МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Чорноморський національний університет

імені Петра Могили

Факультет комп’ютерних наук

Кафедра комп'ютерної інженерії

ДОПУЩЕНО ДО ЗАХИСТУ

Завідувач кафедри,

д-р техн. наук, проф.

_____ І. М. Журавська

« __ » _____ 2024 р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

Апаратно-програмний комплекс для координації дій на полі бою за допомогою коротких текстових повідомлень

Спеціальність 123 Комп’ютерна інженерія

123 – КБР.01 – 405.22010602

Студент _____ Д. О. Голубев

підпис

«__» _____ 202__ р.

Керівник ст. викладач _____ В. В. Старченко

підпис

«__» _____ 202__ р.

Миколаїв – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет імені Петра Могили
Факультет комп'ютерних наук
Кафедра комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Зав. кафедри _____ І. М. Журавська

«_____» _____ 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної бакалаврської роботи

Видано студенту групи 405 факультету комп'ютерних наук

Голубев Денис Олександрович

(прізвище, ім'я, по батькові студента)

1. Тема кваліфікаційної роботи
Апаратно-програмний комплекс для координації дій на полі бою за допомогою коротких текстових повідомлень

Затверджена наказом по ЧНУ ім. Петра Могили від 30.01.2024 № 17.

2. Строк представлення кваліфікаційної роботи «____» _____ 20__ р.

3. Очікуваний результат роботи та початкові дані, якщо такі потрібні
Створення апаратно-програмного комплексу для координації дій військових на полі бою за допомогою коротких текстових повідомлень, який забезпечить швидкий, надійний та безпечний обмін інформацією між підрозділами, навіть в умовах обмежених ресурсів та дії засобів радіоелектронної боротьби. Комплекс має бути простим в експлуатації, енергоефективним та інтегрованим з іншими системами координації.

4. Перелік питань, що підлягають розробці
Провести аналіз існуючих систем координації дій військових на полі бою; розробити архітектуру та функціональні вимоги до комплексу; проектування апаратної частини та розробити програмне забезпечення.

5. Перелік графічних матеріалів

Зображення STM32, дисплею, модуля зв’язку LoRa, клавіатури, GPS модуля.
Зображення блок-схеми роботи ПЗ.
Зображення макетної схеми, принципової електричної схеми.

6. Завдання до спеціальної частини

Проаналізувати та розробити рекомендації з охорони праці при створенні і експлуатації апаратно-програмного комплексу для координації дій на полі бою за допомогою коротких текстових повідомлень. Робота включає аналіз потенційних небезпек, організацію безпечних умов праці, заходи захисту при роботі з електронними компонентами, пожежну безпеку, медичні аспекти та ергономіку, а також психологічний клімат і стресостійкість.

7. Консультанти:

Консультант	Кафедра (організація)	Частина роботи
ст. викладач О. В. Макарова	кафедра екології Медичного інституту ЧНУ ім. Петра Могили	Спеціальна частина з охорони праці

Керівник роботи

Ст. викладач Старченко В'ячеслав Володимирович

(посада, прізвище, ім’я, по батькові)

_____

(підпис)

Завдання прийнято до виконання

Голубев Денис Олександрович

(прізвище, ім’я, по батькові студента)

_____

(підпис)

Дата видачі завдання «____» _____ 20_____ р.

КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

Тема: Апаратно-програмний комплекс для координації дій на полі бою за допомогою коротких текстових повідомлень

№	Найменування роботи	Початок	Закінчення	Примітки
1	Розробка та затвердження завдання на виконання КР	05.02.2024	08.02.2024	Виконано
2	Огляд літератури за темою роботи	09.02.2024	12.03.2024	Виконано
3	Складання календарного плану КБР	26.02.2024	06.03.2024	Виконано
4	Аналіз предметної області	09.03.2024	15.03.2024	Виконано
5	Розробка проєктних рішень	15.03.2024	25.03.2024	Виконано
6	Вибір апаратної платформи	16.03.2024	27.03.2024	Виконано
7	Налаштування АПЗ	01.04.2024	07.04.2024	Виконано
8	Проведення досліджень	07.04.2024	10.05.2024	Виконано
9	Оформлення КРБ та презентації	18.04.2024	29.05.2024	Виконано
10	Перший передзахист	29.05.2024	29.05.2024	Виконано
11	Другий передзахист	06.06.2024	06.06.2024	Виконано
12	Рецензування	29.06.2024	05.06.2024	Виконано
13	Відгук керівника КР	10.06.2024	14.06.2024	Виконано
14	Завершення оформлення КР та презентації	06.06.2024	14.06.2024	Виконано
15	Захист кваліфікаційної роботи	26.06.2024	26.06.2024	Виконано

Розробив здобувач ВО Голубев Денис Олександрович _____

(прізвище, ім'я, по батькові) *(підпис)*

«____» _____ 2024 р.

Керівник роботи

Ст. викладач Старченко В'ячеслав Володимирович _____

(посада, прізвище, ім'я, по батькові) *(підпис)*

«____» _____ 2024 р.

АНОТАЦІЯ

до кваліфікаційної бакалаврської роботи
«Апаратно-програмний комплекс для координації дій на полі бою за допомогою коротких текстових повідомлень»
Студент 405 гр.: Голубев Денис Олександрович
Керівник: ст. викладач Старченко В'ячеслав Володимирович

Сучасні військові операції характеризуються високою динамічністю та залежністю від оперативного та надійного зв'язку. Традиційні системи військового зв'язку, такі як радіо, супутниковий зв'язок та IP-телефонія, мають ряд суттєвих недоліків, зокрема вразливість до радіоелектронної боротьби, обмежену пропускну здатність та недостатній рівень безпеки.

Метою роботи є розробка прототипу апаратно-програмного комплексу для координації дій військових на полі бою з використанням коротких текстових повідомлень, що забезпечить підвищення ефективності та безпеки обміну інформацією в умовах сучасних військових операцій.

Для досягнення мети виконано такі завдання:

1) проведено аналіз існуючих систем координації дій військових на полі бою, включаючи огляд традиційних систем зв'язку, аналіз загроз інформаційній безпеці в умовах війни та обґрунтування необхідності розробки нового комплексу;

2) розроблено архітектуру та функціональні вимоги до комплексу, враховуючи специфіку військових операцій та необхідність забезпечення своєчасності, надійності, конфіденційності та скритності зв'язку;

3) здійснено проектування апаратної частини комплексу, включаючи вибір мікроконтролера та периферійних модулів (LoRa, GPS, дисплей, клавіатура).

Розроблено програмне забезпечення комплексу, включаючи модулі передачі та прийому текстових повідомлень, модуль шифрування та дешифрування за допомогою бібліотеки mbedTLS та інтерфейс користувача.

Методами дослідження є аналіз, синтез, проєктування, алгоритмізація, програмне кодування, моделювання та тестування.

В цілому, бакалаврська робота містить 78 сторінку (без додатків), 37 рисунки, 9 таблиць, 30 джерел посилання.

Ключові слова: *військовий зв'язок, інтерфейс користувача, координація дій, короткі текстові повідомлення, шифрування, GPS, LoRa,, mbedTLS, STM32.*

ABSTRACT

of the Bachelor’s Thesis

"A hardware and software system for coordinating actions on the battlefield via short text messages "

Student: Golubev Denis Aleksandrovich

Supervisor: senior teacher Starchenko Vyacheslav

Modern military operations are characterized by high dynamism and dependence on rapid and reliable communications. Traditional military communication systems, such as radio, satellite communications, and IP telephony, have a number of significant drawbacks, including vulnerability to electronic warfare, limited bandwidth, and insufficient security.

The aim of this work is to develop a prototype hardware and software system for coordinating military actions on the battlefield using short text messages, which will increase the efficiency and security of information exchange in modern military operations.

To achieve this goal, the following tasks were performed:

1) analysis of existing systems for coordinating military actions on the battlefield, including a review of traditional communication systems, analysis of threats to information security in warfare, and justification for the need to develop a new complex;

2) architecture and functional requirements for the complex were developed, taking into account the specifics of military operations and the need to ensure timeliness, reliability, confidentiality and secrecy of communication;

3) designing the hardware of the complex, including the selection of a microcontroller and peripheral modules (LoRa, GPS, display, keyboard).

The software of the complex was developed, including modules for transmitting and receiving text messages, an encryption and decryption module using the mbedTLS library, and a user interface.

The research methods are analysis, synthesis, design, algorithmization, program coding, modeling, and testing.

In total, the bachelor's thesis contains 78 pages (without appendices), 37 figures, 9 tables, and 30 references.

Keywords: *military communications, user interface, coordination, short text messages, encryption, GPS, LoRa, mbedTLS, STM32.*

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АУВ – автоматизоване управління військами

ГШ – генеральний штаб

ПУВ – приховані управління військами

РЕБ – радіоелектронна боротьба

РЕЗ – радіоелектронний захист

МК – мікроконтролер

ШІМ – широтно-імпульносної модуляції

TFT – Thin-Film Transistor

GPIO – General Purpose Input/Output

LoRa – Long Range

AES – Advanced Encryption Standard

SPI – Serial Peripheral Interface

HAL – Hardware Abstraction Layer

ВСТУП

Сучасна війна, яка характеризується швидкими змінами та високим рівнем інформаційних технологій, висуває нові вимоги до систем координації дій військових на полі бою. Ефективність бойових операцій залежить від швидкості та надійності обміну інформацією між підрозділами, а також від спроможності протистояти загрозам інформаційній безпеці. Традиційні системи військового зв'язку, засновані на радіопередачі, все частіше виявляються неефективними в умовах активної радіоелектронної боротьби (РЕБ), а також обмежені обсягом переданих даних та не завжди забезпечують необхідний рівень конфіденційності [1].

З іншого боку, сучасні технології бездротового зв'язку, зокрема, передача коротких текстових повідомлень, мають величезний потенціал для використання в військовій сфері. Цей вид зв'язку характеризується простотою використання, високою швидкістю передачі, низьким енергоспоживанням та можливістю передавати інформацію на відносно невеликі відстані.

Однак, безпосереднє використання стандартних технологій текстових повідомлень для військових цілей неможливе, оскільки вони не відповідають ряду вимог, що висуваються до систем зв'язку в умовах бойових дій. Зокрема, стандартні протоколи передачі текстових повідомлень не забезпечують достатнього рівня захисту від перехоплення та фальсифікації, а також не враховують обмежені ресурси, доступні військовим у польових умовах.

Саме тому виникає потреба у розробці спеціального апаратно-програмного комплексу, призначеного для координації дій військових на полі бою за допомогою коротких текстових повідомлень. Цей комплекс повинен забезпечувати високу надійність передачі та прийому повідомлень навіть в умовах перешкод та радіоелектронної боротьби, захищати передані текстові повідомлення від перехоплення та фальсифікації за допомогою сучасних методів шифрування, забезпечувати швидку передачу та обробку інформації, мати простий та інтуїтивно зрозумілий інтерфейс для використання

військовими незалежно від їхньої підготовки, бути компактним, мати низьке енергоспоживання та працювати на доступних батареях, і, нарешті, інтегруватися з іншими системами координації дій, навігації та управління для створення комплексного рішення для управління бойовими діями .

Наявність такого комплексу дозволить вирішити низку актуальних проблем, що виникають в сучасних військових операціях:

– збільшити швидкість та ефективність обміну інформацією, що дозволить оперативно координувати дії підрозділів, оперативно передавати важливі розвідувальні дані та швидко реагувати на зміни ситуації на полі бою;

– збільшити рівень інформаційної безпеки, забезпечивши високий рівень захисту від перехоплення та фальсифікації переданої інформації, що дозволить запобігти зливці цінних даних та дезінформації;

– збільшити мобільність та автономність військових підрозділів, забезпечивши можливість використовувати комплекс на різних типах бойової техніки та легко переносити військовими;

– створити єдину систему управління бойовими діями, інтегруючи комплекс з іншими системами координації дій та управління, що дозволить створити єдину платформу для збору, обробки та передачі інформації, що значно підвищить ефективність управління військовими операціями.

Таким чином, розробка апаратно-програмного комплексу є надзвичайно актуальною науковою та практичною задачею. Результати цієї роботи дозволять створити сучасну систему зв'язку, яка підвищить ефективність бойових дій та забезпечить необхідний рівень інформаційної безпеки в сучасних умовах.

Мета роботи: розробка прототипу апаратно-програмного комплексу для координації дій військових на полі бою за допомогою коротких текстових повідомлень.

Об'єкт дослідження: засоби забезпечення надійності та конфіденційності обміну короткими текстовими повідомленнями в умовах обмежених ресурсів та дії засобів радіоелектронної протидії.

Предмет дослідження: апаратно-програмний комплекс для координації дій військових на полі бою за допомогою коротких текстових повідомлень.

Для досягнення поставленої мети необхідно вирішити такі **завдання:**

– провести аналіз існуючих систем координації дій військових на полі бою, їхніх переваг та недоліків, особливо в контексті сучасних загроз інформаційній безпеці;

– розробити архітектуру та функціональні вимоги до нового комплексу, враховуючи потреби військових, особливості бойових дій та сучасні технології;

– спроектувати апаратну частину комплексу, що включає в себе портативний пристрій для передачі та прийому текстових повідомлень, а також локальну навігацію.

– розробити програмне забезпечення комплексу з використанням сучасних технологій та підходів до програмування, забезпечуючи передачу та прийом текстових повідомлень, обмін даними з іншими пристроями та високий рівень захисту даних.

Практичне значення роботи: розробка прототипу комплексу, який може бути використаний для створення ефективної системи зв'язку для військових, що підвищить їхню ефективність та інформаційну безпеку.

Наукова новизна: полягає в розробці нового апаратно-програмного комплексу, спеціально розрахованого на використання коротких текстових повідомлень для координації дій військових на полі бою, з урахуванням потреб сучасної війни та специфіки загроз інформаційній безпеці.

1 АНАЛІЗ ІСНУЮЧИХ СИСТЕМ КООРДИНАЦІЇ ДІЙ ВІЙСЬКОВИХ НА ПОЛІ БОЮ

1.1 Огляд традиційних систем зв'язку та їх недоліки в сучасних умовах

У сучасному світі, де військові операції все частіше ведуться у складних і динамічних умовах, координація дій є ключовим фактором успіху. Для забезпечення ефективного управління та обміну інформацією, використовуються різноманітні системи зв’язку.

Існує три основні типи традиційних систем зв'язку: радіо зв'язок; супутниковий зв'язок та IP-телефонія.

Радіо зв'язок, найпоширеніший у військовій сфері, відзначається простотою використання, доступністю та мобільністю. Однак він має низку недоліків, таких як: низька стійкість до завад та РЕБ, що ускладнює надійний зв'язок у сучасних умовах, обмежений обсяг переданих даних, що робить його неефективним для передачі великих обсягів інформації, та можливість перехоплення сигналів, що ставить під загрозу конфіденційність переданої інформації.

Супутниковий зв'язок забезпечує глобальне покриття та високу пропускну здатність, що робить його цінним для координації дій на великих територіях. Проте, супутниковий зв'язок відзначається високою вартістю обладнання та послуг, можливістю перехоплення сигналів з боку противника, що ставить під загрозу конфіденційність переданої інформації, та залежністю від супутників, що може стати проблемою в умовах бойових дій, коли можливі атаки на супутникові системи.

IP-телефонія, заснована на Інтернет-протоколі, надає можливість здійснювати голосові та відео дзвінки, обмінюватись текстовими повідомленнями та передавати дані через мережу Інтернет. Однак, IP-телефонія не завжди надійна в умовах бойових дій: Залежність від наявності

стабільної та надійної мережі Інтернет, що може бути проблемою в умовах обмеженої інфраструктури та можливих обстрілів мережевих вузлів, та можливість перехоплення трафіку з боку противника, що ставить під загрозу конфіденційність переданої інформації.

Однак, військовий зв'язок (відповідно до Військового стандарту 01.112.001–2006 [2]) класифікується за видами та способами зв'язку, та поділяється на телефонний, відеотелефонний, документальний, фельд’єгерсько-поштовий та сигнальний. Однак, документальний ще включає в себе такі типи, як: телеграфний; факсимільний; передавання даних (рис. 1.1).

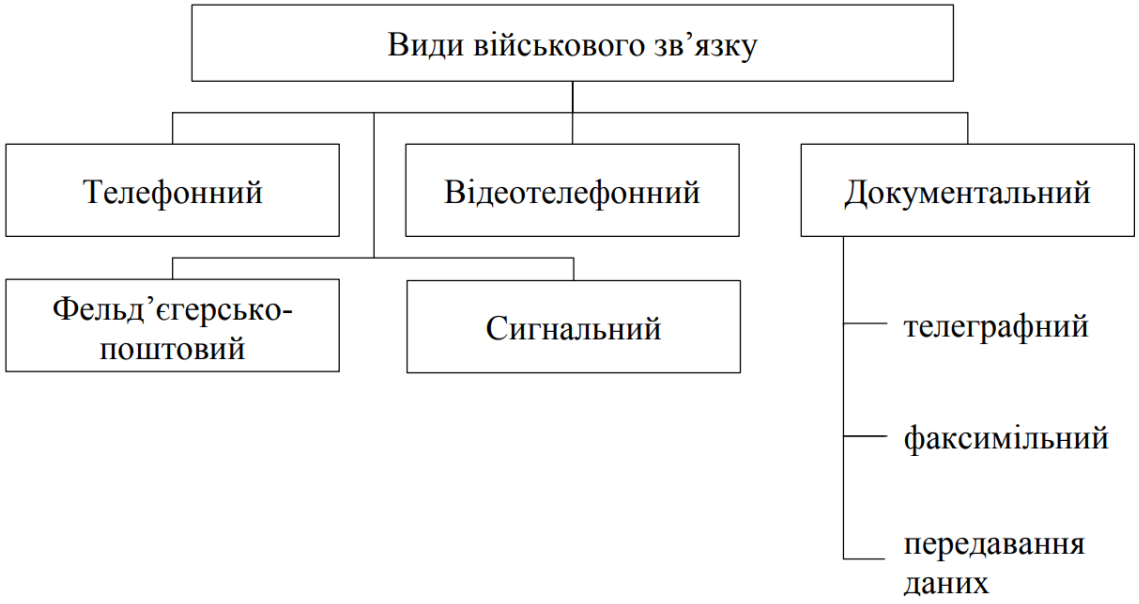


Рисунок 1.1 – Види військового зв’язку

Телефонний зв’язок є одним з основних засобів комунікації у військових умовах. Він забезпечує обмін мовною інформацією, передаючи звукові хвилі, перетворені на електричні сигнали, через мережу телефонних ліній, супутників або радіоканалів. Телефонний зв’язок дозволяє швидко та ефективно передавати голосові команди та інструкції між підрозділами, що є критично важливим у бойових умовах.

Прикладом такої система є «Secure Mobile Anti-jam Reliable Tactical Terminal» (SMART-T). SMART-T забезпечує захищений супутниковий зв'язок

для військових підрозділів, що дозволяє підтримувати телефонні з'єднання навіть у складних умовах бойових дій.

Інший приклад – використання військових варіантів стільникових телефонів, таких як AN/PRC-117G, які забезпечують захищений голосовий зв’язок (рис. 1.2).

Рисунок 1.2 – Стільниковий радіостанція AN/PRC-117G

Даного зв’язку, головною перевагою є – простота використання, високу надійність та можливість швидкої передачі інформації.

Проте цей тип зв’язку має суттєві недоліки в контексті бойових дій. Наприклад, телефонний зв’язок може бути неефективним через можливість перехоплення сигналу, обмежену дальність дії та складність використання в умовах сильних перешкод або відсутності сигналу. Крім того, телефонний зв'язок часто потребує встановлення додаткового обладнання, такого як ретранслятори або антени, що може бути складним і затратним у бойових умовах. Це особливо актуально у випадках мобільних операцій, де підрозділи часто змінюють своє місцезнаходження.

Відеотелефонний зв’язок, або мультимедійний зв’язок, забезпечує одночасно обмін мовною інформацією та рухомими і нерухомими зображеннями, використовуючи технології цифрової обробки сигналу і

передачі даних. Цей тип зв’язку дозволяє командувачам отримувати більш повну картину бойової ситуації, що сприяє більш ефективній координації дій.

Прикладом сучасної системи відеотелефонного зв’язку є система VTC (Video Teleconferencing) використовується багатьма арміями світу для забезпечення оперативного зв'язку між командними пунктами. Наприклад, системи Polycom RealPresence (рис. 1.3) чи Cisco TelePresence дозволяють проводити відеоконференції з високою якістю зображення та звуку, забезпечуючи реалістичне відтворення обстановки на полі бою.

Рисунок 1.3 – Стільниковий радіостанція AN/PRC-117G

Незважаючи на свій потенціал, відеотелефонний зв'язок має деякі суттєві недоліки. По-перше, високий рівень енергоспоживання обмежує його використання в умовах відсутності надійного джерела живлення. По-друге, можливість перехоплення сигналу залишається значною загрозою, особливо при використанні незахищених каналів.

Також, ця система може бути неефективною у зонах з слабким або відсутнім сигналом, що обмежує його застосування в польових умовах, що вимагає значної пропускної здатності каналів зв'язку. Це також підвищує вимоги до обробки і зберігання даних, що потребує додаткових технічних рішень.

Документальний зв’язок є типом електрозв’язку, який дозволяє обмінюватися документальними повідомленнями, передаючи через мережу текстові документи, таблиці, графіки, презентації та інші типи цифрової інформації. Він використовує кілька протоколів передачі даних, що дозволяє надсилати та отримувати файли будь-якого розміру, забезпечуючи швидкий і надійний обмін даними між різними користувачами та пристроями.

Телеграфний зв’язок використовує електричні сигнали, що передаються по проводах або радіоканалах для обміну інформацією у вигляді літерних чи цифрових повідомлень. Код «Морзе» використовується для цього типу зв’язку для перетворення літер, цифр і знаків пунктуації в послідовність коротких і довгих сигналів, які передаються по телеграфному апарату. У 1800-х і 1900-х роках телеграфний зв’язок був першим типом електрозв’язку, який дозволяв передавати інформацію на великі відстані та відіграв значну роль у розвитку суспільства та комунікацій.

Телеграфний зв'язок має свої переваги, включаючи надійність і можливість передачі повідомлень на великі відстані з використанням мінімального обладнання. Проте, його основні недоліки включають обмежену швидкість передачі даних і складність у використанні для передачі складних повідомлень або великих обсягів даних. У сучасних умовах телеграфний зв'язок значною мірою витіснено більш сучасними методами комунікації, але все ще може використовуватися як резервний засіб зв'язку в умовах, коли інші методи недоступні.

Факсимільний зв’язок дозволяє обмінюватися інформацією у вигляді графічних елементів, таких як малюнки, таблиці, графіки, карти та фотографії, а також текстових повідомлень, шляхом перетворення цих елементів у аналоговий сигнал, який передається по телефонних лініях або радіоканалах. Однак, факсимільний зв'язок може бути недостатньо ефективним під час координації дій на полі бою. У швидкоплинних боях передача графічних матеріалів може зайняти багато часу, що є вкрай важливим. Також він не може

передавати великі файли, такі як аерофотознімки, карти або плани операцій, та вимагає спеціального обладнання, яке може бути громіздким і незручним в умовах бойових дій.

Прикладом сучасного використання факсимільного зв’язку є його застосування в деяких військових установах для передачі важливих документів та графічних матеріалів. Наприклад, армії можуть використовувати захищені факсимільні апарати, такі як Panasonic UF-9000, для обміну графічною інформацією між командними пунктами (рис. 1.4).

Рисунок 1.4 – Факсимільний апарат Panasonic UF-9000

Факсимільний зв'язок має певні переваги, такі як можливість передачі точних копій документів та інших графічних матеріалів без спотворення. Проте, його недоліки, включаючи відносно низьку швидкість передачі і обмежену пропускну здатність, роблять його менш придатним для використання в умовах високої інтенсивності бойових дій. Крім того, вимога до спеціального обладнання і залежність від наявності телефонних ліній або радіоканалів обмежують можливості його застосування в польових умовах.

Передавання даних є важливим типом зв’язку в контексті координації дій на полі бою, оскільки це забезпечує ефективне управління військами та

виконання бойових завдань. Передавання даних дозволяє передавати інформацію у формі, яка може бути автоматизована обчислювальними технологіями.

Передавання даних забезпечує високий рівень точності та швидкості обміну інформацією, що є критично важливим у бойових умовах. Проте цей тип зв'язку потребує наявності відповідного обладнання та програмного забезпечення, що може бути складним у польових умовах. Крім того, передавання даних вимагає наявності стабільного джерела живлення і може бути вразливим до кібератак і електронних засобів боротьби, таких як глушіння сигналу.

Фельд’єгерсько-поштовий зв’язок призначений для забезпечення управління військами шляхом доставки рухомих засобів штабам об’єднань, з’єднань, військових частин (кораблів), установам, військовим навчальним закладам, підприємствам та організаціям, а також для створення постійного поштового і телеграфного зв’язку особового складу. Цей вид зв’язку є важливим для передачі секретної інформації, документів та інших важливих матеріалів, які потребують високого рівня захисту.

Основною перевагою фельд’єгерсько-поштового зв’язку є його незалежність від електронних засобів комунікації, що робить його менш вразливим до кібератак та електронного шпигунства. Проте цей вид зв’язку має певні недоліки, такі як низька швидкість передачі інформації та залежність від фізичних засобів транспортування, що може бути проблематичним в умовах активних бойових дій. Крім того, фельд’єгерсько-поштовий зв’язок потребує значної кількості людських ресурсів для забезпечення доставки повідомлень, що може збільшити ризик затримок або втрат інформації в умовах бойових дій. Використання цього виду зв'язку також може вимагати додаткових заходів безпеки для захисту фізичних носіїв інформації від захоплення або знищення.

Сигнальний зв'язок - це система передачі інформації за допомогою узгоджених сигналів, прапорців, вогнів, сирен, піротехнічних засобів та інших засобів. Він використовується для передачі простих команд та інформації у випадках, коли інші засоби зв’язку недоступні або неефективні. Основні переваги сигнального зв’язку включають простоту використання та незалежність від електронних засобів комунікації.

Однак, має багато недоліків, пов'язаних із неправильним тлумаченням сигналів, що може статися через перешкоди або візуальні обмеження, а також через погодні умови, які впливають на видимість і освітлення для ефективного передавання сигналів. Крім того, сигнальний зв’язок не може передавати складні або вичерпні повідомлення, що обмежує його застосування у складних бойових умовах. Іншою проблемою є те, що сигнальний зв'язок легко може бути помічений і перехоплений противником, що підвищує ризик розкриття бойових планів. Також, цей вид зв'язку обмежений у дальності передачі сигналів і потребує наявності прямої видимості між відправником і отримувачем, що не завжди можливо в умовах складного рельєфу або забудови.

Не менш важливим є поняття рід військового зв’язку що визначається середовищем розповсюдження сигналів електрозв’язку і каналоутворюючими засобами зв’язку (рис. 1.5).

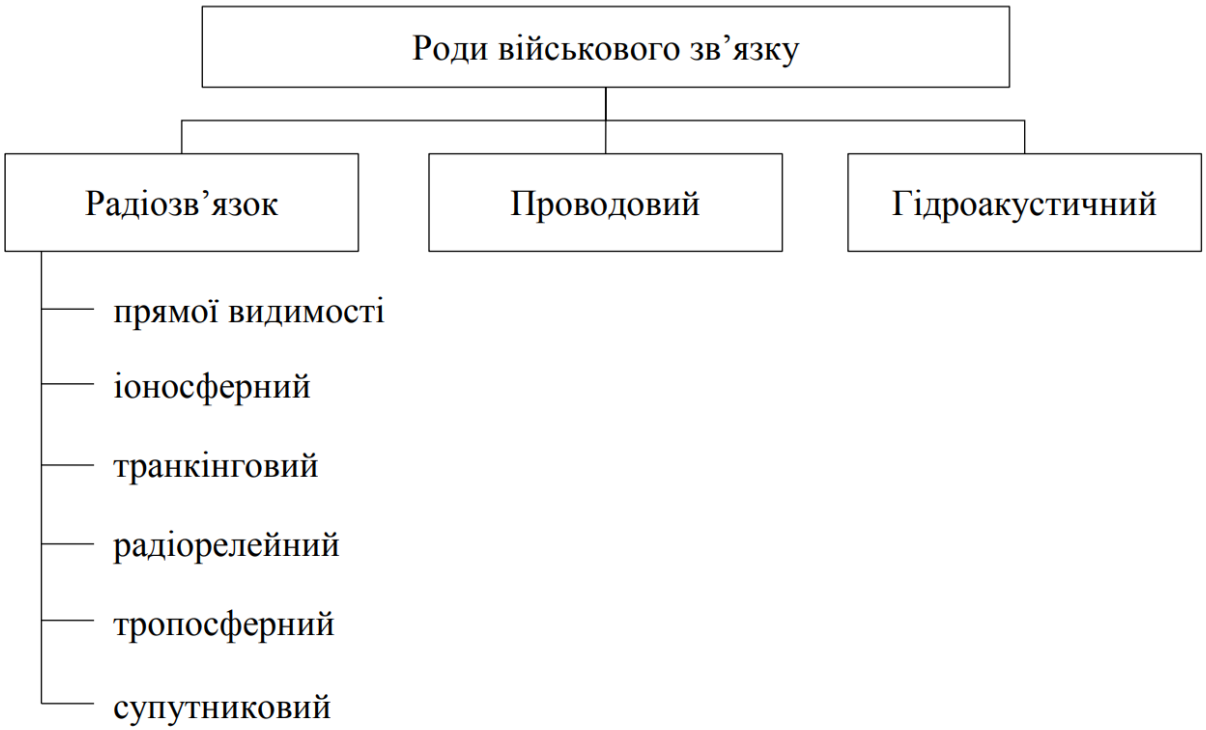


Рисунок 1.5 – Схематичне зображення роду зв’язку

Радіозв’язок – електрозв’язок, що здійснюється з використанням радіохвиль. Він включає в себе зв'язок ***прямої видимості***, який забезпечує передачу сигналу радіостанцією у межах прямої видимості. Так званий ***іоносферний*** зв’язок, який діє за принципом передачі радіохвиль між радіостанціями які відбиваються від іоносфери або розсіюється на неоднорідностях іоносфери. За схожим принципом працює ***тропосферний*** зв’язок який відбувається за рахунок відбиття та розсіювання радіохвиль між станціями поза межами прямої видимості на неоднорідностях тропосфери.

Радіозв’язок також включає ***транкінговий*** зв’язок, коли мобільні абоненти можуть спілкуватися один з одним через обмежену кількість базових приймально-передавальних станцій або безпосередньо між ними. Цей зв’язок використовує частотний, часовий, частотно-часовий або кодовий розподіл радіоканалів між абонентами в межах зони радіо доступу.

До категорії радіозв’язку входить і ***радіорелейний*** зв’язок який створюється шляхом багаторазової ретрансляції радіосигналів через ланцюг радіорелейних станцій.

Супутниковий зв’язок теж належить до категорії радіозв’язку, який здійснюється між земними станціями за допомогою супутникового ретранслятора, що ретранслює радіосигнал.

Також до роду військового зв’язку відносяться ***проводовий*** та ***гідроакустичний*** зв'язок.

Проводовий зв’язок - це тип електрозв’язку, при якому сигнали електрозв’язку розміщуються вздовж проводового кабелю з металевими або волоконно-оптичними жилами.

А ось гідроакустичні зв’язки відбуваються, коли звукові чи ультразвукові хвилі передаються у воді.

1.2 Аналіз загроз інформаційній безпеці в умовах війни

Однак слід пам’ятати, що сучасна війна все більше перетворюється на інформаційну війну, де перемога залежить не тільки від фізичної сили, але й від здатності контролювати інформаційний простір, захищати власні дані та використовувати інформацію противника для отримання переваги.

Інформаційна безпека стає критичним фактором для успішного ведення бойових дій, а загрози в інформаційній сфері, одна з найнебезпечніших[3-5].

1.2.1 Радіоелектронна боротьба (РЕБ) та методи перехоплення сигналів

Радіоелектронна боротьба (РЕБ) – це комплекс заходів, спрямованих на зниження ефективності радіоелектронних засобів противника та захист власних радіоелектронних засобів від його впливу. РЕБ включає в себе різні методи, такі як радіоелектронне придушення, радіоелектронна розвідка та радіоелектронний захист.

Радіоелектронне придушення (РЕП) – це сукупність дій, спрямованих на порушення роботи радіоелектронних засобів противника шляхом створення перешкод їх сигналам. РЕП може бути спрямована на різні типи систем, такі

як радіозв'язок, радіолокація, навігація, системи управління та інші. Для досягнення цього застосовують такі методи як зашумлення, імітація та спотворення. Зашумлення полягає у створенні потужного шумового сигналу в діапазоні частот, що використовується противником, що робить неможливим прийом корисного сигналу. Зашумлення може бути широкосмуговим, що охоплює широкий діапазон частот, або вузькосмуговим, що спрямоване на конкретну частоту. Імітація полягає у створенні фальшивих сигналів, які імітують сигнали противника, що може призвести до дезінформації, помилкових рішень та неправильних дій. Імітація може бути спрямована на різні типи систем, такі як радіолокація, навігація та системи управління. Спотворення полягає у спотворенні сигналів противника, що робить їх нерозбірливими або непридатними для використання. Спотворення може бути досягнуто за допомогою різних методів, таких як фазова маніпуляція, частотна маніпуляція та інші.

Радіоелектронна розвідка (РЕР) – це сукупність дій, спрямованих на збір інформації про радіоелектронні засоби противника, такі як їх типи, характеристики, розташування та режими роботи. РЕР дозволяє отримати цінну інформацію про можливості противника, його плани та наміри.

Основними методами РЕР є перехоплення сигналів, пеленгація та радіоелектронна розвідка на основі безпілотних літальних апаратів (БПЛА). Перехоплення сигналів полягає у перехопленні радіосигналів противника за допомогою спеціальних приймальних пристроїв. Перехоплені сигнали можуть бути проаналізовані для визначення типу системи, її характеристик та іншої інформації. Пеленгація полягає у визначенні напрямку на джерело радіосигналу. Пеленгація дозволяє визначити розташування радіоелектронних засобів противника. БПЛА можуть бути оснащені спеціальними сенсорами та приймальними пристроями для збору розвідувальної інформації, включаючи радіоелектронну розвідку.

Радіоелектронний захист (РЕЗ) спрямованих на захист власних радіоелектронних засобів від впливу РЕБ противника. РЕЗ включає в себе різні методи, такі як екранування, фільтрація, частотна агіляція та інші.

Для захисту застосовують екранування, фільтрацію та частотну агіляцію. Екранування полягає у використанні спеціальних матеріалів для блокування електромагнітних випромінювань. Екранування може бути використане для захисту окремих пристроїв або цілих приміщень. Фільтрація полягає у використанні спеціальних пристроїв для видалення небажаних сигналів з корисного сигналу. Фільтрація може бути використана для видалення шуму, перешкод та інших небажаних сигналів. Частотна агіляція полягає у зміні частоти передачі сигналу для уникнення перешкод та РЕБ противника. Частотна агіляція може бути використана для захисту радіозв'язку, радіолокації та інших систем.

РЕБ може суттєво вплинути на ефективність систем координації дій на полі бою, порушуючи роботу систем зв'язку, навігації та управління. Це може призвести до дезорієнтації військ, втрати контролю над бойовими діями та інших негативних наслідків.

Перехоплення сигналів є важливим елементом РЕБ та розвідки. Сучасні технології дозволяють перехоплювати радіосигнали на великих відстанях та аналізувати їх для отримання цінної інформації.

Основними методами перехоплення сигналів є пасивне та активне перехоплення. Пасивне перехоплення полягає у перехопленні радіосигналів без їх активного виявлення. Пасивне перехоплення дозволяє збирати інформацію про радіоелектронні засоби противника, не розкриваючи своєї присутності. Активне перехоплення полягає у передачі спеціальних сигналів, які викликають реакцію радіоелектронних засобів противника. Активне перехоплення дозволяє визначити тип системи, її характеристики та розташування.

Для захисту від перехоплення сигналів використовуються різні методи, такі як шифрування, спрямована передача, частотна агіляція та інші[6].

1.2.2 Кіберзагрози та методи дезінформації

Кіберзагрози – це дії, спрямовані на порушення роботи або компрометацію інформаційних систем та даних. У військових умовах кіберзагрози можуть бути використані для порушення роботи систем зв'язку, навігації, управління, збору розвідувальної інформації та інших цілей.

Основні типи кіберзагроз включають зломи систем, розповсюдження шкідливого програмного забезпечення (malware), відмову в обслуговуванні (DoS-атаки) та фішинг. Хакери можуть зламувати інформаційні системи для отримання доступу до даних, порушення їх роботи або встановлення шкідливого програмного забезпечення. Malware може бути використане для крадіжки даних, порушення роботи систем або навіть для саботажу. DoS-атаки спрямовані на перевантаження інформаційних систем трафіком, що робить їх недоступними для легітимних користувачів. Фішинг – це вид шахрайства, спрямований на отримання конфіденційної інформації, такої як паролі та номери кредитних карток, шляхом обману користувачів.

Дезінформація – це поширення неправдивої інформації з метою маніпулювання громадською думкою або поведінкою людей. У військових умовах дезінформація може бути використана для деморалізації військ, поширення паніки, підриву довіри до командування та інших цілей.

Основними методами дезінформації є фейкові новини, пропаганда та психологічні операції. Фейкові новини – це неправдива інформація, яка подається як справжні новини. Фейкові новини можуть бути поширені через соціальні мережі, веб-сайти та інші канали. Пропаганда – це систематичне поширення інформації з метою формування певної думки або поведінки. Пропаганда може бути використана для деморалізації противника, підтримки власних військ або для впливу на громадську думку. Психологічні операції –

це комплекс заходів, спрямованих на вплив на психологічний стан противника. Психологічні операції можуть включати в себе пропаганду, дезінформацію, залякування та інші методи.

Для захисту від кіберзагроз та дезінформації необхідно використовувати комплексний підхід, який включає в себе технічні, організаційні та інформаційні заходи. Технічні заходи включають використання антивірусного програмного забезпечення, файрволів, систем виявлення вторгнень та інших технічних засобів. Організаційні заходи включають розробку політик безпеки, навчання персоналу, регулярне оновлення програмного забезпечення та інші організаційні заходи. Інформаційні заходи включають розповсюдження правдивої інформації, протидія дезінформації, розвиток медіаграмотності та інші інформаційні заходи.

В цілому, аналіз загроз інформаційній безпеці в умовах війни показує, що ці загрози є реальними та небезпечними. Для забезпечення ефективного захисту необхідно використовувати комплексний підхід, який включає в себе технічні, організаційні та інформаційні заходи.

1.3 Обґрунтування необхідності розробки апаратно-програмного комплексу для передачі коротких текстових повідомлень

Сучасні бойові дії – це швидкоплинний такий собі танцювальний марафон, де кожне рішення та команда мають бути надані вчасно, щоб не відставати від ритму[4]. Успіх бойових дій залежить не лише від фізичної сили, а й від можливості злагоджено та оперативно обмінюватися інформацією між різними підрозділами, ніби танцюристи, що рухаються в єдиному ритмі. Об'єднання сил різного призначення, щоб творити потужний хор, вимагає ефективного зв'язку.

Але традиційні системи зв'язку не завжди підходять для цього, адже мають свої недоліки. Радіозв’язок, який так широко використовується, часто не впорається з перешкодами та ЕРБ, якщо раптом виникне хвиля шуму.

Також обмежена кількість інформації, що можна передати за один раз, ризик перехоплення сигналів противником. Супутниковий зв’язок дороговартісний, та залежить від супутників, що може стати проблемою під час бойових дій, де ситуація може змінюватися непередбачувано.

IP-телефонія може бути не надійна в умовах бойових дій, бо залежить від наявності мережі Інтернет, що може бути проблемою в умовах обмеженої інфраструктури та можливих обстрілів мережевих вузлів. Телефонний зв’язок може бути не ефективним через можливість перехоплення сигналу, обмежену дальність дії та складність використання в умовах сильних перешкод або відсутності сигналу [10].

Телеграфний зв’язок характеризується обмеженою швидкістю передачі даних та складнощами з передачею складних повідомлень або великих обсягів даних.

Сигнальний зв’язок не може передавати складні або вичерпні повідомлення, легко перехоплюється, обмежений в дальності передачі сигналів.

На жаль, сучасне поле бою – це не лише фізична битва, а й війна за інформацію. Противник може перехоплювати радіосигнали, супутниковий зв'язок, а також підслуховувати телефонні розмови, щоб отримати цінну інформацію про плани та рухи. Кіберзагрози також представляють серйозну небезпеку, адже за вдяки ним можливі порушення роботи систем зв'язку і крадіжка конфіденційної інформації, що в свою чергу може спричинити дезінформацію, яку протиник може поширювати за для дезорієнтування чи то військових, чи цивільних [1].

Тому система зв’язку має бути максимально легкою, компактною та зручною, щоб працювати в різноманітних умовах, включаючи обмежені простори, складні погодні умови та швидке пересування.

На сам перед має бути не лише простою в експлуатації, але й енергоефективною, щоб забезпечити тривалу роботу без підзарядки в умовах обмежених ресурсів та можливих перебоїв з електропостачанням.

Також, важливим нюансом є те, що текстові повідомлення швидше передаються та отримуються і можуть бути зашифровані для ускладнення перехоплення та вимагають менше енергії для передачі між пристроями, а також можуть бути використані для оперативної передачі команд, інструкцій та іншої важливої інформації між військовими підрозділами.

Тому необхідність в розробці апаратно-програмного комплексу дозволить покращити ефективність координації дій на полі бою, підвищити рівень безпеки передачі інформації та забезпечити успішне контролювання і ведення бойових дій.

Висновки до розділу 1

У першому розділі був проведений аналіз існуючих систем координації дій військових на полі бою. Розглянуто традиційні системи зв'язку, такі як радіо, супутниковий зв'язок та IP-телефонія, та визначено їх недоліки в сучасних умовах. Відсутність надійного та швидкого зв'язку може призвести до неправильних рішень, втрати контролю над ситуацією на полі бою та втрат серед військових.

Проаналізовано проблеми з інформаційною безпекою в умовах війни, зокрема з радіоелектронною боротьбою, перехопленням сигналів та кіберзагрозами. Це підкреслює необхідність розробки нових рішень для зв'язку за для більшої гнучкості та ефективності у використані.

2 РОЗРОБКА АРХІТЕКТУРИ ТА ФУНКЦІОНАЛЬНИХ ВИМОГ ДО КОМПЛЕКСУ

2.1 Вимоги до зв’язку і автоматизація управління військами

Засоби зв'язку є основним засобом автоматичного управління військ (АУВ), бойовими засобами та озброєнням [8]. Командири і начальники штабів зобов'язані за будь-яких обставин підтримувати постійний зв'язок з вищестоящими і підлеглими командирами, штабами.

Зв'язок виконує завдання обміну інформацією в системі управління силами. Для виконання цих завдань засоби зв’язку та АУВ повинні відповідати вимогам своєчасності, надійності та конфіденційності.

Своєчасність – засоби військового зв’язку забезпечують можливість обміну інформацією, обробки інформації та вирішення інформаційно-обчислювальних завдань у задані часові рамки [13].

Сучасні операції пред'являють високі вимоги до своєчасності зв'язку. Це пояснюється швидким і високим темпом розвитку військових дій, а також частими і різкими змінами обстановки внаслідок застосування ракетно-ядерної зброї. Раптові зміни обстановки вимагають від командирів негайної реакції, особливо в критичні моменти бою. Значення своєчасності зв'язку при отриманні інформації від різних розвідок, значення радіоактивного, хімічного та бактеріологічного зараження різко зростає при передачі сигналів про повітряного противника, радіоактивне, хімічне та бактеріологічне зараження. Своєчасність зв'язку особливо важлива в ракетних військах і військах протиповітряної оборони.

Показники оцінки своєчасності різні як для телефонного, так і для телеграфного зв’язку.

Кількісна оцінка своєчасності телефонного зв’язку (за умови) визначається часом очікування з’єднання ($\mathbf{t}_{оч}$), який визначається від моменту

посилки виклику тому чи іншому абоненту до моменту з’єднання з цим абонентом.

Органи управління виконають вимоги до телефонного зв’язку вчасно, якщо $\mathbf{t}_{\text{оч}} \leq \mathbf{T}_{\text{оч доп}}$ (тут допустимий час очікування - $\mathbf{T}_{\text{оч доп}}$).

Імовірність своєчасного встановлення з’єднання ($\mathbf{Q}_{\text{тф}}$) може бути використана як показник якості телефонного зв’язку по своєчасності: $\mathbf{Q}_{\text{тф}} = \mathbf{Q}(\mathbf{t}_{\text{оч}} \leq \mathbf{T}_{\text{оч доп}}), \mathbf{Q}_{\text{тф}} = \mathbf{Q}_{\text{тф вим}}$. .

Щоб отримати кількісну оцінку своєчасності телеграфного зв’язку, використовувується час перебування повідомлень у системі зв’язку ($\mathbf{t}_{\text{сз}}$), який починається з моменту подачі повідомлень для відправлення та триває до моменту вручення повідомлень на іншому управлінському пункті.

Вимоги управління до телеграфного зв’язку будуть виконані за своєчасністю, якщо $\mathbf{t}_{\text{сз}} \leq \mathbf{T}_{\text{сз. доп.}}$ ($\mathbf{T}_{\text{сз доп}}$ – допустимий час перебування повідомлень в системі зв’язку).

Імовірність своєчасної передачі повідомлення ($\mathbf{Q}_{\text{тг}}$), яка не нижче необхідної, та слугує показником якості телеграфного зв’язку за своєчасністю:

$$Q_{\text{тг}} = Q\left(t_{\text{сз}} \leq T_{\text{сз доп}}\right),\ Q_{\text{тг}} = Q_{\text{тг вим}}. \qquad (2.1)$$

Відповідні нормативні документи ГШ визначають контрольні терміни проходження повідомлень до технічних засобів зв’язку.

Своєчасність досягається за допомогою наступного: постійної готовності зв’язку та АУВ до виконання покладених на них завдань з обміну, обробки та зберігання інформації, вирішення інформаційних і розрахункових завдань у задані (нормативні) строки; висококваліфікованого персоналу, чітко організованого чергування в елементах системи зв’язку та автоматизації; правильного вибору засобів і методів організації та забезпечення зв’язку та АУВ.

Довіра - це здатність військових зв’язків передавати та обробляти інформацію з певною точністю.

Існує можливість оцінити кількісну достовірність зв’язку за допомогою оцінки ймовірності правильного прийому повідомлення, яка визначається як відношення кількості правильно прийнятих елементів повідомлення до загальної кількості повідомлень, які були передані.

Розбірливість є основним критерієм телефонного зв’язку:

$$A = \frac{M_0}{M}, \tag{2.2}$$

де $\boldsymbol{M_0}$, $\boldsymbol{M}$ – відповідно до кількості елементів мови, які були правильно отримані та передані.

Звуки, слова та фрази можуть складати мову. Відмінна якість військового зв’язку повинна мати оцінку 0,99, хороша якість 0,97 і задоволена якість 0,96.

Імовірність правильного прийому повідомлення ($\mathbf{P}_{\text{п}}$) є основним показником для передачі даних і телеграфного зв’язку:

$$P_{\text{п}} = \frac{M_{\text{п}}}{M_{\text{п}} + M_{\text{пом}} \times P_{\text{пом}}} = 1 - P_{\text{п}}, \tag{2.3}$$

де $\mathbf{P}_{\text{пом}}$ – ймовірність того, що повідомлення буде прийнято помилково;

$\mathbf{M}_{\text{п}}$– кількість правильних символів;

$\mathbf{M}_{\text{пом}}$ – помилкових знаків;

$\mathbf{M}_{\text{п}} + \mathbf{M}_{\text{пом}}$ – загальна кількість знаків, які транслюються каналом зв’язку.

При передачі телеграфних повідомлень ймовірність помилки знаків не повинна перевищувати 10-3.

Для факсимільного зв'язку показником надійності є ймовірність розпізнавання символу (букви, символу, символу тощо). При передачі факсів він повинен бути не менше 0,995.

Довірливість зв’язку та АУВ досягається за допомогою регулярного контролю та підтримки характеристик каналів, трактів, засобів зв’язку та автоматизації відповідно до стандартів, повторне передавання інформації, а

також передавання повідомлень одночасно по декількох каналах зв’язку, створених різними засобами, також, використання кращих каналів зв’язку для передавання найважливіших повідомлень і використання апаратних та програмних методів підвищення достовірності.

Скритність – здатність військового зв’язку зберігати в таємниці як факт передачі, так і зміст інформації під час обміну, обробки, зберігання та вирішення задач, пов’язаних з інформацією та розрахунками.

Визначення ступеня засекречування (шифрування або кодування) інформації в системі зв’язку визначає рівень безпеки змісту повідомлень. Більшість повідомлень у низових підрозділах носять таємний характер.

Це пов’язано з тим, що повідомлення, які циркулюють від пунктів управління до елементів бойового порядку, містять бойові завдання, які вирішують підрозділи, а деякі містять відомості про замисел майбутнього бою та прийняту структуру управління. У таких обставинах швидке отримання та розповсюдження інформації противником, навіть у вигляді окремих повідомлень, дозволить йому протистояти нашим військам. Повідомлення, які засекречені з грифом «для службового користування», можна дешифрувати практично в реальному часі, якщо противник використовує сучасні обчислювальні техніки. Таким чином, більшість повідомлень, які надсилаються технічними засобами зв’язку, повинні бути засекречені.

Використання апаратури і засекречування з грифом «для службового користування» і документів прихованого управління військами (ПУВ) буде використовуватися для забезпечення стійкості апаратури засекречування. Документи можуть використовуватися для доставки повідомлень таємного характеру, які потребують значного часу реакції (декількох годин).

Основні критерії скритності:

коефіцієнт «закриття» зв’язку каналів:

$$K_з = \frac{N_{\text{закр.(кан) лін.}}}{N_{\text{заг.}}}, \qquad (2.4)$$

де $\boldsymbol{N}_{\text{закр.(кан) лін.}}$ – кількість заблокованих каналів чи ліній;

$\boldsymbol{N}_{\text{заг.}}$ – загальна кількість.

Досягається скритність зв’язку та АУВ:

– обмеження доступу до інформації, яку отримують службові особи;

– використання засобів засекречування та дотримання інструкцій щодо їх експлуатації;

– уникнення несанкціонованого доступу до інформації за допомогою апаратних, програмних, криптографічних методів і організаційних заходів.;

– використання документації ПУВ;

– використання ефективних методів паролювання та імітозахисту;

– перевірка даних шляхом повторного передавання;

– дотримання правил і організація контролю за встановленням зв’язку, обміном інформацією, її обробкою, використанням засобів автоматизації, виконанням вимог режиму секретності та боротьбою з нав’язуванням хибних режимів роботи засобам зв’язку та автоматизації.

2.2 Порівняння апаратних платформ для розробки

Перш ніж розробляти пристрій, важливо визначити платформу на найкращому мікроконтролері (МК), щоб підключити всі модулі, які будуть використовуватися, щоб забезпечити оптимальну роботу. Для правильної роботи периферійних приладів потрібно порівняти кілька МК.

Для цього було детально розглянуто кілька популярних МК, включаючи STM32, Arduino та інші відповідні компоненти.

На сам перед, розглянуто та порівняти основні параметри апаратної платформи, такі як:

– ядро;

– тактова частота;

– оперативна пам'ять;

- флеш-пам'ять;
- кількість GPIO;
- інтерфейси;
- напруга живлення.

Оскільки, для нормальної роботи всіх приєднаних компонентів, дуже велику роль відіграє саме бистрота виконання задач в МК.

Основну увагу потрібно приділити ядру, адже тип ядра визначає архітектуру процесора, на якому базується мікроконтролер. І є багато типів на якому базується мікроконтролер, наприклад, «ARM Cortex-M3», «AVR», «PIC», «RISC-V». Та мають різні розрядності, найпоширеніші це 8-бітні, 16-бітні та 32-бітні.

Також, не менш важливою є: тактова частота, вона визначає швидкість оброблення даних МК; оперативна пам'ять яка дозволить визначити кількість даних, які можуть бути оброблені одночасно; флеш-пам'ять яка вказує на кількість даних, які можна зберегти в мікроконтролері; кількість GPIO для розуміння кількості вхідних/вихідних пінів, які можна використовувати для підключення компонентів; інтерфейси що визначають, які типи зв'язку підтримуються мікроконтролером; напруга живлення при яких мікроконтролер може працювати.

2.2.1 Апаратна платформа Arduino Mega

«Arduino Mega 2560» – потужна МК плата, яка набула популярності серед розробників і любителів електроніки завдяки широкому діапазону функцій і простоті використання. Вона базується на ATmega2560, та має великий обсяг пам’яті і велику кількість вхідних/вихідних пінів, що робить її зручною для проектування проєктів [14].

Крім того, вона має 54 піни цифрового вводу/виводу, з яких 15 можуть бути використані як виходи широтно-імпульсної модуляції (ШІМ) та 16 аналогових вхідних пінів, з яких шість можуть бути вихідами ШІМ. На платі

також розташовані SPI, TWI та UART інтерфейси, що дозволяє підключати різні периферійні модулі (табл. 2.1).

Рисунок 2.1 – Вигляд МК Arduino Mega ADK на базі ATmega2560

Таблиця 2.1 – Загальні характеристики Arduino Mega

Параметр	Значення
Ядро	ATmega2560
Тактова частота	16 МГц
Оперативна пам'ять	8 КБ
Флеш-пам'ять	256 КБ
Кількість GPIO	54
Інтерфейси	I2C, SPI, UART
Напруга живлення	5 В
Робоча температура	0°C до 70°C

Крім потужних можливостей, даний МК також вирізняється своїм відкритим кодом, що дозволяє легко модифікувати та покращувати її функціональність, великим та активним співтовариством розробників, яке забезпечує широку підтримку та доступність безлічі прикладів скетчів, що значно спрощує процес навчання та розробки за доступною ціною.

2.2.2 Апаратна платформа STM32

«STM32F407VGT6» – це потужний 32-бітний МК, що належить до сімейства STM32F4 від компанії «STMicroelectronics» [16].

МК базується на ядрі ARM Cortex-M4F і має тактову частоту 168 МГц. Він має великий об’єм пам’яті, включаючи 1 МБ флеш-пам’яті для зберігання програмного скетчу та 192 КБ оперативної пам’яті SRAM і 64 КБ EEPROM для зберігання даних.

Ця плата має кілька периферійних пристроїв для розширення її функціональності, до них належать:

– дисплей TFT LCD 2,4 дюйма з роздільною здатністю 320 x 240 пікселів, який може відображати графічну та текстову інформацію;

– вбудований мікрофон, який дозволяє використовувати плату для розпізнавання голосу або запису звуку;

– вбудований Wi-Fi модуль, який дозволяє підключати бездротове підключення до інтернету; і широкий спектр інтерфейсів, таких як UART, SPI, I2C, CAN та USB.

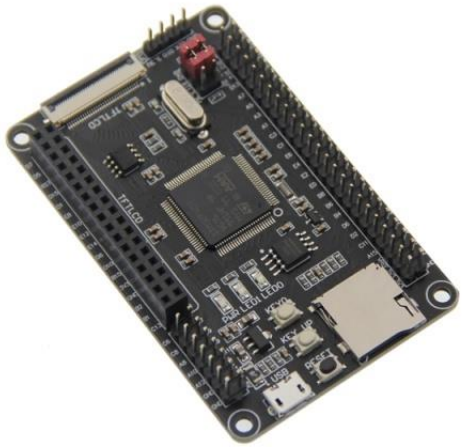


Рисунок 2.2 – Вигляд МК STM32F407VGT6 на базі ARM Cortex-M4

Таблиця 2.2 – Загальні характеристики STM32F407VGT6

Параметр	Значення
Ядро	ARM Cortex-M4
Тактова частота	До 168 МГц
Оперативна пам'ять	192 КБ
Флеш-пам'ять	1 МБ
Кількість GPIO	82
Інтерфейси	I2C, SPI, UART, CAN, USB, Ethernet
Напруга живлення	1.8-3.6 В
Робоча температура	-40°C до 85°C

2.3 Порівняння і висновки вибору МК Arduino та STM32

При виборі апаратної платформи важливо було детально розглянути можливості та обмеження різних мікроконтролерів. Одними з найпоширеніших варіантів є мікроконтролери серії Arduino та STM32.

Arduino – це відкрита апаратна та програмна платформа, яка здобула популярність завдяки своїй простоті використання та великій спільноті користувачів. Основні МК в серії Arduino базуються на архітектурі AVR від Atmel.

Ця платформа вирізняється простотою програмування, що базується на C/C++, а середовище розробки (IDE) надає всі необхідні інструменти для написання, компіляції та завантаження програм до мікроконтролера. Також, завдяки великій спільноті розробників доступні численні бібліотеки та приклади для полегшення роботи з різними модулями.

Однак, зважаючи на все, обчислювальні можливості Arduino обмежені через 8-бітову архітектуру і відносно низьку тактову частоту, що може бути

критичним коли потрібна висока продуктивність або обробка великих обсягів даних.

Крім того, енергоспоживання «Arduino Mega 2560» може бути високим у порівнянні з сучасними 32-бітними мікроконтролерами, що може стати проблемою в автоматизації системи.

STM32 - це серія мікроконтролерів від компанії STMicroelectronics, які побудовані на базі 32-бітових ядер ARM Cortex. Зокрема, розглянемо модель STM32F407VGT6, яка оснащена ядром ARM Cortex-M4. Цей МК працює на тактовій частоті до 168 МГц, має 1 МБ флеш-пам'яті та 192 КБ оперативної пам'яті SRAM. STM32F407VGT6 підтримує численні периферійні інтерфейси, такі як I2C, SPI, UART, CAN, USB, Ethernet та інші, що дозволяє використовувати його у складних системах з великою кількістю підключень.

Він має значно вищу обчислювальну потужність у порівнянні з Arduino Mega 2560 завдяки 32-бітовому ядру та високій тактовій частоті. Це дозволяє виконувати складні обчислення та обробляти великі обсяги даних швидше та ефективніше. Крім того, «ARM Cortex-M4» має розширену підтримку інструкцій для цифрової обробки сигналів (DSP), що відкриває нові можливості для обробки аудіо- та відеосигналів, а також для реалізації складних алгоритмів обробки даних.

Енергоспоживання мікроконтролерів STM32 також оптимізоване. Вони можуть працювати в різних режимах низького енергоспоживання, що дозволяє значно продовжити час автономної роботи пристроїв. Це особливо важливо для військових систем, де економія енергії є критичним фактором.

Програмування STM32 може бути складнішим у порівнянні з Arduino через більшу складність архітектури та більшу кількість налаштувань. Однак, на ринку доступні потужні інструменти розробки, такі як «STM32CubeIDE», яка надає всі необхідні засоби для розробки, налагодження та тестування програм. Крім того, STMicroelectronics надає широкий набір бібліотек та

прикладів скетчу, що спрощує роботу з периферійними інтерфейсами та модулем.

Таблиця 2.3 – Порівняння МК STM32 та Arduino Mega

Параметр	STM32F407VGT6	Arduino Mega 2560
Ядро	ARM Cortex-M4	AVR ATmega2560
Тактова частота	До 168 МГц	16 МГц
Оперативна пам'ять	192 КБ	8 КБ
Флеш-пам'ять	1 МБ	256 КБ
Кількість GPIO	82	54
Інтерфейси	I2C, SPI, UART, CAN, USB, Ethernet	I2C, SPI, UART
Напруга живлення	1.8-3.6 В	5 В

Вибір між Arduino та STM32 залежав від вимог до проєкту.

Так, для складного завдання, що вимагає високої продуктивності та енергетичної ефективності, STM32 є кращим варіантом.

У розробки апаратно-програмного комплексу, де критичними є продуктивність, надійність та енергоспоживання, «STM32F407VGT6» було вибрано більш придатною платформою. Висока обчислювальна потужність дозволила ефективно обробляти шифровані повідомлення та управляти складними комунікаційними протоколами. Розширені периферійні можливості забезпечили гнучкість у підключенні різних модулів, таких як дисплеї, клавіатури та комунікаційні модулі. Крім того, підтримка режимів низького енергоспоживання дозволила використовувати цей МК як автономну систему, що є важливим аспектом у військових умовах.

У підсумку, обидві платформи мають свої сильні та слабкі сторони. Arduino є відмінним вибором для простих та швидких проєктів, де важливими є простота використання та доступність ресурсів. Однак, STM32 надає значно

більшу продуктивність та гнучкість, що робило його ідеальним для розробки військової системи координації.

2.4 Вибір та характеристики модулів для розробки

Вибір модулів та компонентів є критичним етапом у розробці апаратно-програмного комплексу. Для забезпечення ефективної роботи системи необхідно було обрати компоненти, які відповідають вимогам щодо надійності, енергоспоживання, функціональності та зручності інтеграції. У цьому розділі було детально розглянуто вибір основних модулів та компонентів, які були використані у розробці комплексу. Серед них: комунікаційний модуль, дисплей, клавіатура, живлення та інші периферійні пристрої.

2.4.1 Характеристики модуля Long Range

Комунікаційний модуль є одним із найважливіших компонентів системи, оскільки забезпечує передачу даних між пристроями. Для досягнення мети, було обирано модуль «Long Range (LoRa) SX1278», який має високу надійність та дальність передачі [11].

LoRa – це технологія бездротового зв’язку, яка дозволяє передавати дані на великі відстані з низьким енергоспоживанням. Модуль SX1278 працює на частотах 433 MHz і забезпечує передачу даних на відстань до 10 км в умовах прямої видимості (табл. 2.4).

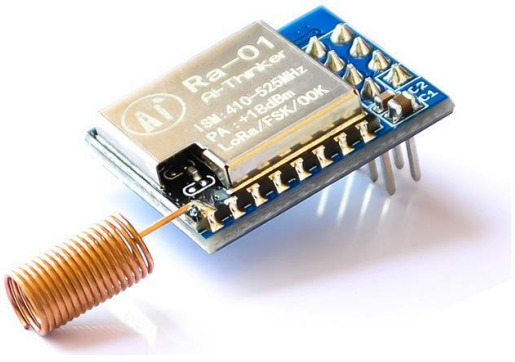


Рисунок 2.3 – Зображення модуля LoRa SX1278

Таблиця 2.4 – Характеристика модуля LoRa SX1278

Параметр	Значення
Частотний діапазон	433 MHz
Максимальна вихідна потужність	+20 dBm
Чутливість приймача	до -148 dBm
Швидкість передачі даних	від 0.018 до 37.5 kbps
Енергоспоживання в режимі передачі	120 мА при 20 dBm
Енергоспоживання в режимі очікування	< 1 мА
Інтерфейс	SPI

Модуль LoRa SX1278 є оптимальним вибором для системи завдяки своїй високій чутливості та здатності працювати в умовах значних перешкод. Низьке енергоспоживання дозволило використати його для автоматизації системи з обмеженням живлення, що критично важливо для військових застосувань.

2.4.2 Характеристики дисплейного модуля TFT LCD SPI

Дисплей також є ключовим компонентом, оскільки забезпечує відображення інформації користувачеві. Для комплексу було обрано «TFT LCD SPI ILI9341» дисплей 2.8". Цей дисплей забезпечує високу контрастність і чіткість зображення при низькому енергоспоживанні.

Рисунок 2.4 – Зображення дисплейного модуля TFT LCD SPI

Таблиця 2.5 – Характеристика дисплею TFT LCD SPI ILI9341

Параметр	Значення
Тип дисплея	TFT LCD
Контролер	ILI9341
Розмір дисплея	2.8
Роздільна здатність	240 x 320 пікселів
Інтерфейс	SPI, 8/16-бітний паралельний інтерфейс
Кольори	262K (18-бітний режим), 65K (16-бітний режим)
Живлення	2.8-3.3V для логіки, 3.3V для підсвічування
Підсвічування	Світлодіодне (LED), біле
Частота оновлення	до 60 Гц
Вбудована пам'ять	172800 байтів (для зберігання графічних даних)

TFT дисплей ILI9341 ідеально підходить для відображення графічної та текстової інформації завдяки своїй високій роздільній здатності та насиченим кольорам. Його ширококутний огляд забезпечує відмінну видимість під будь-яким кутом, що є важливим для використання в польових умовах. Компактні розміри дисплея дозволили легко інтегрувати його до пристрою, а підтримка SPI інтерфейсу спростило підключення до різноманітних мікроконтролерів.

Світлодіодне підсвічування забезпечує хорошу видимість навіть в умовах низької освітленості, а енергоспоживання в межах 2.8-3.3V робить його ефективним для автоматизації системи.

2.4.3 Характеристики матричної клавіатури

Клавіатура є невід'ємним компонентом для введення даних користувачем. Тому, було обрано матричну клавіатуру 4x4, яка забезпечує зручність введення числової та алфавітної інформації. Матрична клавіатура складається з 16 клавіш, розташованих у матриці 4x4, що дозволяє легко інтегрувати її з мікроконтролером.

Рисунок 2.5 – Зображення клавіатури 4x4

Таблиця 2.6 – Характеристика матричної клавіатури 4x4

Параметр	Значення
Кількість клавіш	16
Конфігурація	4x4
Матеріал	Пластик, гумові контакти
Інтерфейс	Паралельний
Струм комутаціїї	100мА
Розміри	77x70x0,8 мм

Матрична клавіатура 4x4 забезпечує надійне введення даних користувачем та було легко інтегрувати з мікроконтролером завдяки простому інтерфейсу. Вона є зручною у використанні і має компактні розміри, що важливо для портативного пристрою.

2.4.4 Характеристика GPS модуля

Надання інформації про координати інших пристроїв є важливим аспектом координації дій на полі бою. Для цього було використано GPS модуль Neo-6M, який забезпечує точне визначення координат у реальному часі.

Рисунок 2.5 – Зображення GPS модулі Neo-6M

Таблиця 2.7 – Характеристика GPS модуля

Параметр	Значення
Чутливість	-161 дБм
Частота оновлення даних	до 10 Гц
Інтерфейс	UART
Напруга живлення	3.3-5 В
Точність позиціонування	2.5 м

Система відстеження координат дозволяє кожному пристрою передавати свої координати іншим пристроям у мережі. Це забнзпечило

створення інтерактивної карти розташування військових підрозділів, що є критично важливим для ефективного планування та координації дій.

2.4.5 Характеристика живлення

Живлення є критичним аспектом для портативного апаратно-програмного комплексу. Було обирано літій-іонний акумулятор ємністю 2000 мАг, який забезпечує тривалу автономну роботу пристрою навіть у важких умовах. Літій-іонні акумулятори відомі своєю високою енергетичною щільністю та низьким рівнем саморозряду, що робить його ідеальним вибором для портативних систем.

Рисунок 2.6 – Зображення модуля LoRa SX1278

Таблиця 2.8 – Характеристика Літій-іонного акумулятора

Параметр	Значення
Ємність	2000 мАг
Номінальна напруга	3.7 В
контролер заряду	захист розряду /перезарядження
Максимальна напруга	4.2 В
Мінімальна напруга	2.75 В
Максимальний струм розряду	2 А
Розміри	50x34x10 мм

Літій-іонний акумулятор забезпечує надійне живлення для всіх компонентів системи, дозволяючи їм працювати протягом тривалого часу без необхідності частого перезаряджання. Це критично важливо для військових застосувань, де доступ до джерел живлення може бути обмеженим.

2.5 Обґрунтування вибору програмного забезпечення

Вибір програмного забезпечення для розробки апаратно-програмного комплексу базується на необхідності забезпечення високої надійності, ефективності та простоти інтеграції з апаратною частиною.

Використання STM32CubeIDE дозволилло скористатися потужними інструментами для налаштування мікроконтролерів STM32, включаючи генерацію ініціалізаційного скетчу, що значно скорочує час розробки. Цей інструмент підтримує інтеграцію з бібліотеками HAL та CMSIS, що забезпечує спрощений доступ до периферійних модулів та функцій реального часу.

µVISION IDE від Keil також є обґрунтованим вибором завдяки його потужному відлагоджуваню та широкій підтримці мікроконтролерів ARM. Ці середовища розробки забезпечують високий рівень контролю над апаратними ресурсами та дозволяють ефективно реалізувати необхідні функціональні можливості комплексу.

2.5.1 STM32CubeIDE

STM32CubeIDE – це універсальний інструмент розробки для кількох ОС, який є частиною програмної екосистеми STM32Cube. STM32CubeIDE – це передова платформа розробки C/C++ з периферійною конфігурацією, генерацією скетчу, компіляцією коду та функціями налагодження для мікроконтролерів і мікропроцесорів STM32. Він заснований на фреймворку Eclipse/CD та ланцюзі інструментів GCC для розробки та GDB для налагодження. Він дозволяє інтегрувати сотні існуючих плагінів, які доповнюють функції Eclipse IDE.

STM32CubeIDE інтегрує функції конфігурації STM32 і створення проєктів від STM32CubeMX, щоб запропонувати інструмент «все в одному» та заощадити час на встановлення та розробку. Після вибору порожнього STM32 створюється проєкт і генерується скетч ініціалізації. У будь-який момент під час розробки можна повернутися до ініціалізації та конфігурації периферійних пристроїв або проміжного програмного забезпечення та відновити скетч ініціалізації без впливу на поточний скетч.

STM32CubeIDE включає аналізатори збірки та стека, які надають корисну інформацію про стан проєкту та вимоги до пам’яті. STM32CubeIDE також включає стандартні та розширені функції налагодження, включаючи перегляди регістрів ядра ЦП, пам'яті та регістрів периферійних пристроїв, а також перегляд змінних змінних, інтерфейс Serial Wire Viewer або аналізатор несправностей.

Усі функції:

– інтеграція сервісів від STM32CubeMX: мікроконтролер STM32, мікропроцесор, платформа розробки та вибір прикладу проєкту: розведення, годинник, периферійне обладнання та конфігурація проміжного програмного забезпечення, створення проєкту та генерація скетчу ініціалізації, програмне забезпечення та проміжне програмне забезпечення доповнено вдосконаленими пакетами розширення STM32Cube;

– на основі Eclipse CD з підтримкою доповнень Eclipse, GNU C/C++ для ланцюга інструментів Arm і налагоджувача GDB;

– серія STM32MP1: Підтримка проєктів OpenSTLinux: LinuxПідтримка Linux;

– додаткові розширені функції налагодження, зокрема: ядро ЦП, периферійний регістр і вид пам'яті, живий змінний перегляд годинника, системний аналіз і відстеження в реальному часі (SWV)Інструмент аналізу несправностей ЦП, підтримка налагодження з підтримкою RTOS, включаючи Azure;

– підтримка налагоджувальних зондів ST-LINK (STMicroelectronics) і J- Link (SEGGER);

– імпорт проєкту з Atollic TrueSTUDIO і AC6 System Workbench для STM32 (SW4STM32);

– підтримка кількох ОС: Windows , Linux і MacOS , лише 64-розрядні версії.

2.5.2 µVISION IDE

µVision IDE поєднує управління проектами, середовище виконання, засоби для створення, редагування вихідного коду та налагодження програм в єдиному потужному середовищі. µVision простий у використанні та прискорює розробку вбудованого програмного забезпечення. µVision підтримує декілька екранів і дозволяє створювати індивідуальні макети вікон у будь-якому місці візуальної поверхні.

Налагоджувач µVision забезпечує єдине середовище, в якому можна було тестувати, перевіряти та оптимізувати код програми. Налагоджувач включає традиційні функції, такі як прості та складні точки зупинки, вікна спостереження та контроль виконання, і забезпечує повну видимість периферійних пристроїв пристрою. Інтегрований редактор µVision Editor включає всі стандартні функції сучасного редактора вихідного коду, а також доступний під час налагодження. Підсвічування синтаксису кольорів, відступи в тексті та окреслення джерела оптимізовані для C/C++.

2.6 Функціональні вимоги

2.6.1 Передача та прийом текстових повідомлень

Передача та прийом текстових повідомлень є однією з ключових функцій апаратно-програмного комплексу для координації дій на полі бою. Ця функція забезпечує обмін інформацією між військовими підрозділами в

режимі реального часу. Основними вимогами до цієї функції є швидкість, надійність та зручність використання.

Для реалізації цієї функції використовуються модулі бездротового зв'язку LoRa SX1278, яка забезпечує далекобійність і низьке енергоспоживання. Технологія LoRa дозволяє передавати повідомлення на великі відстані, що є важливим для координації дій у великих зонах бойових дій. Застосування даної технології обумовлене її здатністю передавати дані на відстань до 10 км в ідеальних умовах, при цьому забезпечуючи високу енергоефективність.

У системі також використовується TFT дисплей розміром 2.8 дюйма для відображення отриманих та відправлених повідомлень. Це забезпечило зручний інтерфейс, що є важливим у стресових умовах бойових дій. Для введення текстових повідомлень використано матричну клавіатурау 4x4, яка дозволяє швидко і ефективно здійснювати необхідні операції.

2.6.2 Захист інформації від перехоплення та фальсифікації

Захист інформації від перехоплення та фальсифікації є критично важливим аспектом у військових комунікаціях. Для забезпечення високого рівня безпеки необхідно використовувати сучасні методи шифрування та автентифікації [9,14].

У системі застосовується алгоритм шифрування AES (Advanced Encryption Standard), який забезпечує високий рівень захисту даних. AES є симетричним блоковим шифром з фіксованою довжиною блоку 128 біт і довжиною ключа 128, 192 або 256 біт. Це забезпечує надійний захист даних від несанкціонованого доступу.

Для автентифікації користувачів використовуються криптографічні хеш-функції, такі як SHA-256. Це забезпечує захист від підробки повідомлень і гарантує, що тільки авторизовані користувачі можуть надсилати та отримувати повідомлення. Використання SHA-256 дозволило створити

криптографічні підписи, які неможливо підробити, забезпечуючи тим самим автентичність переданих даних.

Завдяки використанню AES для шифрування та SHA-256 для автентифікації, система забезпечує високий рівень захисту даних від перехоплення та фальсифікації [7,17]. Це дозволяє військовим підрозділам безпечно обмінюватися важливою інформацією, що є критичним у бойових умовах.

2.6.3 Модуль шифрування та дешифрування повідомлень

Шифрування в mbedTLS включає широкий спектр криптографічних алгоритмів і протоколів, які забезпечують конфіденційність, цілісність та автентифікацію даних у програмному забезпеченні. Основні аспекти шифрування в mbedTLS включають симетричне шифрування, асиметричне шифрування, хеш-функції та цифрові підписи, кожен з яких має свої важливі властивості і застосування.

Симетричне шифрування використовує один ключ як для шифрування, так і розшифрування даних. Ключ був використаний для шифрування повідомлення (***M***) у зашифрований текст (***C***) і для розшифрування ***C*** назад у ***M***.

Алгоритмом симетричного шифрування є – AES (Advanced Encryption Standard):

$$C = E_K(M), \tag{2.5}$$

де ***C*** – зашифрований текст;

$\boldsymbol{E_K}$ – функція шифрування з ключем ***K***;

M – відкритий текст.

AES використовує ключі різної довжини (128, 192 або 256 бітів) для захисту даних від несанкціонованого доступу.

Асиметричне шифрування використовує пару ключів: публічний ключ для шифрування і приватний ключ для розшифрування. Це дозволяє відправнику зашифрувати повідомлення за допомогою публічного ключа одержувача, який потім розшифровує його за допомогою свого приватного ключа.

Найпоширеніших алгоритмів асиметричного шифрування є - RSA (Rivest-Shamir-Adleman):

$$C = E_{PK}(M), \tag{2.6}$$

де $\boldsymbol{C}$ – зашифрований текст;

$\boldsymbol{E_{PK}}$ – функція шифрування з ключем $\boldsymbol{PK}$;

$\boldsymbol{M}$ – відкритий текст.

RSA використовується для обміну ключами і захисту даних в інтернет-протоколах, таких як TLS (Transport Layer Security).

Також використовуються хеш-функції SHA (Secure Hash Algorithm) для створення унікального «відбитка» вхідного повідомлення. Це коротке числове значення, яке представляє усюдикувату характеристику вхідного повідомлення. Він перевіряє цілісності даних у цифрових підписах та зберігання паролів у безпечному вигляді:

$$H = H_{ash}(M), \tag{2.7}$$

де $\boldsymbol{H}$ – хеш-значення;

$\boldsymbol{H_{ash}}$ – функція хешування;

$\boldsymbol{M}$ – вхідне повідомлення.

Цифрові підписи, такі як ECDSA (Elliptic Curve Digital Signature Algorithm), використано для забезпечення автентичності і цілісності повідомлення. Це дозволяє одержувачеві перевірити, що повідомлення було підписане відправником і не було змінено після підпису:

$$S = Sign_{SK}(M), \tag{2.8}$$

де $\boldsymbol{S}$ – цифровий підпис;

$\boldsymbol{Sign_{SK}}$ – функція підпису з приватним ключем $\boldsymbol{SK}$;

$\boldsymbol{M}$ – вхідне повідомлення.

ECDSA використовує еліптичні криві для створення цифрових підписів, що забезпечує високий рівень безпеки і ефективності.

Бібліотека підтримує імплементацію стандартів TLS, DTLS, SSL і має високий рівень оптимізації для обмежених ресурсів. Забезпечує підтримку широкого спектру платформ.

mbedTLS використовується для захисту даних у різних сценаріях, включаючи:

– *IoT безпека*: захист зв'язку та даних між IoT пристроями і хмаровими сервісами;

– *клієнт-серверні системи*: забезпечення безпеки з'єднань між клієнтами і серверами у мережевих додатках і веб-сайтах;

– *криптовалюта і блокчейн*: забезпечення конфіденційності та цілісності транзакцій у блокчейн мережах та криптовалютних гаманцях;

– *мобільні додатки*: шифрування даних у мобільних додатках для забезпечення приватності користувачів та захисту конфіденційної інформації;

– *вбудовані системи*: захист інформації, що передається між вбудованими пристроями (наприклад, в медичних приладах чи автомобільних системах).

mbedTLS забезпечує високий рівень безпеки завдяки криптографічним примітивам і захисту від атак, таких як злам пароля, перехоплення даних, атаки на цифрові підписи та інші.

Інтеграція mbedTLS відбувається через його API та бібліотеки, які надають доступ до різноманітних криптографічних функцій і протоколів. В основі інтеграції лежить створення і управління криптографічними контекстами, установка параметрів шифрування і підписів, обробка ключів і даних, а також управління сертифікатами та ідентифікаторами.

Вона також має документацію, приклади скетчів та різноманітні ресурси, що полегшують інтеграцію та розробку з використанням бібліотеки.

2.6.4 Надання інформації про координати інших пристроїв

Надання інформації про координати інших пристроїв є важливим аспектом координації дій на полі бою. Для цього використовуються GPS модулі Neo-6M, які забезпечують точне визначення координат у реальному часі. Система відстеження координат дозволяє кожному пристрою передавати свої координати іншим пристроям у мережі, що створює інтерактивну карту розташування військових підрозділів.

GPS модулі Neo-6M забезпечує високу точність позиціонування, що дозволяє точно визначати місцезнаходження підрозділів з точністю до кількох метрів. Це дозволяє командирам краще розуміти ситуацію на полі бою та приймати оперативні рішення на основі точних даних.

Для відображення координат використовується TFT дисплей, який показує поточні координати та координати інших пристроїв. Це дозволило користувачам бачити розташування своїх товаришів по команді в реальному часі. Система автоматично оновлює координати в реальному часі, забезпечуючи точну та актуальну інформацію про розташування підрозділів.

2.6.5 Інтеграція з іншими системами координації дій

Інтеграція з іншими системами координації дій є важливим аспектом, який забезпечує взаємодію між різними військовими підрозділами та підвищує ефективність командування. Для цього було забезпечено сумісність з існуючими системами зв'язку та координації.

Одним із важливих елементів інтеграції є використання стандартних протоколів обміну даними, таких як MQTT (Message Queuing Telemetry Transport) та JSON (JavaScript Object Notation). Протокол MQTT дозволив ефективно передавати повідомлення між пристроями у мережі,

використовуючи модель публікації-підписки. Це забезпечило надійну та масштабовану інтеграцію з іншими системами координації дій.

Для забезпечення сумісності з різними типами даних використано формат JSON, який є легким текстовим форматом обміну даними. Це дозволило забезпечити ефективну інтеграцію з іншими системами, зокрема системами управління базами даних та аналітичними системами.

Інтеграція з іншими системами також передбачає можливість підключення до централізованих серверів та баз даних для зберігання та обробки інформації. Це дозволило створювати розширені системи аналізу даних та забезпечувати високу точність і швидкість обробки інформації. Важливим аспектом є також забезпечення безпеки під час передачі даних між різними системами, що досягається використанням сучасних методів шифрування та автентифікації.

Таким чином, інтеграція з іншими системами координації дій забезпечує високу ефективність управління військовими підрозділами та підвищує оперативність прийняття рішень.

Висновки до розділу 2

У другому розділі було проведено аналіз вимог до системи зв'язку та автоматизації управління військами.

Розглянуто ключові фактори, що впливають на ефективність системи зв'язку, такі як, швидкість передачі інформації, захист від перехоплення та збереження цілісності даних.

Також було проаналізовано апаратні платформи для розробки апаратно-програмного комплексу. Розглянуто основні характеристики МК STM32 та Arduino Mega 2560. Було визначено, що STM32 більш підходить для створення ефективної системи зв’язку завдяки вищій обчислювальній потужності, розширеним периферійним можливостям та більшій енергоефективності.

3 ПРОЕКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1 Розробка схеми портативного пристрою

Розробка схеми портативного пристрою є важливим етапом у створенні апаратно-програмного комплексу для координації дій на полі бою. Основною метою є забезпечення коректного підключення всіх модулів та компонентів, щоб гарантувати надійність і функціональність пристрою. Для цього було використано МК STM32F407VGT6, що є основою пристрою, а також декілька зовнішніх модулів.

3.1.1 Підключення модулів до STM32

Радіомодуль LoRa забезпечує бездротовий зв'язок для передачі та прийому текстових повідомлень. Підключення «LoRa SX1278» до STM32 наведено на рисунку 3.1.

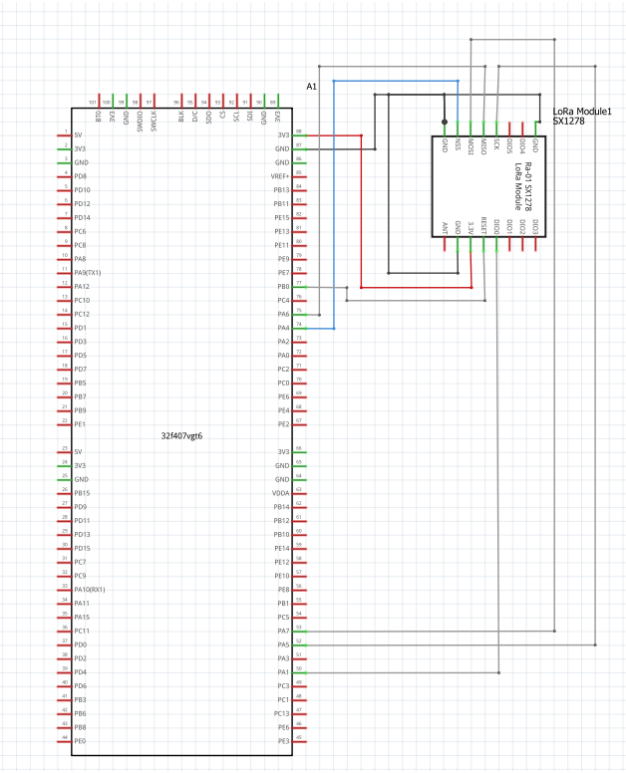


Рисунок 3.1 – З’єднання LoRa SX1278 до STM32

Даний модуль підключений до МК таким чином:

– **MOSI** під’єднаний до **PA7** і служить для передачі даних від STM32 до LoRa модуля, працюючи на логічному рівні 3.3V з максимальною швидкістю до 10 МГц;

– **MISO** до **PA6** для прийому даних від LoRa модуля до STM32 на тому ж логічному рівні і швидкості;

– **SCK** під’єднаний до **PA5** для синхронізації передачі даних по SPI з тактовою частотою до 10 МГц;

– **NSS** під’єднаний до **PA4** для активації вибору LoRa модуля при передачі даних, працюючи на логічному рівні 3.3V з активним низьким сигналом;

– **RES** до **PB0** і виконує функцію перезавантаження модуля, подаючи імпульсний сигнал на рівні 3.3V;

– **DIO0** до **PA1** і використовується як інтерфейс для обробки подій, таких як переривання.

Також, було під’єднано дисплейний модуль «TFT LCD SPI ILI9341», що грає не менш важливу роль, адже він використовується для візуалізації оператору інформацію та взаємодії із пристроєм.

Схематичне зображення підключення дисплейного модуля наведено на рисунку 3.2.

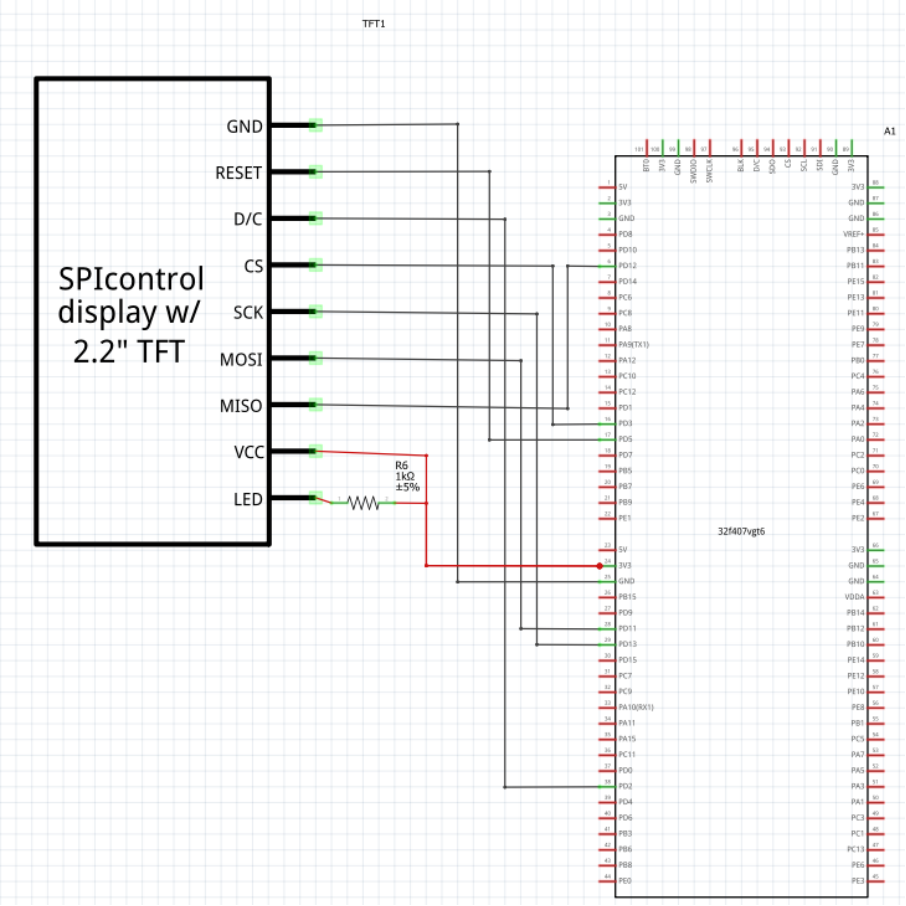


Рисунок 3.2 – Схема з’єднання TFT дисплею до STM32

Підключення TFT модуля до пінів МК здійснено за таки порядком:

– **MOSI** під’єднаний до **PD12** для передачі даних на логічному рівні 3.3V з максимальною швидкістю до 10 МГц.

– **MISO** до **PD11** для прийому даних на тому ж рівні і швидкості.

– **SCK** до **PD13** для синхронізації передачі даних по SPI з тактовою частотою до 10 МГц.

– **CS** під’єднаний до **PD3** для вибору модуля дисплея при передачі даних з активним низьким сигналом.

– **DC** до **PD2** для перемикання між даними і командами, працюючи на рівні 3.3V.

– **RESET** до **PA8** і виконує функцію перезавантаження дисплея, подаючи імпульсний сигнал на рівні 3.3V.

Було під’єднано модуль «GPS Neo-6M», який надає інформацію про координати пристрою, що є дуже важливим для координації на полі бою.

Модуль Neo-6M підключається до МК через інтерфейс UART, що дозволяє здійснювати передачу даних з високою швидкістю та низькою затримкою (рис. 3.3).

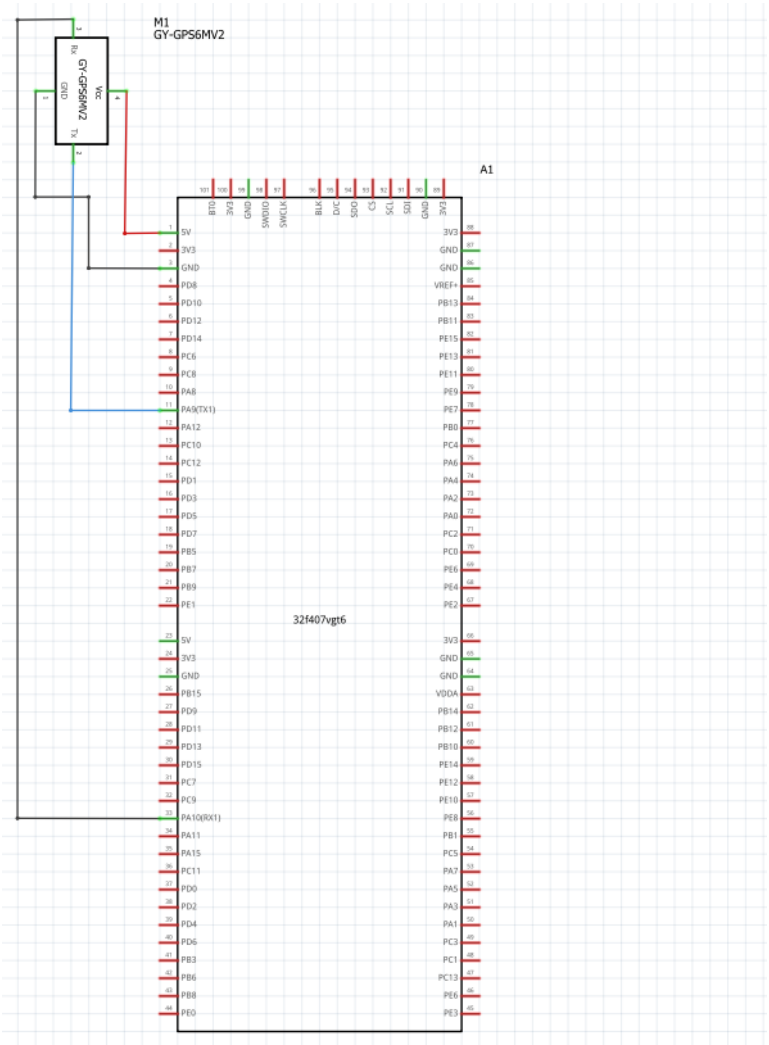


Рисунок 3.3 – Схема з’єднання модуля GPS Neo-6M

Підключення цього модуля до МК здійснено таким чином:

– **TX** підключається до **PA9** для передачі даних від **GPS** модуля до STM32, працюючи на логічному рівні 3.3V з швидкістю до 9600 бод;

– **RX** підключається до **PA10** для прийому даних від STM32 до GPS модуля на тому ж рівні і швидкості.

Також було підключено матричну клавіатуру, яка використовується для введення команд та текстових повідомлень.

Клавіатура має 8 ліній (4 рядки та 4 стовпці), які підключаються до пінів МК (рис. 3.4).

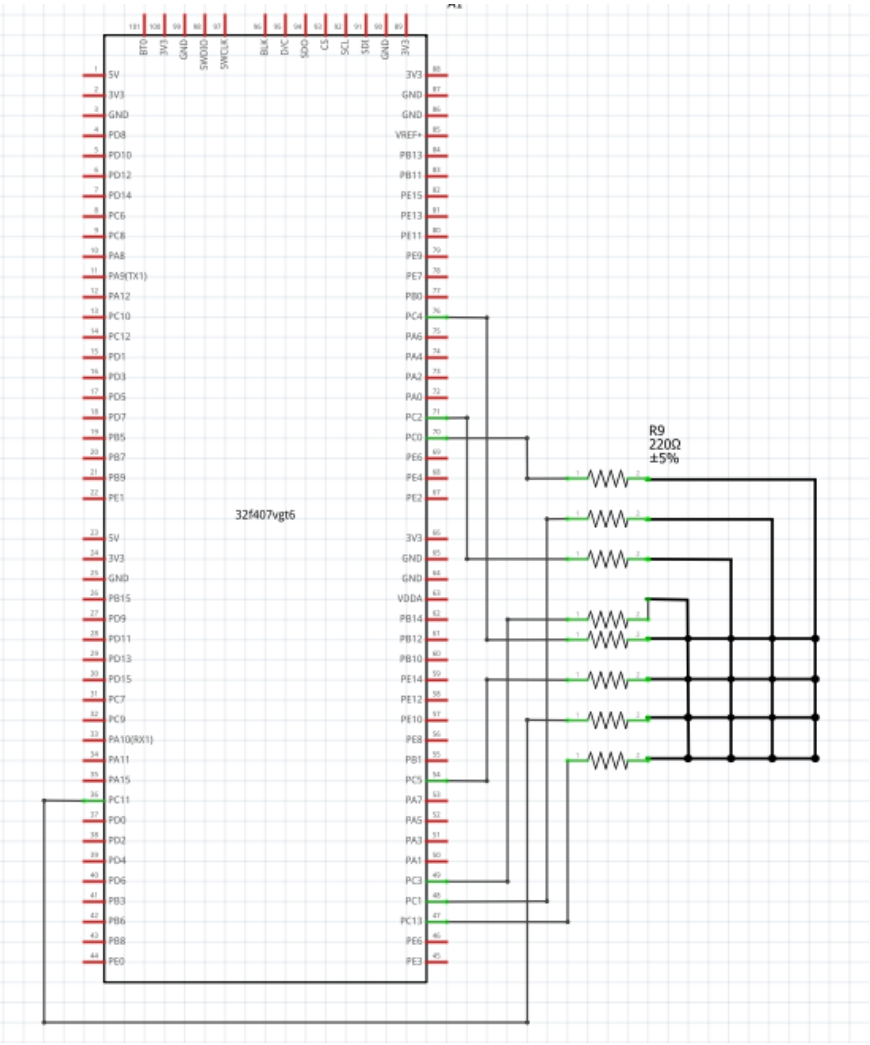


Рисунок 3.4 – Схема з’єднання матричної клавіатури 4x4

Рядки під’єднані до **PC0**, **PC1**, **PC2** та **PC3** як **GPIO_Input**, працюючи на логічному рівні 3.3V і забезпечуючи інтерфейс для зчитування стану рядків.

Стовпці підключаються до **PC4**, **PC5**, **PC11** та **PC13** як **GPIO_Output**, також на рівні 3.3V, і забезпечують активацію стовпців для зчитування стану рядків.

Необхідно було створити алгоритм сканування, який може перевіряти стан кожної клавіші шляхом активації рядків і зчитування сигналів зі стовпців. Це дозволить клавіатурі працювати правильно.

Нижче (рис. 3.5) наведено схему підключення головних модулів у програмі «Fritzing».

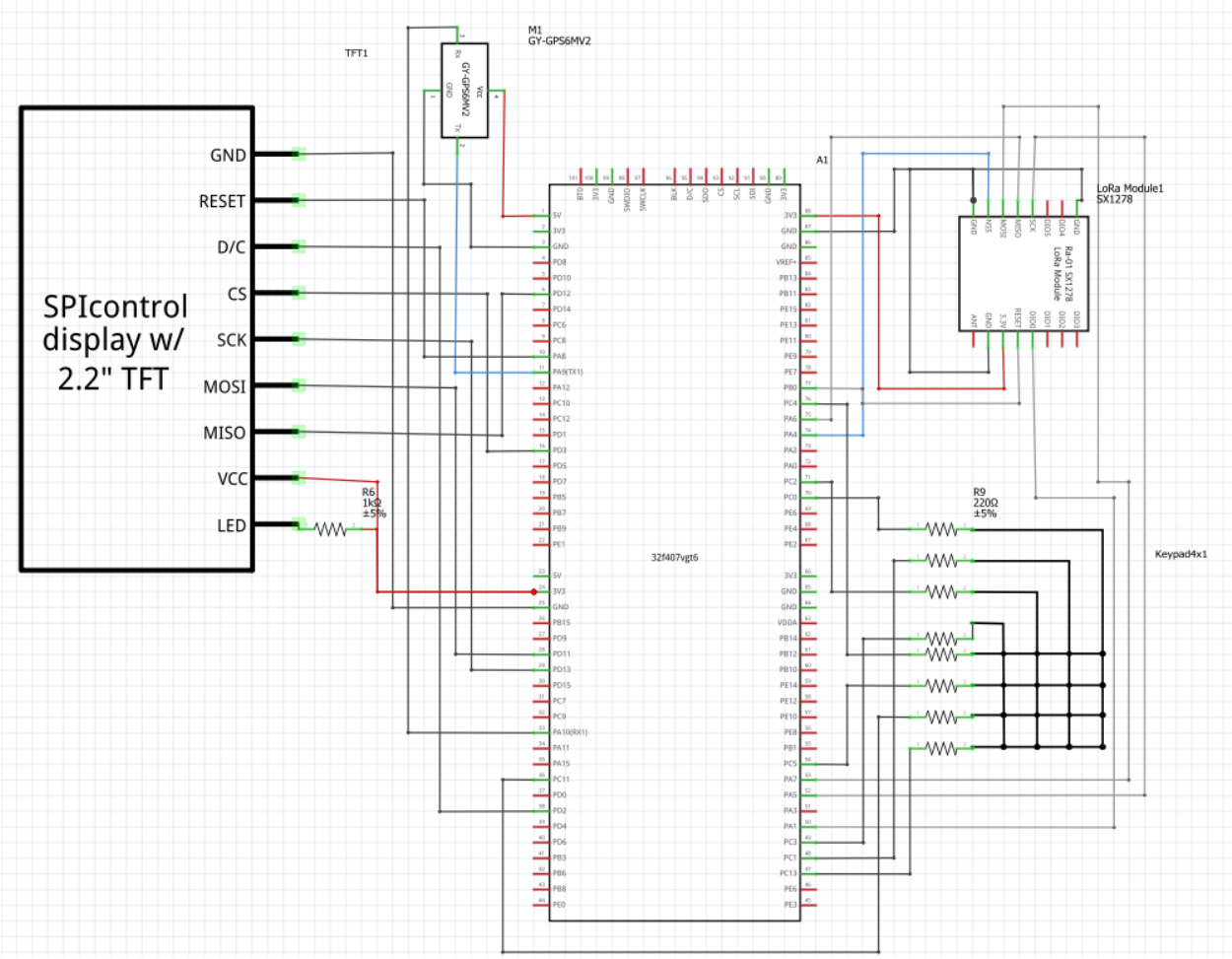


Рисунок 3.5 – Схема з’єднання основних компонентів

Ця схема показує всі з'єднання між мікроконтролером STM32F407VGT6 та основними зовнішніми модулями.

3.2 Розробка модулів програмного забезпечення

Програмне забезпечення було створено за допомогою інтегрованого середовища розробки STM32CubeMX. Це графічний інструмент, який робить конфігурацію МК та мікропроцесорів STM32 надзвичайно простою (рис. 3.6).

Крім того, він дозволяє використовувати покроковий процес для створення відповідного скетчу ініціалізації на мові C для ядра Arm Cortex-M. Одним із перших кроків є вибір між мікропроцесором, мікроконтролером STMicrolectronics STM32 або платформою розробки, яка відповідає необхідному набору периферійних пристроїв, або приладом, який працює на певній платформі розробки [18].

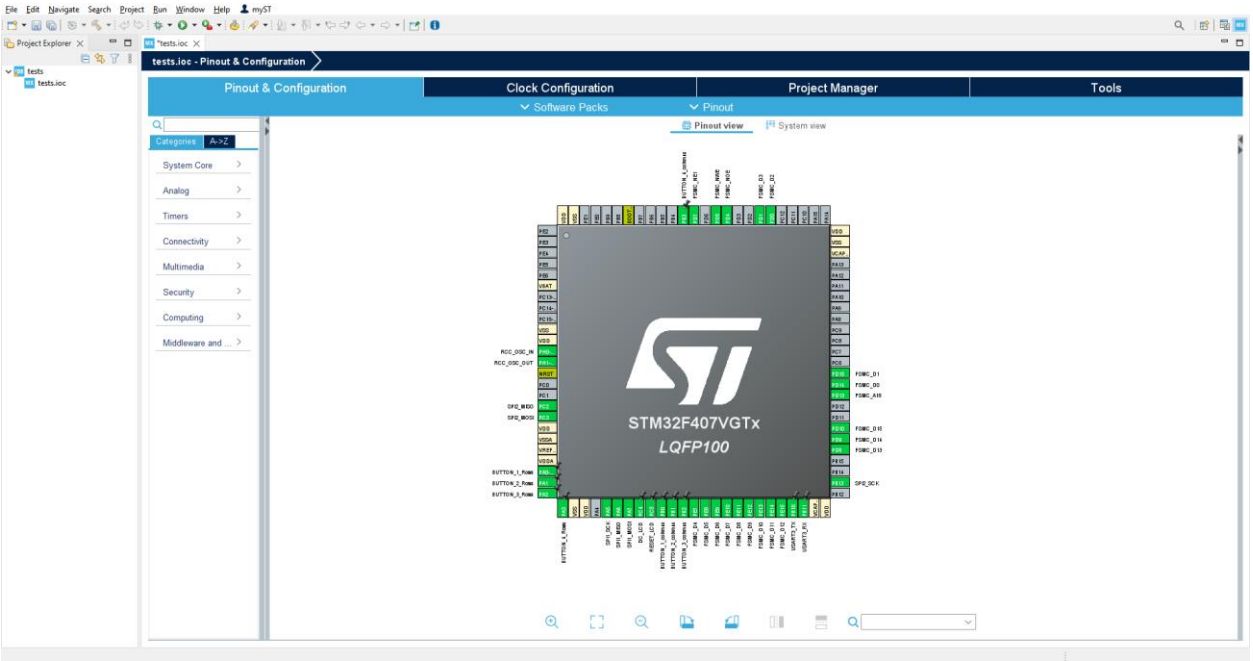


Рисунок 3.6 – Інтерфейс інтегроване середовища розробки STM32CubeMX

Для мікропроцесорів другий крок дозволяє інтерактивно призначити периферію або Arm Cortex -M, а також налаштувати GPIO та годинника для всієї системи. Процес початку роботи з мікропроцесорами STM32 полегшується спеціалізованими утиліти, такими як налаштування та конфігурація DDR. Конфігурація ядра включає додаткові процедури, які точно відповідають інструкціям мікроконтролерів.

Для МК та мікропроцесора Arm Cortex -M другий крок включає налаштування кожного необхідного вбудованого програмного забезпечення за допомогою вирішувача конфлікту, помічника настройки годинника, калькулятора енергоспоживання та утиліти, яка налаштовує периферію

(наприклад, GPIO або USART) та стеки проміжного програмного забезпечення (наприклад, USB або TCP / IP).

Вдосконалені пакети розширення STM32Cube дозволяють розширювати пакети програмного забезпечення, а також пакети проміжного програмного забезпечення. У STM32CubeMX є спеціальний диспетчер пакетів, який дозволяє завантажувати STMicrolectronics або партнерські пакети безпосередньо. Інші пакети можна встановити з локального диска.

3.2.1 Огляд бібліотеки HAL та приклади скетчів

Для коректної роботи всіх підключених модулів до платформою STM32 потрібно підключити всі відповідні бібліотеки, що полегшують процес розробки і забезпечать бажане функціонування модулів.

На сам перед, основною бібліотекою є – «STM32Cube HAL», що надає високорівневі функції для роботи з периферійними пристроями, такими як UART, SPI, I2C, GPIO. Ця бібліотека дозволяє абстрагуватися від низькорівневих деталей роботи з апаратною частиною і зосередитися на основній логікі додатка для забезпечення зручності і ефективність розробки шляхом зменшення необхідного скетчу для взаємодії з апаратними модулями. А також, має функції для керування енергоспоживанням або роботою з перериваннями та конфігурацією додаткових модулів.

Для прикладу було налаштовано і використано SPI для зв'язку з дисплеєм ILI9341, який потім створив початковий скетчу необхідний для роботи з дисплеєм.

Спочатку у вкладці «Pinout & Configuration» було увімкнене SPI1 і призначено піни, що описувалися раніше(рис. 3.7).

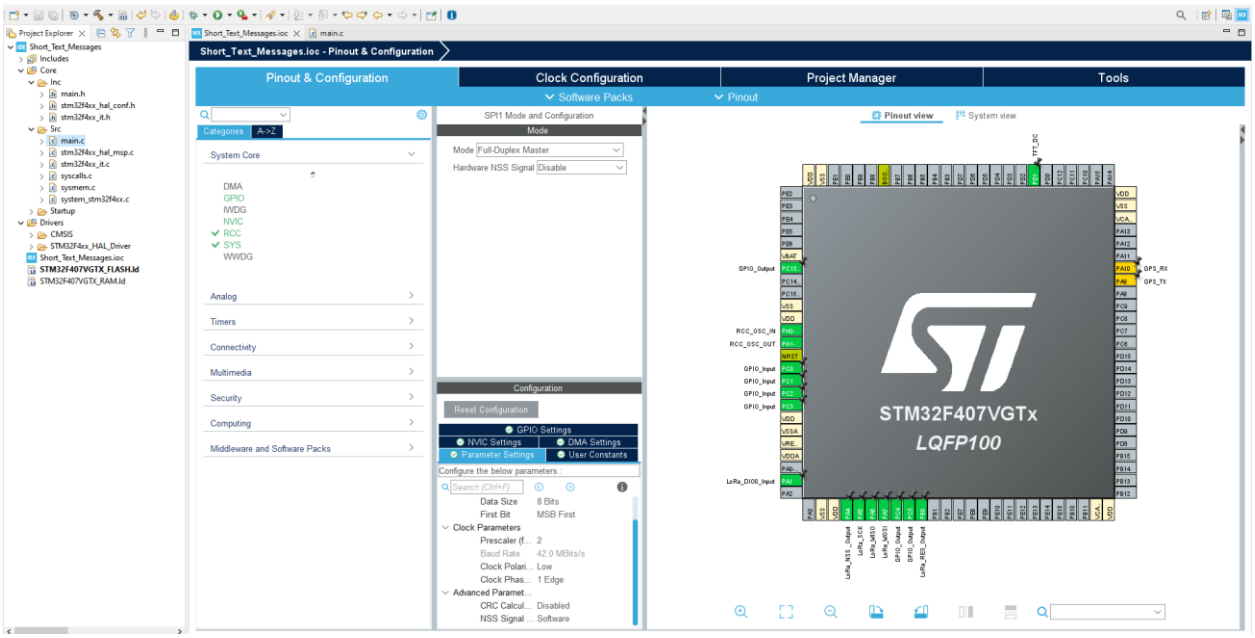


Рисунок 3.7 – Підключення пінів в середовищі STM32CubeMX

Потім у вкладці «Configuration» було налаштовано параметри «Clock Phase» на 1 Edge, також «Clock Polarity» на Low, «Data Size» на 8 Bits, «First Bit» на MSB First та «Mode» на «Full-Duplex Master». І також, було налаштування GPIO для DC і RESET дисплея. Після чого в «Project Manager» було заповнено поля «Project Name» та «Toolchain/IDE», та натиснуто кнопку «Devise Configuration Tool Code Generate» (рис. 3.8).

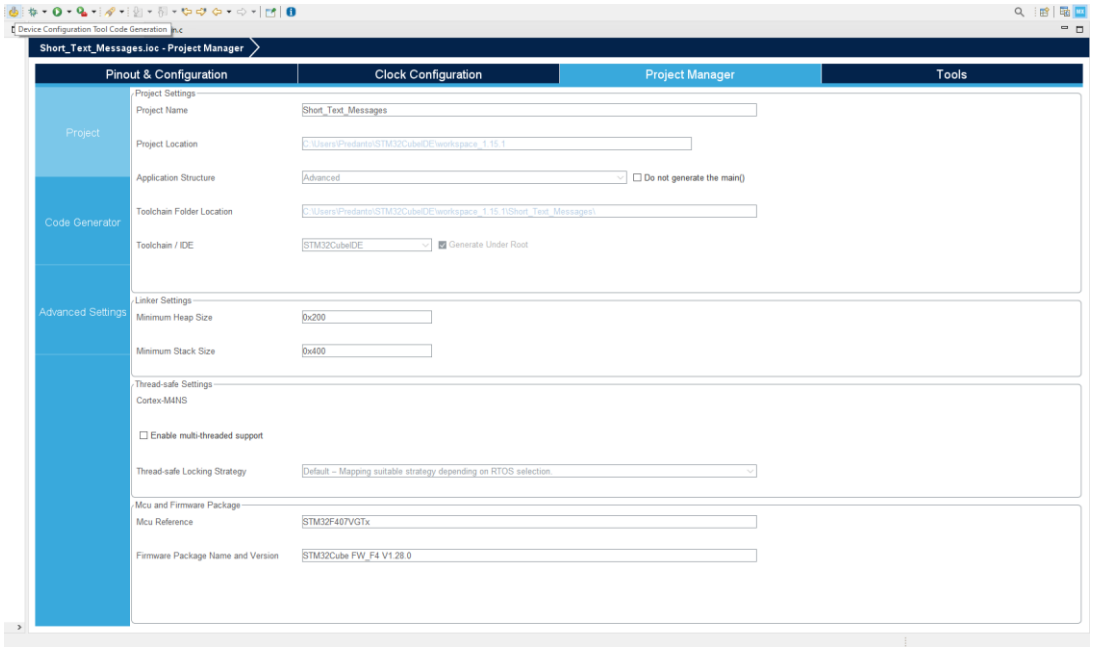


Рисунок 3.8 – Початок генерування скетчу

Після генерації, у файлі «main.c» була створена базова структура та доданий скетч для роботи з дисплеєм ILI9341.

```
int main(void) {
    HAL_Init();
    SystemClock_Config();
    MX_GPIO_Init();
    MX_SPI1_Init();

    ILI9341_Init();

    while (1) {

    }
}

void SystemClock_Config(void) {
    // System Clock Configuration
}
```

Лістинг 3.9 – Приклад вигляду скетчу ініціалізації HAL

У головній функції «main» виконується ініціалізація HAL, системного годинника, GPIO та SPI, та ініціалізація дисплея ILI9341 (ліст. 3.9). Основна програма відбувається у нескінченному циклі, що дозволяє пристрою працювати постійно.

Після йде функція, що конфігурує GPIO піни для роботи з дисплеєм (рис. 3.10).

```
static void MX_GPIO_Init(void) {
    GPIO_InitTypeDef GPIO_InitStruct = {0};

    __HAL_RCC_GPIOD_CLK_ENABLE();
    __HAL_RCC_GPIOA_CLK_ENABLE();

    GPIO_InitStruct.Pin = ILI9341_DC_PIN;
    GPIO_InitStruct.Mode = GPIO_MODE_OUTPUT_PP;
    GPIO_InitStruct.Pull = GPIO_NOPULL;
    GPIO_InitStruct.Speed = GPIO_SPEED_FREQ_LOW;
    HAL_GPIO_Init(ILI9341_DC_PORT, &GPIO_InitStruct);

    GPIO_InitStruct.Pin = ILI9341_RST_PIN;
    HAL_GPIO_Init(ILI9341_RST_PORT, &GPIO_InitStruct);
}
```

Лістинг 3.10 – Приклад вигляду функції ініціалізації GPIO

В ній відбувається ініціалізація піну для DC та RESET сигналу. Це забезпечує коректну роботу з SPI дисплеєм, та дозволяє контролювати режими команди та даних.

```
static void MX_SPI1_Init(void) {
    hspi1.Instance = SPI1;
    hspi1.Init.Mode = SPI_MODE_MASTER;
    hspi1.Init.Direction = SPI_DIRECTION_2LINES;
    hspi1.Init.DataSize = SPI_DATASIZE_8BIT;
    hspi1.Init.CLKPolarity = SPI_POLARITY_LOW;
    hspi1.Init.CLKPhase = SPI_PHASE_1EDGE;
    hspi1.Init.NSS = SPI_NSS_SOFT;
    hspi1.Init.BaudRatePrescaler = SPI_BAUDRATEPRESCALER_16;
    hspi1.Init.FirstBit = SPI_FIRSTBIT_MSB;
    hspi1.Init.TIMode = SPI_TIMODE_DISABLE;
    hspi1.Init.CRCCalculation = SPI_CRCCALCULATION_DISABLE;
    hspi1.Init.CRCPolynomial = 10;
    if (HAL_SPI_Init(&hspi1) != HAL_OK) {
        Error_Handler();
    }
}
```

Лістинг 3.11 – Приклад вигляду функції ініціалізації SPI

Функція, яка наведена на лістингу 3.11, забезпечує ініціалізацію SPI периферії на МК. Вона налаштовує SPI у режим «Master» з параметрами, такими, як полярність і фаза тактового сигналу, розмір даних та швидкість передачі.

```
void ILI9341_SendCommand(uint8_t cmd) {
    HAL_GPIO_WritePin(ILI9341_DC_PORT, ILI9341_DC_PIN, GPIO_PIN_RESET);
    HAL_SPI_Transmit(&hspi1, &cmd, 1, HAL_MAX_DELAY);
}

void ILI9341_SendData(uint8_t data) {
    HAL_GPIO_WritePin(ILI9341_DC_PORT, ILI9341_DC_PIN, GPIO_PIN_SET);
    HAL_SPI_Transmit(&hspi1, &data, 1, HAL_MAX_DELAY);
}
```

Лістинг 3.12 – Приклад вигляду функцій для відправки даних

Функції «*ILI9341_SendCommand*» та «*ILI9341_SendData*» потрібні для відправки команд та даних до дисплея через SPI. «*ILI9341_SendCommand*» – відправляє команду для встановлення DC піну в стан LOW, тоді як «*ILI9341_SendData*» – встановлює DC пін у стан HIGH (ліст. 3.12).

```
void ILI9341_Reset(void) {
    HAL_GPIO_WritePin(ILI9341_RST_PORT, ILI9341_RST_PIN, GPIO_PIN_RESET);
    HAL_Delay(100);
    HAL_GPIO_WritePin(ILI9341_RST_PORT, ILI9341_RST_PIN, GPIO_PIN_SET);
    HAL_Delay(100);
}

void ILI9341_Init(void) {
    ILI9341_Reset();
    ILI9341_SendCommand(0x28); // Display Off
    ILI9341_SendCommand(0xCF);
    ILI9341_SendData(0x00);
    ILI9341_SendData(0x81);
    ILI9341_SendData(0x30);
    ILI9341_SendCommand(0x29); // Display On
}
```

Лістинг 3.13 – Приклад вигляду функцій для скидання дисплею

Функція *«ILI9341_Reset»* виконує скидання дисплея шляхом встановлення піну RESET у стан LOW, а потім у стан HIGH з відповідною затримкою, а функція *«ILI9341_Init»* виконує початкову ініціалізацію дисплея, відправляючи необхідні команди та дані для включення дисплея та його налаштування (ліст. 3.13).

3.2.2 Модуль передачі та прийому текстових повідомлень

Перший етап робочого процесу включає введення текстового повідомлення за допомогою інтерфейсу користувача. Оператор використовує клавіатуру для набору повідомлення, яке відображається на дисплеї пристрою в реальному часі. Це дозволяє перевірити правильність введення та внести необхідні корективи перед відправкою.

Інтерфейс повинен інтуїтивно зрозумілим і зручним, щоб мінімізувати час, необхідний для введення повідомлення, особливо в стресових умовах бойових дій.

Оскільки використовується матричний тип клавіатури із 16-кнопками, де 10 цифр, 2 символи і 4 літери, то було прийнято рішення використовувати та створити систему кодів для відправки коротких повідомлень.

Військові часто використовують метод кодування інформації для передавання команд, тому, ця система кодів значно скоротить час при ведені

та відправці повідомлень, а також зменшить кількість помилок при ведені того повідомлення, яке зашифроване в ньому (табл. 3.1).

Таблиця 3.1 – Приклади кодів які були задіяні в проєкті

Категорія	Код	Опис
Командні повідомлення	A1	Атакувати позицію 1
	B2	Відступити з позиції 2
	C3	Перегрупуватися в точці 3
	D4	Надати медичну допомогу
	*5	Запит підтримки
Інформаційні повідомлення	#10	10 ворожих солдатів
	#T2	2 танки, мої координати
	#P3	3 поранених, мої координати
	#A	Координати
Підтверджуючі повідомлення	*A	Команда отримана
	#B	Команда виконана
	*C	Повідомлення отримано

Окрім цього, самі повідомлення будуть зашифровані методом шифрування в mbedTLS, що забезпечить високий захист від дешифрування перехоплених ворогом повідомлень [6].

Нижче наведено блок-схему, яка описує алгоритм роботи приладу (рис. 3.14).

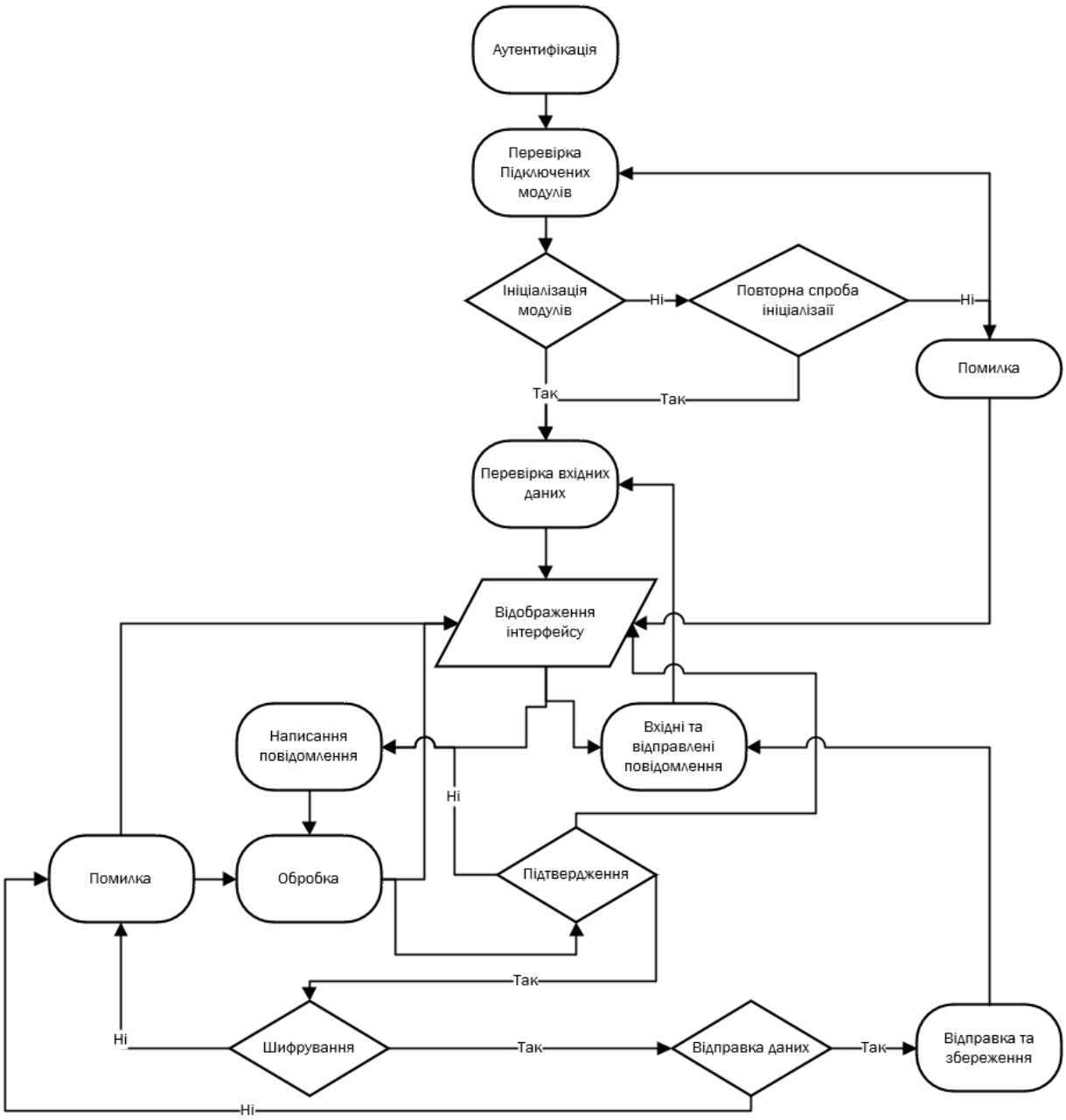


Рисунок 3.14 – Блок схема алгоритму роботи приладу

В ньому описується алгоритм роботи приладу, що починається з аутентифікації користувача у вигляді паролю, за для забезпечення безпеки доступу до системи, ініціалізації всіх компонентів, перевірки на наявність нових повідомлень та відображення інтерфейсу з написанням повідомлення чи перегляду вхідних.

При написані оператором повідомлення, відбувається обробка повідомлення, яка також відображає на екрані смислові речення, що були

створені оператором за допомогою кодових слів. Після чого, оператор перевіряє та підтверджує на відправу повідомлення, натисканням відповідної клавіші, де дані шифруються і відправляються (ліст. 3.15).

```
{
  "message_type": "command",
  "sender_id": "12345",
  "recipient_id": "67890",
  "timestamp": 1655431200,
  "data": {
    "command_code": "*C",
    "coordinates": {
      "latitude": 48.4651,
      "longitude": 32.0432
    }
  }
}
```

Лістинг 3.15 – Приклад відправлених даних

Також, оператор може перевірити наявність нових повідомлень, які дешифровані та вже відображаються у вигляді зрозумілого тексту, без кодових символів.

3.2.3 Модуль шифрування та дешифрування за допомогою mbedTLS

Для забезпечення безпеки передачі було застосовано бібліотеку «mbedTLS». Ця бібліотека забезпечує надійне шифрування та дешифрування текстових повідомлень, що передаються між пристроями [21-24].

Завдяки бібліотеці «mbedTLS», було реалізовано функції для шифрування та дешифрування текстових повідомлень у реальному часі, що забезпечує безпечну передачу даних між пристроями. За основу було використано алгоритм AES-128 для симетричного шифрування текстових повідомлень.

Спочатку було додано необхідні бібліотеки mbedTLS для роботи з AES, та визначено розмір ключа для AES-128 і блоку даних (ліст.3.16).

```
#include "mbedtls/aes.h"
#include "mbedtls/entropy.h"
#include "mbedtls/ctr_drbg.h"
#include "string.h"

#define KEY_SIZE 16 // AES-128
#define BLOCK_SIZE 16

static mbedtls_aes_context aes;
static mbedtls_entropy_context entropy;
static mbedtls_ctr_drbg_context ctr_drbg;
static unsigned char key[KEY_SIZE];
static unsigned char iv[BLOCK_SIZE];
```

Лістинг 3.16 – Додавання бібліотек для генерації ключів

Потім було додано статичні змінні для контекстів шифрування AES, а також для ключа та вектора ініціалізації, та створено функцію «*encryption_init*» для ініціалізації їх (ліст. 3.17). Після чого, було визначено персоналізатор і викликано функцію «*mbedtls_ctr_drbg_seed*» для ініціалізації генератора випадкових чисел. Згенеровано ключ і вектор ініціалізації за допомогою функції «*mbedtls_ctr_drbg_random*».

```
void encryption_init() {
    mbedtls_aes_init(&aes);
    mbedtls_entropy_init(&entropy);
    mbedtls_ctr_drbg_init(&ctr_drbg);

    const char *pers = "aes_generate_key";
    mbedtls_ctr_drbg_seed(&ctr_drbg, mbedtls_entropy_func, &entropy, (const unsigned char *)pers, strlen(pers));

    mbedtls_ctr_drbg_random(&ctr_drbg, key, KEY_SIZE);
    mbedtls_ctr_drbg_random(&ctr_drbg, iv, BLOCK_SIZE);
}
```

Лістинг 3.17 – Створення функції для ініціалізації контекстів шифрування

Слідом створено функцію «*encrypt_message*», що приймає вхідне повідомлення і вихідний буфер та довжину повідомлення (ліст. 3.18).

```
void encrypt_message(const unsigned char *input, unsigned char *output, size_t length) {
    mbedtls_aes_setkey_enc(&aes, key, KEY_SIZE * 8);
    mbedtls_aes_crypt_cbc(&aes, MBEDTLS_AES_ENCRYPT, length, iv, input, output);
}

void decrypt_message(const unsigned char *input, unsigned char *output, size_t length) {
    mbedtls_aes_setkey_dec(&aes, key, KEY_SIZE * 8);
    mbedtls_aes_crypt_cbc(&aes, MBEDTLS_AES_DECRYPT, length, iv, input, output);
}
```

Лістинг 3.18 – Створення функції шифрування та дешифрування

У цій функції було встановлено ключ для шифрування за допомогою функції «*mbedtls_aes_setkey_enc*», а потім було зашифровано повідомлення за допомогою «*mbedtls_aes_crypt_cbc»*. За такою ж аналогією виконується функція «*decrypt_message*» приймаючи зашифроване повідомлення, а також вихідний буфер та довжину повідомлення. Встановлено ключ для дешифрування за допомогою «*mbedtls_aes_setkey_dec*», а потім було дешифровано повідомлення за допомогою «*mbedtls_aes_crypt_cbc*».

3.3 Розробка інтерфейсу пристрою

Для створення та перевірки інтерфейсу було використано онлайн - симулятор електроніки – «Wokwi» [20]. Завдяки цьому сервісу можна імітувати найпопулярніші МК, та багатьох популярних плат, деталей та датчиків.

В онлайн – симуляторі «Wokwi», було розроблено приклади інтерфейсу для дисплейного модуля ILI9341, що будуть використані в подальшому, як шаблон для відображення, що відображає різні екрани та меню для керування пристроєм.

Отже, було створено екран авторизації, де оператор вводить пароль за допомогою матричної клавіатури (рис. 3.19).

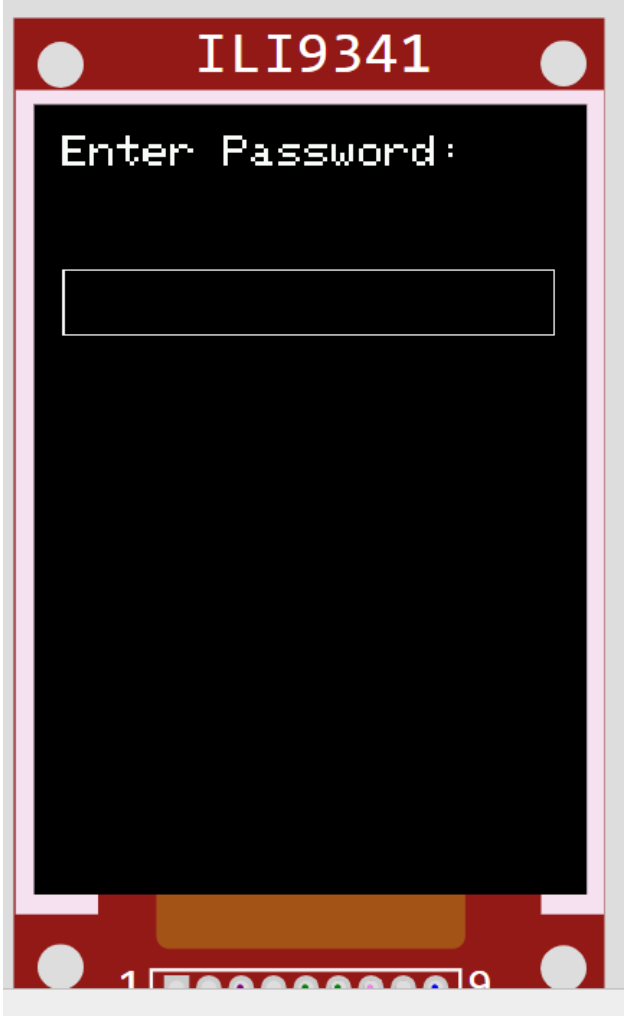


Рисунок 3.19 – Концепт інтерфейсу авторизації

Матрична клавіатура відіграє дуже важливу роль в взаємодії з інтерфейсом. Як було описано раніше, клавіатура має 10 цифр, 2 символи та 4 літери, що достатньо для взаємодії з інтерфейсом.

Для взаємодії були призначені відповідні кнопки, а саме, кнопка з цифрою «5» не лише для ведення кодових фраз, але й для підтвердження дій, для того щоб застосувати підтвердження, потрібно два рази натиснути на неї, це буде свідчити про взаємодію із кнопки що зображена в інтерфейсі. Також кнопки з позначками – «4 – «←»; 2 – «↑»; 6 – «→»; 8 – «↓»», відповідають за переміщенням між активними полями інтерфейсу (рис. 3.20).

Рисунок 3.20 – Вигляд розміщення стрілок керування на клавіатурі

Після введення правильного пароля, користувач переходить до головного меню. Це меню містить індикатори сигналу, стану батареї та координат пристрою, які відображаються у всіх подальших меню. Крім того, у головному меню відображається останнє вхідне повідомлення та три кнопки: вхідні повідомлення, відправити повідомлення та налаштування (рис. 3.21).

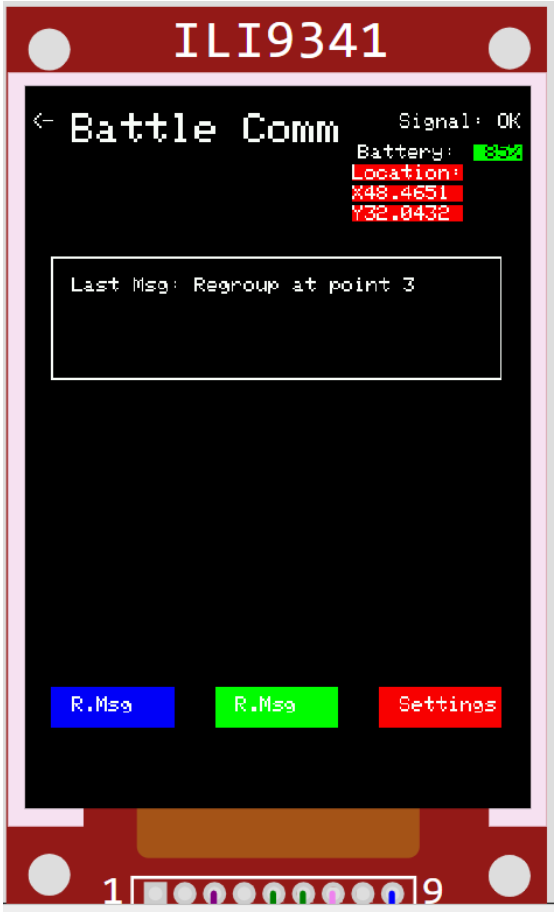


Рисунок 3.21 – Концептуальний вигляд головного меню

При натисканні кнопки «Вхідні повідомлення» відображається меню зі списком усіх отриманих повідомлень. Непрочитані повідомлення виділяються зеленим фоном, а прочитані – красним (рис. 3.22).

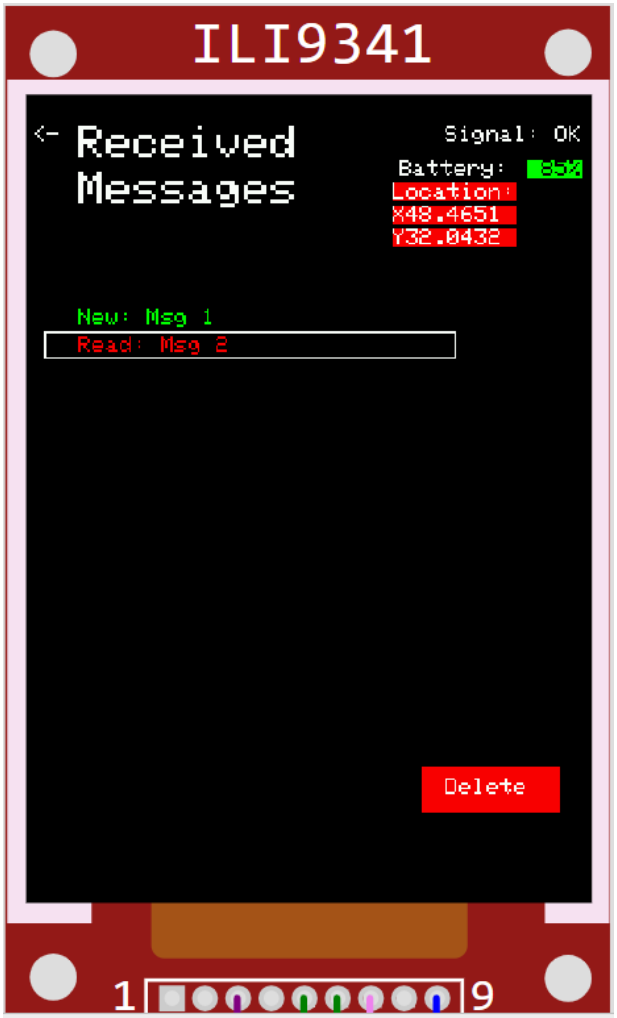


Рисунок 3.22 – Меню «Вхідні повідомлення»

У верхньому лівому куті розташована кнопка «Назад», яка дозволяє повернутися до попереднього меню. Внизу екрану розміщена кнопка «Видалити», яка дозволяє очистити прочитані повідомлення.

При виборі конкретного повідомлення здійснюється переходи до екрану з детальним відображенням повідомлення (рис. 3.23).

Рисунок 3.23 – Меню детального відображення повідомлень

Тут можна повністю прочитати повідомлення та відразу написати відповідь за допомогою кнопки, розташованої внизу справа. Натискання цієї кнопки переводить до екрану для написання повідомлення.

На екрані написання повідомлення є дві рамки для тексту: одна для введення кодів, інша для автоматичного відображення їх значень (рис. 3.24).

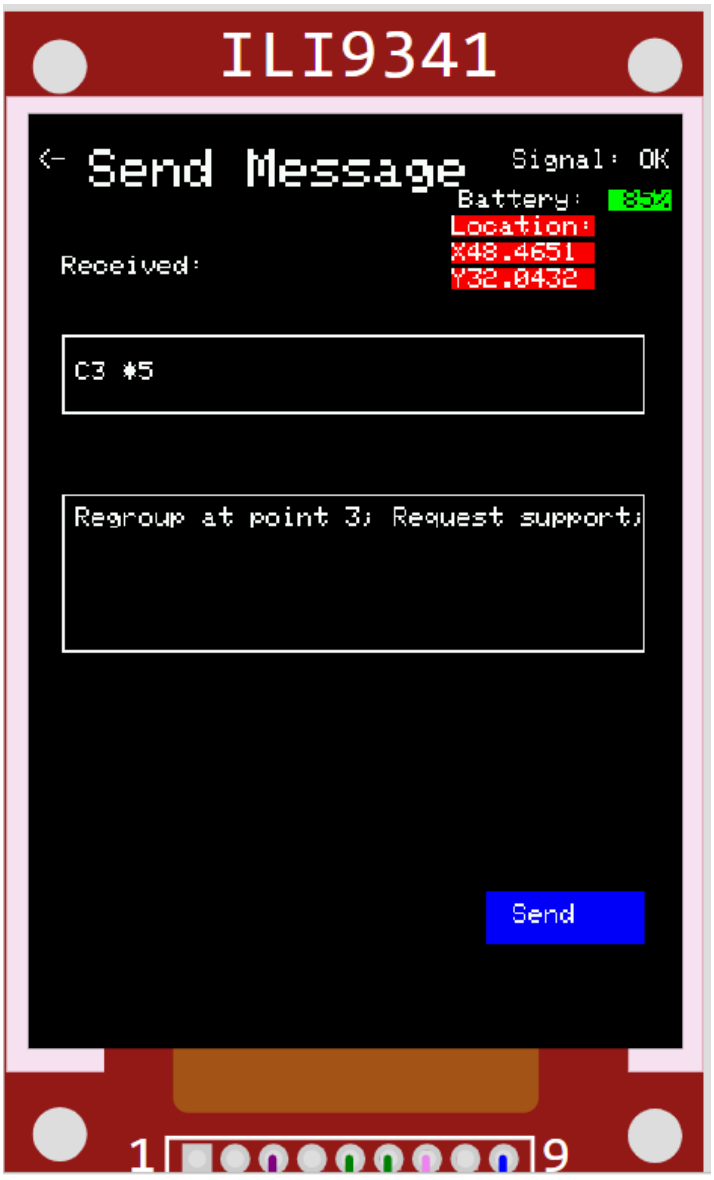


Рисунок 3.24 – Меню написання повідомлення

Для того щоб видалити неправильно ведені дані, потрібно натиснути на клавіатурі відповідну кнопку, за це відповідає кнопка «D», що теж може слугувати для ведення тексту, щоб примінити цю функцію потрібно два бистрих рази натиснути на неї, це змусить видалити ведений текст, але лише по символьно.

У верхньому лівому куті розташована кнопка «Назад», яка повертає до попереднього меню, також внизу розміщена кнопка «Відправити», яка дозволяє відправити створене повідомлення.

Повернувшись назад до головного меню, розміщена кнопка «Налаштування», що забезпечить перехід до екрану налаштувань (рис. 3.25).

Рисунок 3.25 – Меню налаштувань

В меню налаштувань є функції завдяки яким відбувається налаштуваня зв'язку чи GPS, зміна паролю чи перевірка журнал помилок. Це меню забезпечує доступ до важливих параметрів і дозволяє налаштовувати пристрій відповідно до потреб оператора.

Висновки до розділу 3

У третьому розділі було проведено детальне проектування апаратної частини та розробку програмного забезпечення апаратно-програмного комплексу.

Була розроблена схема підключення елементів пристрою з використанням МК «STM32F407VGT6», який забезпечує високу обчислювальну потужність та гнучкість у підключенні різних модулів.

Було створено алгоритм сканування матричної клавіатури, який дозволяє правильно зчитувати натискання кнопок. Додатково було розроблено модуль програмного забезпечення, який забезпечує передачу та прийом текстових повідомлень з можливістю шифрування та дешифрування за допомогою бібліотеки mbedTLS. Для реалізації цієї функції було використано алгоритм AES-128, що гарантує високий рівень захисту від перехоплення.

Розроблено інтерфейс користувача, де було використано онлайн-симулятор електроніки «Wokwi», що дозволило створити концептуальні екрани інтерфейсу.

ВИСНОВКИ

Дипломна робота була присвячена розробці апаратно-програмного комплексу для координації дій військових на полі бою за допомогою коротких текстових повідомлень. Аналіз існуючих систем координації виявив значні недоліки, які виникають в умовах швидкоплинних бойових дій. Традиційні системи військового зв'язку, засновані на радіопередачі, не завжди можуть забезпечити необхідний рівень надійності та безпеки, особливо в умовах активної радіоелектронної боротьби.

Для подолання цих обмежень, було розроблено комплекс, що ґрунтується на потужному 32-бітному мікроконтролері STM32F407VGT6. STM32F407VGT6 забезпечує високу обчислювальну потужність та гнучкість в роботі, дозволяючи ефективно обробляти шифровані повідомлення, управляти складними комунікаційними протоколами та інтегрувати різноманітні модулі.

Для бездротової передачі даних комплекс використовує технологію LoRa, яка забезпечує високу дальність передачі та низьке енергоспоживання. Крім того, комплекс оснащений дисплейним модулем, що дозволяє оператору зручно взаємодіяти з пристроєм та візуалізувати отримані дані. Додатково було реалізовано систему відстеження координат за допомогою GPS-модуля, що дозволяє командирам отримувати точну інформацію про розташування підрозділів.

Розроблений комплекс має значне теоретичне значення. Він демонструє новий підхід до координації дій військових, враховуючи специфічні вимоги сучасної війни та загрози інформаційній безпеці. Завдяки використанню STM32F407VGT6 та технології LoRa, комплекс забезпечує високу продуктивність, надійність та безпеку обміну інформацією в умовах обмежених ресурсів та дії засобів радіоелектронної протидії.

Розроблений прототип має високе практичне значення. Його використання дозволить:

– збільшити швидкість та ефективність обміну інформацією, що забезпечить оперативне управління підрозділами та швидке реагування на зміни обстановки;

– підвищити рівень інформаційної безпеки шляхом надійного захисту від перехоплення та фальсифікації переданих даних;

– збільшити мобільність та автономність військових підрозділів, забезпечивши можливість використовувати комплекс на різних типах бойової техніки та легко переносити його військовими;

– створити єдину систему управління бойовими діями, інтегруючи комплекс з іншими системами координації дій та управління.

Виконана робота є важливим внеском у розвиток сучасних систем військового зв'язку та координації дій. Вона сприяє підвищенню ефективності бойових дій та забезпеченню необхідного рівня інформаційної безпеки в сучасних умовах.

Проте, подальші розробки та дослідження є перспективними для вдосконалення комплексу. Наприклад, можливо розширити функціонал програмного забезпечення, додавши можливості для голосового зв'язку або передачі фото- та відеоданих. Доцільним є також дослідження інтеграції комплексу з іншими сучасними технологіями, такими як системи штучного інтелекту, дронові технології або розвідувальні системи.

Збільшення рівня криптографічного захисту переданої інформації також потребує подальших досліджень. Нарешті, проведення тестування комплексу в реальних умовах дозволить перевірити його ефективність та надійність.

У цілому, розроблений комплекс має значний потенціал для використання в сучасних військових операціях, сприяючи підвищенню ефективності та безпеки дій військових підрозділів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Гаврилюк А. В. Апаратні засоби захисту інформації в умовах сучасних військових конфліктів. Воєнна наука і техніка; Нац. ун-т оборони України. 2020. Вип. 41. С. 132-140.

2. Військовий стандарт 01.112.001–2006. Зв'язок у Збройних Силах України. Терміни та визначення. – Київ: Міністерство оборони України, 2006. С. 32–37.

3. Доценко С. В. Захист інформації в автоматизованих системах. – Київ: Видавничий дім «Академперіодика», 2011. 480 с.

4. Петров В. В. Інформаційна безпека держави. – Київ: Знання, 2010. 287 с.

5. Кузнецов А. Ю. «Проблеми забезпечення інформаційної безпеки в сучасних умовах», Науковий вісник Національного університету оборони України, 2018. № 2. С. 85-92.

6. Іванов І. О. Використання криптографічних методів для захисту даних у військових системах зв'язку. Військова техніка і технології; Київ. нац. ун-т оборони. 2018. Вип. 25. С. 45-53.

7. Сидоренко С. М. Інтеграція криптографічних бібліотек в системи обміну повідомленнями. Кібербезпека та інформаційні технології; Дніпров. держ. техн. ун-т. 2019. Вип. 33. С. 75-82.

8. Малярчук М. В. Сучасні проблеми інформаційного забезпечення автоматизованих систем управління тактичної ланки Збройних Сил України / М. В. Малярчук, С. П. Колачов, Ю. П. Недайбіда, О. В. Драглюк // Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2009. – Вип. № 3. – С. 40–44.

9. Кузьменко О.В., Лисицький В.Ф. Аналіз сучасних засобів криптографічного захисту інформації. - Збірник наукових праць Військового інституту телекомунікацій та інформатизації, 2020, № 1, с. 67-74.

10. Омельчук Л.О., Павлов В.В. Проблеми забезпечення інформаційної безпеки в сучасних системах зв'язку. - Вісник Національного університету оборони України, 2021, № 4, с. 104-111.

11. Кушнір В.О. Перспективи розвитку та застосування мереж LoRaWAN у військовій сфері. - Наука і оборона, 2022, № 1, с. 43-49.

12. Зацеркляний М.М., Мельник А.О. Інформаційна безпека: основи теорії та практики. Навчальний посібник. - Львів: ЛНУ ім. І. Франка, 2018. - 304 с.

13. Шевченко В. О. Системний підхід до розроблення методологічних основ дослідження телекомунікаційних мереж військового призначення / В. О. Шевченко // Наука і оборона. – 2004. № 4. С. 42–46.

14. Павловський В.В., Литвиненко О.Є., Пасічник В.В. Захист інформації в комп'ютерних системах. Навчальний посібник. - Харків: ХНУРЕ, 2019. - 460 с.

15. Баранов В.М., Хоменко І.В. Мікроконтролери AVR: від простого до складного. - Львів: ЛНУ ім. Івана Франка, 2019. - 400 с.

16. Гузик В.Ф., Зайченко С.А., Кавун С.В. Мікропроцесорні системи на базі мікроконтролерів STM32. - Київ: КПІ ім. Ігоря Сікорського, 2020. - 320 с.

17. Доценко С.В., Коломоець О.В. Захист інформації в автоматизованих системах. - Київ: Видавничий дім "Академперіодика", 2011. - 480 с.

18. Ковальов А.В., Ткаченко О.М. Розробка програмного забезпечення для мікроконтролерних систем управління з використанням середовища STM32CubeIDE. - Вісник Національного технічного університету України "Київський політехнічний інститут", 2021, № 1, с. 85-92.

19. Інформаційно-керуючі системи на залізничному транспорті: Матеріали XII Міжнародної науково-практичної конференції (Харків, 2022). - Харків: УкрДАЗТ, 2022.

20. Корнієнко А.А., Коваленко О.І. Розробка інтерфейсу користувача для вбудованих систем з використанням графічних дисплеїв. - Вісник

Харківського національного університету радіоелектроніки, 2020, № 4, С. 72 - 79.

21. Cormen T., Leiserson Ch., Rivest R. and Stein C. Introduction to algorithms, fourth edition.: MIT Press, 2022. – 1332 p. 1312 p.

22. Ozdemir, S., Yavuz, A. G. A comprehensive overview of wireless sensor network applications in military environments. - Journal of Network and Computer Applications, 2017, vol. 97, pp. 108-120.

23. Fuchs, G., Fuchs, M., Socek, D., & Mares, P. Military communication systems: Current state and challenges. - Radioengineering, 2020, vol. 29, no. 2, pp. 334-345.

24. Kotenko, I. V., Kushnir, V. O., & Kushnir, O. V. Military communication: Current state and development prospects. - Eastern-European Journal of Enterprise Technologies, 2021, vol. 1, no. 7 (109), pp. 6-14.

25. Sharma, R. K., & Sharma, P. LoRaWAN: A survey on architecture, security, and applications. - Wireless Personal Communications, 2023, vol. 128, no. 3, pp. 2403-2433

26. Joseph Yiu. The Definitive Guide to ARM® Cortex®-M3 and Cortex®-M4 Processors. - Newnes, 2018. – 672 p.

27. Richard Barnett, Sarah Cox, Larry O'Cull. Embedded C Programming and the Atmel AVR. - Delmar Cengage Learning, 2009. - 752 p.

28. Han-Way Huang. STM32 ARM Programming for Embedded Systems. - Packt Publishing, 2015. - 436 p.

29. Simon Monk. Programming Arduino: Getting Started with Sketches. - McGraw-Hill Education, 2016. - 288 p.

30. Mazidi M.A., McKinlay R.D., Causey D. The 8051 Microcontroller and Embedded Systems: Using Assembly and C. - Pearson Education, 2013. - 672 p.

ДОДАТОК А.

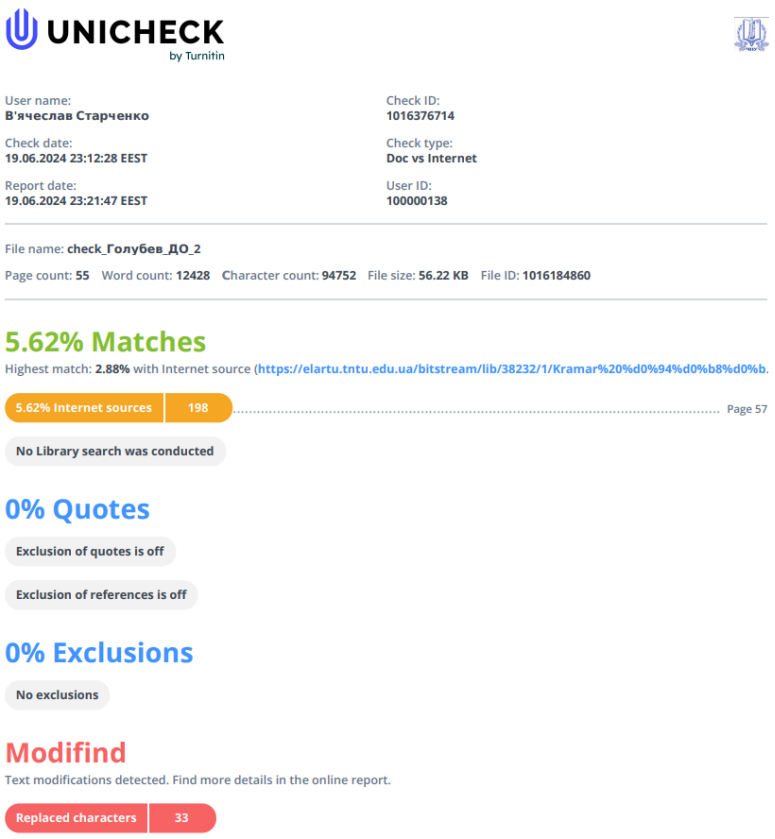
Довідка про перевірку на унікальність пояснювальної записки

бакалаврської кваліфікаційної роботи на тему:
«Апаратно-програмний комплекс для координації дій на полі бою
за допомогою коротких текстових повідомлень»

студента спеціальності 123 «Комп'ютерна інженерія», 405 групи
Голубев Денис Олександрович
прізвище, ім'я, по-батькові

Перевірку тексту здійснено сервісом: онлайн-сервіс Unicheck

Результат перевірки тексту бакалаврської кваліфікаційної роботи: схожість складає 5,62%.



UNICHECK
by Turnitin

User name: В'ячеслав Старченко
Check ID: 1016376714
Check date: 19.06.2024 23:12:28 EEST
Check type: Doc vs Internet
Report date: 19.06.2024 23:21:47 EEST
User ID: 100000138

File name: check_Голубев_ДО_2

Page count: 55 Word count: 12428 Character count: 94752 File size: 56.22 KB File ID: 1016184860

5.62% Matches

Highest match: 2.88% with Internet source (https://elartu.tntu.edu.ua/bitstream/lib/38232/1/Kramar%20%d0%94%d0%b8%d0%b.

5.62% Internet sources 198 ..... Page 57

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters 33

Здобувач:

_____ Д. О. Голубев
підпис ініціали, прізвище

Керівник:

ст. викладач

_____ В. В. Старченко
підпис ініціали, прізвище

Дата: «___» _____ 2024 р.

ДОДАТОК Б. Скетч модулів

```
#include "stm32f4xx_hal.h"
#include "spi.h"
#include "gpio.h"
#include "ILI9341.h"

#define ROW1_PIN GPIO_PIN_2
#define ROW1_PORT GPIOA
#define ROW2_PIN GPIO_PIN_12
#define ROW2_PORT GPIOA
#define ROW3_PIN GPIO_PIN_11
#define ROW3_PORT GPIOA
#define ROW4_PIN GPIO_PIN_1
#define ROW4_PORT GPIOA

#define COL1_PIN GPIO_PIN_11
#define COL1_PORT GPIOB
#define COL2_PIN GPIO_PIN_1
#define COL2_PORT GPIOB
#define COL3_PIN GPIO_PIN_0
#define COL3_PORT GPIOF
#define COL4_PIN GPIO_PIN_1
#define COL4_PORT GPIOF

void Display_MainInterface(void);
void Display_Menu(void);
void Display_Settings(void);
void Display_Errors(void);
void Scan_Keypad(void);

enum State { MAIN_INTERFACE, MENU, SETTINGS, ERRORS } currentState =
MAIN_INTERFACE;

void HAL_GPIO_EXTI_Callback(uint16_t GPIO_Pin) {

    if (GPIO_Pin == GPIO_PIN_0) {
        if (currentState == MAIN_INTERFACE) {
            currentState = MENU;
            Display_Menu();
        } else if (currentState == MENU) {
            currentState = MAIN_INTERFACE;
            Display_MainInterface();
        }
    } else if (GPIO_Pin == GPIO_PIN_1) {
        if (currentState == MENU) {
            currentState = SETTINGS;
            Display_Settings();
        } else if (currentState == SETTINGS) {
```

```
            currentState = ERRORS;
            Display_Errors();
        } else if (currentState == ERRORS) {
            currentState = MAIN_INTERFACE;
            Display_MainInterface();
        }
    }
}

void Display_MainInterface(void) {

    ILI9341_FillScreen(ILI9341_BLACK);

    ILI9341_SetCursor(10, 10);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_BLACK);
    ILI9341_SetTextSize(2);
    ILI9341_WriteString("Battle Comm", ILI9341_WHITE);

    ILI9341_SetCursor(10, 50);
    ILI9341_SetTextSize(1);
    ILI9341_WriteString("Received:", ILI9341_GREEN);

    ILI9341_DrawRect(10, 70, 220, 60, ILI9341_WHITE);

    ILI9341_SetCursor(15, 75);
    ILI9341_WriteString("C3 *5", ILI9341_WHITE);

    ILI9341_DrawRect(10, 140, 220, 60, ILI9341_WHITE);

    ILI9341_SetCursor(15, 145);
    ILI9341_WriteString("Regroup at point 3;", ILI9341_WHITE);
    ILI9341_SetCursor(15, 160);
    ILI9341_WriteString("Request support;", ILI9341_WHITE);

    ILI9341_FillRect(10, 290, 100, 20, ILI9341_BLUE);
    ILI9341_SetCursor(40, 295);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_BLUE);
    ILI9341_WriteString("Send", ILI9341_WHITE);

    ILI9341_FillRect(120, 290, 100, 20, ILI9341_RED);
    ILI9341_SetCursor(150, 295);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_RED);
    ILI9341_WriteString("Menu", ILI9341_WHITE);

    ILI9341_SetCursor(180, 10);
    ILI9341_SetTextSize(1);
    ILI9341_WriteString("Signal:", ILI9341_YELLOW);
    ILI9341_SetTextColor(ILI9341_BLACK, ILI9341_GREEN);
    ILI9341_SetCursor(218, 10);
```

```
    ILI9341_WriteString("OK", ILI9341_GREEN);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_RED);
    ILI9341_SetCursor(160, 25);
    ILI9341_WriteString("Battery:", ILI9341_WHITE);
    ILI9341_SetTextColor(ILI9341_BLACK, ILI9341_GREEN);
    ILI9341_SetCursor(216, 25);
    ILI9341_WriteString("85%", ILI9341_GREEN);

    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_RED);
    ILI9341_SetCursor(157, 35);
    ILI9341_WriteString("Location:", ILI9341_WHITE);

    ILI9341_SetCursor(157, 45);
    ILI9341_WriteString("X48.4651", ILI9341_WHITE);

    ILI9341_SetCursor(157, 55);
    ILI9341_WriteString("Y32.0432", ILI9341_WHITE);
}

void Display_Menu(void) {

    ILI9341_FillScreen(ILI9341_BLACK);

    ILI9341_SetCursor(10, 10);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_BLACK);
    ILI9341_SetTextSize(2);
    ILI9341_WriteString("Settings Menu", ILI9341_WHITE);

    ILI9341_SetCursor(10, 50);
    ILI9341_SetTextSize(1);
    ILI9341_WriteString("1. Disable GPS", ILI9341_WHITE);
    ILI9341_SetCursor(10, 70);
    ILI9341_WriteString("2. Change Password", ILI9341_WHITE);
    ILI9341_SetCursor(10, 90);
    ILI9341_WriteString("3. View Errors", ILI9341_WHITE);

    ILI9341_FillRect(10, 290, 100, 20, ILI9341_BLUE); // кнопка відправки
    ILI9341_SetCursor(40, 295);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_BLUE);
    ILI9341_WriteString("Select", ILI9341_WHITE);

    ILI9341_FillRect(120, 290, 100, 20, ILI9341_RED); // кнопка навігації
    ILI9341_SetCursor(150, 295);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_RED);
    ILI9341_WriteString("Back", ILI9341_WHITE);
}

void Display_Settings(void) {
```

```
    ILI9341_FillScreen(ILI9341_BLACK);

    ILI9341_SetCursor(10, 10);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_BLACK);
    ILI9341_SetTextSize(2);
    ILI9341_WriteString("Settings", ILI9341_WHITE);

    ILI9341_SetCursor(10, 50);
    ILI9341_SetTextSize(1);
    ILI9341_WriteString("GPS Disabled", ILI9341_RED);

    ILI9341_FillRect(120, 290, 100, 20, ILI9341_RED); // кнопка навігації
    ILI9341_SetCursor(150, 295);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_RED);
    ILI9341_WriteString("Back", ILI9341_WHITE);
}

void Display_Errors(void) {
    ILI9341_FillScreen(ILI9341_BLACK);

    ILI9341_SetCursor(10, 10);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_BLACK);
    ILI9341_SetTextSize(2);
    ILI9341_WriteString("Error Log", ILI9341_WHITE);

    ILI9341_SetCursor(10, 50);
    ILI9341_SetTextSize(1);
    ILI9341_WriteString("No errors detected.", ILI9341_GREEN);

    ILI9341_FillRect(120, 290, 100, 20, ILI9341_RED); // кнопка навігації
    ILI9341_SetCursor(150, 295);
    ILI9341_SetTextColor(ILI9341_WHITE, ILI9341_RED);
    ILI9341_WriteString("Back", ILI9341_WHITE);
}

void Scan_Keypad(void) {
    for (int row = 0; row < 4; row++) {
        HAL_GPIO_WritePin(ROW_PORTS[row], ROW_PINS[row], GPIO_PIN_SET);

        for (int col = 0; col < 4; col++) {
            if (HAL_GPIO_ReadPin(COL_PORTS[col], COL_PINS[col]) == GPIO_PIN_SET)
{
                char key = KEYS[row][col];
                Handle_Key(key);
            }
        }
        HAL_GPIO_WritePin(ROW_PORTS[row], ROW_PINS[row], GPIO_PIN_RESET);
    }
}
```

```
void Handle_Key(char key) {
    if (key == '1') {
        currentState = SETTINGS;
        Display_Settings();
    } else if (key == '2') {
    } else if (key == '3') {
        currentState = ERRORS;
        Display_Errors();
    } else if (key == 'B') {
        currentState = MENU;
        Display_Menu();
    } else if (key == 'M') {
        currentState = MAIN_INTERFACE;
        Display_MainInterface();
    }
}

int main(void) {
    HAL_Init();
    SystemClock_Config();
    MX_GPIO_Init();
    MX_SPI1_Init();
    ILI9341_Init();

    Display_MainInterface();

    while (1) {
        Scan_Keypad();
    }
}
```