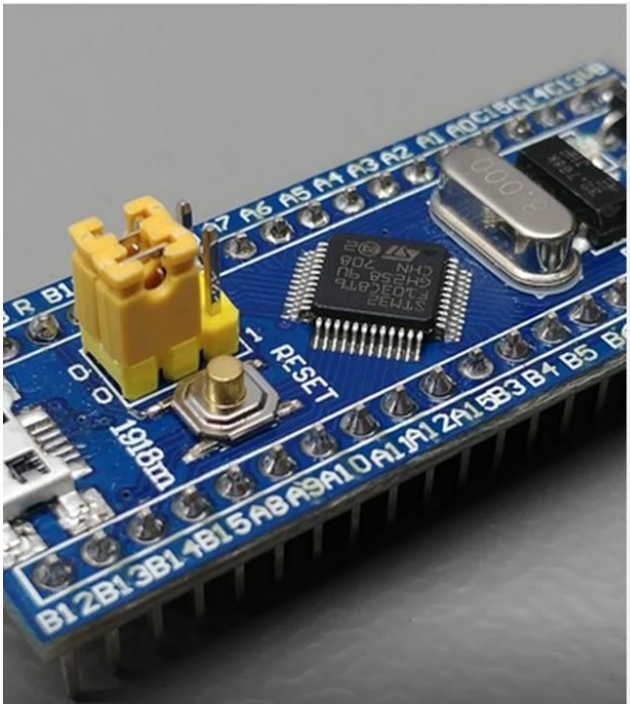
MSP430 (Texas Instruments)

Raspberry Pi та подібні

СТРУКТУРНА СХЕМА СИСТЕМИ СКАНУВАННЯ

Схема включає ключові компоненти:

- **Радіомодуль** приймає сигнал у діапазоні 2.4 ГГц, вимірює його рівень і передає дані мікроконтролеру через SPI/I2C.
- **Ядро керування (МК)** ініціалізує модулі, обробляє дані, керує дисплеєм і реагує на події.
- **Кнопка** дозволяє вручну запускати сканування чи змінювати режим.
- **Дисплей** виводить інформацію (спектр, текстові дані) через I2C або SPI.
- **Зв'язок із ПК** (опційно) дозволяє передавати результати сканування для подальшої обробки.
- Схема забезпечує функціональність відповідно до технічного завдання.



ГОТОВИЙ МОДУЛЬ “BLUE PILL” З МІКРОКОНТРОЛЕРОМ STM32F103C8T6

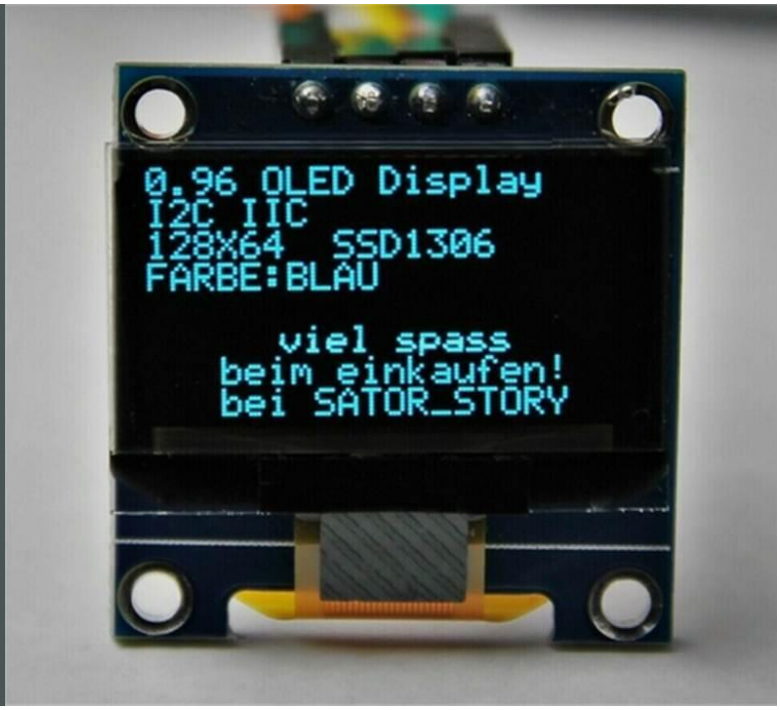
- Для реалізації аналізатора спектру обрано готовий модуль “Blue Pill” з мікроконтролером STM32F103C8T6 на базі ядра ARM Cortex-M3 (72 МГц, 20 КБ ОЗП, 64 КБ флеш). Модуль має широкий набір периферії (SPI, UART, USB, DMA), що дозволяє ефективно працювати з радіомодулем nRF24L01 і виводити дані на ПК. “Blue Pill” оснащений готовими контактами GPIO, стабільним живленням 3.3 В та сумісний із популярними середовищами розробки (STM32CubeIDE, Arduino IDE), що робить його оптимальним вибором для швидкого прототипування проекту.

БЕЗДРОТОВИЙ ІНТЕРФЕЙС NRF24L01

- Для сканування радіочастотного діапазону 2.4 ГГц обрано модуль nRF24L01, який має 126 каналів із кроком 1 МГц та внутрішні регістри для аналізу рівня сигналу. Завдяки низькому енергоспоживанню, компактним розмірам і підтримці багатьох платформ, він є оптимальним вибором для мобільних систем моніторингу спектру. Переваги модуля — швидке виявлення зайнятих частот, ширший частотний діапазон і висока швидкість сканування порівняно з Wi-Fi модулями.

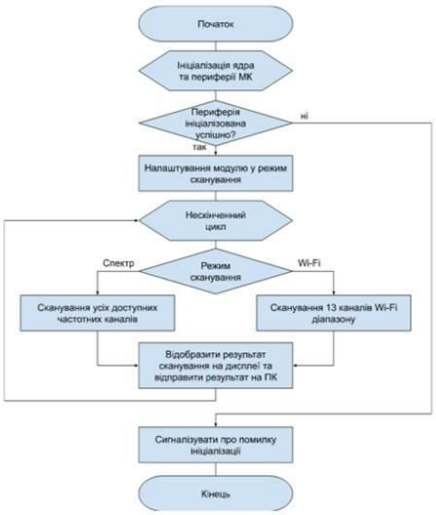
OLED-ДИСПЛЕЙ НА БАЗІ КОНТРОЛЕРА SSD1306

- Для відображення спектру радіочастот обрано монохромний OLED-дисплей на базі контролера SSD1306 з роздільною здатністю 128×64 пікселів. Він підтримує графічне та текстове відображення рівня сигналу для 126 каналів, максимальних значень і частотних позначок. OLED-дисплей має низьке енергоспоживання, компактні розміри та сумісний з інтерфейсами SPI і I2C, що робить його оптимальним вибором для проєкту.



АЛГОРИТМ ФУНКЦІОНУВАННЯ ПРИСТРОЮ

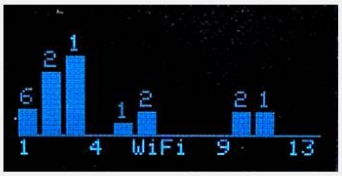
- Відповідно до документації радіомодуля було розроблено алгоритм роботи пристрою сканування спектру. Для ініціалізації необхідно налаштувати тактування мікроконтролера, інтерфейси, а також перевірити і ініціалізувати модулі дисплея та радіомодуля. Алгоритм роботи наведено на рисунку.



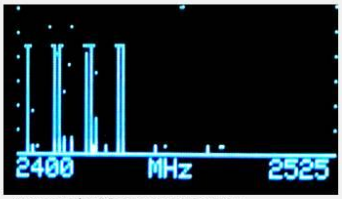
СТРУКТУРНО-ФУНКЦІОНАЛЬНА СХЕМА ПРИСТРОЮ

Система складається з функціональних блоків:
•**Блок керування** (STM32F103)– обробляє дані, керує модулями, відповідає за логіку роботи.
•**Модуль nRF24L01** – виконує прийом радіосигналу та вимірювання рівня на частотному каналі (SPI).
•**Дисплей SSD1306** – відображає інформацію у графічному вигляді (I2C).
•**Кнопка керування** – перемикає режими роботи, підключена до цифрового входу.
•**Інтерфейс ПК** – передає результати сканування через USB до комп'ютера для візуалізації.
•**Живлення** – 5 В від USB або зовнішнього блоку.
Після ввімкнення пристрій самотестується та розпочинає сканування. У разі помилки – інформує користувача через дисплей та ПК.

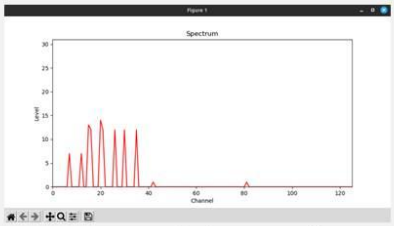
РЕЗУЛЬТАТИ РОБОТИ РОЗРОБЛЕНОГО СТЕНДУ



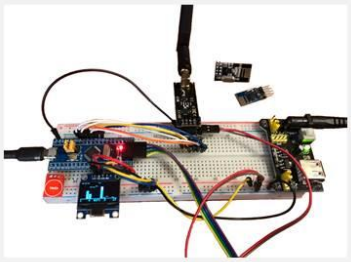
Режим відображення Wi-Fi каналів



Режим відображення спектру



Вигляд додатку для відображення прийнятих даних



Зовнішній вигляд розробленого макету приладу

ВИСНОВКИ

- В ході виконання кваліфікаційної роботи було виконана розробка пристрою для сканування радіочастотного спектру та пошуку прихованих бездротових мереж
- Було проведено огляд існуючих систем виявлення каналів передачі сигналу та моніторингу радіоспектру, проаналізовані переваги та недоліки існуючих засобів
- Було запропоновано структурно-функціональну схему пристрою та розроблена принципова електрична схема
- Були обрані програмні засоби для розробки проєкту та інструменти для програмування пристрою

ДОДАТОК Б

Розроблений програмний код проєкту на мові програмування C та Python.

Файл plotter.py:

```
import serial
import argparse
import time
import re
import matplotlib.pyplot as plt
import matplotlib.animation as animation

class SpectrumPlot:
  def __init__(self, comport, baudrate, ch_num):
    # open serial port
    self.ser = serial.Serial(comport, baudrate, timeout=None)
    # time.sleep(1)
    # self.ser.flushInput()
    # init plot
    self.levels = [0] * ch_num
    self.ch_num = ch_num

  # update plot
  def update(self, frameNum, line):
    try:
      if not self.ser.is_open: return line,
      data_lines = self.ser.readlines(8) # self.ch_num
      for data_str in data_lines:
        data = re.split(',|:', data_str.decode().strip()) # strip newline
characters.
        if (not data) or (data[0] != "ch"): continue
        # Update plot data
        ch = int(data[1])
        if (ch >= self.ch_num): ch = self.ch_num - 1
        level = int(data[2])
        self.levels[ch] = level
        line.set_data(range(self.ch_num), self.levels)
    except KeyboardInterrupt:
      print('exiting')
    return line,

  # clean up
  def close(self):
    # close serial
    self.ser.flush()
    self.ser.close()

def main():
  # create parser
  parser = argparse.ArgumentParser(description="Serial plotter")
  parser.add_argument('--port', dest='port', required=True)
  parser.add_argument('--baudrate', dest='baudrate', required=False,
default='115200')
  parser.add_argument('--ch_num', dest='ch_num', required=False,
default='126')
  args = parser.parse_args()
```

```
  port_str = args.port
  baudrate_str = args.baudrate
  ch_num_str = args.ch_num

  print('reading from serial port %s...' % port_str)
  # readserial(port_str, int(baudrate_str))

  # plot parameters
  spectrum = SpectrumPlot(port_str, int(baudrate_str), int(ch_num_str))

  # set up animation
  fig = plt.figure()
  ax = plt.axes(xlim=(0, int(ch_num_str) - 1), ylim=(0, 31))
  line, = ax.plot([], [], 'r-')
  anim = animation.FuncAnimation(fig, spectrum.update,
                                 fargs=(line,),
                                 interval=50)
  plt.xlabel('Channel')
  plt.ylabel('Level')
  plt.title('Spectrum')

  # show plot
  plt.show()

  # clean up
  spectrum.close()
  print('exiting.')

# call main
if __name__ == '__main__':
  main()
```

Файл main_app.c:

```
#include "main_app.h"
#include "main.h"
#include "nrf24.h"
#include "ssd1306.h"
#include "dwt_delay.h"
#include <stdio.h>
#include <stdint.h>
#include <stdbool.h>
#include <string.h>

#define USB_SERIAL_ENABLE
#include "serial_print.h"

#define SCAN_SAMPLES_NUM 128
#define SCAN_GAIN 8

#define CHART_WIDTH RF24_CHANNELS_MAX
#define CHART_HEIGHT (SSD1306_HEIGHT - 10)
#define CHART_OFFSET_X 1
#define CHART_OFFSET_Y 0
#define CHART_GRID_POINTS 6
#define CHART_BOTTOM_Y (CHART_OFFSET_Y + CHART_HEIGHT)
#define CHART_GRID_Y_STEP (CHART_HEIGHT / CHART_GRID_POINTS)

typedef enum {
  MODE_SPECTRUM,
  MODE_WIFI,
```

```
} device_mode_e;

static device_mode_e mode = MODE_SPECTRUM;
static bool need_grid_redraw = true;
static uint8_t spectrum[RF24_CHANNELS_MAX]; // channels levels
static uint8_t spectrum_peaks[RF24_CHANNELS_MAX]; // hold max peaks of signal

#define WIFI_CH_NUM 13
static const uint8_t wifi_ch[WIFI_CH_NUM] = {12, 17, 22, 27, 32, 37, 42, 47,
52, 57, 62, 67, 72};
static const uint8_t noiseAddress[RF24_PIPES_NUM][2] = {
  { 0x55, 0x55 }, { 0xAA, 0xAA }, { 0xA0, 0xAA }, { 0xAB, 0xAA }, { 0xAC,
0xAA }, { 0xAD, 0xAA }
};

void setup(void) {
  DWT_Init(); // Enable microseconds
  // I2C OLED
  ssd1306_Init();
  ssd1306_Fill(Black);
  // SPI NRF24L01
  LL_SPI_Enable(SPI1);
  if (!nrf24_init()) {
    ssd1306_FillRectangle(10, 10, 117, 45, White);
    char str[32];
    sprintf(str, "NRF24 hardware");
    ssd1306_SetCursor(15, 17);
    ssd1306_WriteString(str, Font_7x10, Black);
    sprintf(str, "not responding!");
    ssd1306_SetCursor(12, 29);
    ssd1306_WriteString(str, Font_7x10, Black);
    ssd1306_UpdateScreen();
    while (1);
  }
  // Setup for scanning mode
  nrf24_set_auto_ack(0); // disable acknowledgement
  nrf24_set_crc_length(NRF24_CRC_DISABLED); // accept any signal we find
  nrf24_set_address_width(2);
  for (uint8_t i = 0; i < RF24_PIPES_NUM; ++i) {
    nrf24_open_reading_pipe(i, noiseAddress[i], 2);
  }
  nrf24_set_data_rate(NRF24_DATARATE_1MBPS);
  // Get into standby mode
  nrf24_start_listening();
  nrf24_stop_listening();
  nrf24_flush_rx();
  reset_spectrum_peaks();
  update_mode();
}

void loop(void) {
  if (mode == MODE_SPECTRUM) {
    draw_spectrum();
    nrf24_scan_channels();
    print_spectrum();
  }
  else if (mode == MODE_WIFI) {
    draw_wifi();
    nrf24_scan_wifi();
  }
}

void set_spectrum(uint8_t ch, uint8_t level) {
```

```
  spectrum[ch] = level;
  if (level > spectrum_peaks[ch]) {
    spectrum_peaks[ch] = level;
  }
}

void reset_spectrum_peaks(void) {
  for (uint32_t i = 0; i < RF24_CHANNELS_MAX; i++) {
    spectrum_peaks[i] = 0;
  }
}

void print_spectrum(void) {
  char str[128];
  char *p_str = str;
  for (uint8_t i = 0; i < RF24_CHANNELS_MAX; i++) {
    p_str += sprintf(p_str, "ch:%u,%u\n", i, spectrum[i]);
    if (p_str - str >= 117) {
      p_str = str;
      PRINT_SERIAL(str);
    }
  }
  PRINT_SERIAL(str);
}

uint8_t calc_spectrum_chart_level(uint8_t val) {
  uint32_t level = ((uint32_t)val * CHART_HEIGHT * SCAN_GAIN) /
SCAN_SAMPLES_NUM;
  if (level > CHART_HEIGHT) level = CHART_HEIGHT;
  return level;
}

void draw_spectrum(void) {
  if (need_grid_redraw) {
    need_grid_redraw = false;
    reset_spectrum_peaks();
    ssd1306_Fill(Black);
    // draw grid scale
    uint8_t y = CHART_BOTTOM_Y;
    for (uint8_t cnt = 0; cnt < CHART_GRID_POINTS; cnt++) {
      y -= CHART_GRID_Y_STEP;
      ssd1306_DrawPixel(0, y, White);
      ssd1306_DrawPixel(SSD1306_WIDTH - 1, y, White);
    }
    ssd1306_Line(0, CHART_BOTTOM_Y, SSD1306_WIDTH - 1, CHART_BOTTOM_Y,
White);
    // draw labels
    char str[32];
    sprintf(str, "2400     MHz     2525");
    ssd1306_SetCursor(0, CHART_BOTTOM_Y + 2);
    ssd1306_WriteString(str, Font_6x8, White);
  } else {
    ssd1306_FillRectangle(
      CHART_OFFSET_X,
      CHART_OFFSET_Y,
      CHART_OFFSET_X + CHART_WIDTH - 1,
      CHART_OFFSET_Y + CHART_HEIGHT - 1,
      Black
    );
  }

  // draw levels
  for (uint32_t i = 0; i < RF24_CHANNELS_MAX; i++) {
```

```
    ssd1306_Line(
      CHART_OFFSET_X + i,
      CHART_BOTTOM_Y - calc_spectrum_chart_level(spectrum[i]),
      CHART_OFFSET_X + i,
      CHART_BOTTOM_Y,
      White
    );
    uint8_t peak_pos = CHART_BOTTOM_Y -
calc_spectrum_chart_level(spectrum_peaks[i]);
    ssd1306_DrawPixel(CHART_OFFSET_X + i, peak_pos, White);
  }

  ssd1306_UpdateScreen();
}

void draw_spectrum_ch(uint8_t ch) {
  ssd1306_Line(
    CHART_OFFSET_X + ch,
    CHART_OFFSET_Y,
    CHART_OFFSET_X + ch,
    CHART_BOTTOM_Y,
    Black
  );
  ssd1306_Line(
    CHART_OFFSET_X + ch,
    CHART_BOTTOM_Y - calc_spectrum_chart_level(spectrum[ch]),
    CHART_OFFSET_X + ch,
    CHART_BOTTOM_Y,
    White
  );
  uint8_t peak_pos = CHART_BOTTOM_Y -
calc_spectrum_chart_level(spectrum_peaks[ch]);
  ssd1306_DrawPixel(CHART_OFFSET_X + ch, peak_pos, White);
  ssd1306_DrawPixel(((ch + 1) % RF24_CHANNELS_MAX) + CHART_OFFSET_X,
CHART_OFFSET_Y, White);
  ssd1306_UpdateScreen();
}

void draw_wifi(void) {
  if (need_grid_redraw) {
    need_grid_redraw = false;
    reset_spectrum_peaks();
    ssd1306_Fill(Black);
    // draw grid scale
    ssd1306_Line(0, CHART_BOTTOM_Y, SSD1306_WIDTH - 1, CHART_BOTTOM_Y,
White);
    // draw labels
    char str[32];
    sprintf(str, "1    4  WiFi  9    13");
    ssd1306_SetCursor(0, CHART_BOTTOM_Y + 2);
    ssd1306_WriteString(str, Font_6x8, White);
  } else {
    ssd1306_FillRectangle(
      0,
      CHART_OFFSET_Y,
      SSD1306_WIDTH,
      CHART_OFFSET_Y + CHART_HEIGHT - 1,
      Black
    );
  }

  // draw levels
  for (uint8_t i = 0; i < WIFI_CH_NUM; i++) {
```

```
    uint8_t ch = wifi_ch[i];
    ssd1306_FillRectangle(
      i * 10,
      CHART_BOTTOM_Y - calc_spectrum_chart_level(spectrum[ch]),
      i * 10 + 7,
      CHART_BOTTOM_Y,
      White
    );
    uint8_t peak_pos = CHART_BOTTOM_Y -
calc_spectrum_chart_level(spectrum_peaks[ch]);
    ssd1306_Line(i * 10, peak_pos, i * 10 + 7, peak_pos, White);
  }
  ssd1306_UpdateScreen();
}

void update_mode(void) {
  if (mode == MODE_SPECTRUM) {
    draw_spectrum();
  }
  else if (mode == MODE_WIFI) {
    draw_wifi();
  }
}

void nrf24_scan_channels(void)
{ // Scanning all channels in the 2.4GHz band (2400 - 2525 MHz)
  nrf24_rf_disable();
  DWT_Delay(2);
  for (uint8_t ch = 0; ch < RF24_CHANNELS_MAX; ch++) {
    if (mode != MODE_SPECTRUM) {
      update_mode();
      return;
    }
    set_spectrum(ch, nrf24_get_channel_level(ch, SCAN_SAMPLES_NUM));
    draw_spectrum_ch(ch);
  }
}

void nrf24_scan_wifi(void)
{ // Scanning 2.4GHz WiFi bands
  nrf24_rf_disable();
  DWT_Delay(2);
  for (uint8_t wch = 0; wch < WIFI_CH_NUM; wch++) {
    if (mode != MODE_WIFI) {
      update_mode();
      return;
    }
    uint8_t ch = wifi_ch[wch];
    set_spectrum(ch, nrf24_get_channel_level(ch, SCAN_SAMPLES_NUM));
  }
}

void nrf24_spi_begin_transfer(void) {
  // reset NRF24_CSN pin to '0'
  LL_GPIO_ResetOutputPin(NRF24_CSN_GPIO_Port, NRF24_CSN_Pin);
  DWT_Delay(0);
}

void nrf24_spi_end_transfer(void) {
  // set NRF24_CSN pin to '1'
  DWT_Delay(0);
  LL_GPIO_SetOutputPin(NRF24_CSN_GPIO_Port, NRF24_CSN_Pin);
}
```

```
uint8_t nrf24_spi_transfer(uint8_t data) {
  // transmit and receive one byte via SPI
  while (!LL_SPI_IsActiveFlag_TXE(SPI1)) {;}
  LL_SPI_TransmitData8(SPI1, data);
  // Wait until the transmission is complete
  //while (LL_SPI_IsActiveFlag_BSY(SPI1)) {;}
  while (!LL_SPI_IsActiveFlag_RXNE(SPI1)) {;}
  return LL_SPI_ReceiveData8(SPI1);
}

void nrf24_rf_enable(void) {
  // Enable RX and TX
  // Set NRF24_CE pin to '1'
  LL_GPIO_SetOutputPin(NRF24_CE_GPIO_Port, NRF24_CE_Pin);
}

void nrf24_rf_disable(void) {
  // Disable RX and TX
  // Reset NRF24_CE pin to '0'
  LL_GPIO_ResetOutputPin(NRF24_CE_GPIO_Port, NRF24_CE_Pin);
}

void EXTI_13_Callback(void) {
  mode = (mode == MODE_SPECTRUM) ? MODE_WIFI : MODE_SPECTRUM;
  need_grid_redraw = true;
}
```

Відомість кваліфікаційної роботи

«Сканер прихованих бездротових мереж в діапазоні 2.4 ГГц»

	Прізвище та ініціали відповідальної особи	Підпис	Дата
Роботу виконав студент групи КІУКІ-21-9 Структура кваліфікаційної роботи: – пояснювальна записка 49 с.; – графічний матеріал _13_ арк..	Сасько А.О.		10.06.2025
Керівник роботи	Шевченко О.Ю.		10.06.2025
Перевірка на антиплагіат здійснено, відповідальна особа	Литвинова Є. І.		06.06.2025
Нормоконтроль проведено:	Шевченко О.Ю.		10.06.2025