Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *другий (магістерський)*

Дослідження сучасних засобів для організації військового зв'язку

(тема)

Виконав:
здобувач *2* року навчання,
групи *ІМІзм-24-1*
Вадим Стрілка
(власне ім'я, прізвище)

Спеціальність *172 Електронні комунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. к.т.н. Дарія Чеботарьова*
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ІМІ _____ *Микола Москалець*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Вадим Стрілка*
(підпис) (власне ім'я, прізвище)

Керівник _____ *Дарія Чеботарьова*
(підпис) (власне ім'я, прізвище)

Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Електронні комунікації та радіотехніка*
(код і повна назва)

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

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ_____
(підпис)

"*25*" *грудня* 2025р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Стрілці Вадиму Ярославовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження сучасних засобів для організації військового зв'язку*

затверджена наказом університету від "*20*" *жовтня* 2025 р. № *179 Стз*

2. Термін подання здобувачем роботи до екзаменаційної комісії *20 червня 2025 р.*

3. Вихідні дані до роботи *Дослідити основи організації, завдання та вимоги до військового зв'язку, виконати аналіз сучасного стану та тенденцій розвитку військового зв'язку. Дослідити системи військового зв'язку, визначити переваги та недоліки різних сучасних систем військового зв'язку. Проаналізувати сучасні засоби для організації військового зв'язку. Виконати порівняльний аналіз програмно-визначених радіостанцій та багатокритеріальний аналіз військових смартфонів. Сформувати рекомендації для покращення військового зв'язку.*

4. Перелік питань, що потрібно опрацювати в роботі

1. Аналіз стану та розвитку військового зв'язку

2. Системи та засоби військового зв'язку

3. Порівняльний аналіз сучасних засобів ВЗ

4. Перспективи покращення військового зв'язку

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____

Слайди у форматі Power Point (назва, мета та задачі роботи, основи організації сучасного ВЗ, основні вимоги до ВЗ, сучасний стан та тенденції розвитку ВЗ, структура та основні характеристики ВЗ, порівняльний аналіз сучасних СВЗ, засоби ВЗ, порівняльний аналіз SDR, військові смартфони, порівняння найкращих моделей військових смартфонів, вибір оптимального військового смартфона, рекомендації для покращення ВЗ, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*20.10.25*	*Виконано*
2	*Підбір літератури за темою роботи.*	*21.10 - 29.10.25*	*Виконано*
3	*Виконання розділу 1*	*30.10 - 10.11.25*	*Виконано*
4	*Виконання розділу 2*	*11.11 – 21.11.25*	*Виконано*
5	*Виконання розділу 3*	*22.11 – 01.12.25*	*Виконано*
6	*Виконання розділу 4*	*02.12 - 14.12.25*	*Виконано*
7	*Оформлення пояснювальної записки,*		
	презентаційного матеріалу та підготовка		
	до захисту у ЕК	*15.12 - 20.12.25*	*Виконано*

Дата видачі завдання *20 жовтня 2025 р.*

Здобувач _____
(підпис)

Керівник роботи _____ *доц. Чеботарьова Д.В.*
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 84 с., 16 рис., 10 табл.,31 джерело, 2 додатки

Об'єкт дослідження – засоби військового зв’язку.

Мета роботи – дослідження сучасних засобів військового зв’язку та вибір оптимальних засобів з урахуванням сукупності показників якості.

Результати – в роботі розглянуто основи організації, завдання та вимоги до сучасного військового зв’язку, виконано аналіз сучасного стану та тенденцій розвитку військового зв’язку. Досліджено системи військового зв’язку, їх структуру та основні характеристики, виконано аналіз різних сучасних систем військового зв’язку. Розглянуто сучасні засоби для організації військового зв’язку. Виконано порівняльний аналіз програмно-визначених радіостанцій та багатокритеріальний аналіз військових смартфонів. Визначено оптимальний військовий смартфон з урахуванням сукупності показників якості. Сформовано та запропоновано рекомендації для покращення військового зв’язку.

ВІЙСЬКОВИЙ ЗВ’ЯЗОК, ЗАСІБ, СИСТЕМА, ТЕХНОЛОГІЯ, ІНФОКОМУНІКАЦІЇ, ІНФОРМАЦІЯ, SDR, ВІЙСЬКОВИЙ СМАРТФОН, УПРАВЛІННЯ, ОПТИМІЗАЦІЯ.

THE ABSTRACT

Explanatory note: 84 p., 16 fig., 10 tabl., 31 sources, 2 app.

Object of research - military communication means.

The purpose of the work is to study modern military communications and select the optimal means taking into account a set of quality indicators.

Results - the work considers the basics of organization, tasks and requirements for modern military communications, analyzes the current state and trends in the development of military communications. Military communications systems, their structure and main characteristics are studied, and various modern military communications systems are analyzed. Modern means for organizing military communications are considered. A comparative analysis of software-defined radio stations and a multi-criteria analysis of military smartphones are performed. The optimal military smartphone is determined taking into account a set of quality indicators. Recommendations for improving military communications are formulated and proposed.

MILITARY COMMUNICATIONS, DEVICE, SYSTEM, TECHNOLOGY, INFOCOMMUNICATIONS, INFORMATION, SDR, MILITARY SMARTPHONE, MANAGEMENT, OPTIMIZATION.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

АУВ – автоматизація управління військами;

БПЛА – безпілотний літальний апарат;

ВЗ – військовий зв’язок;

ЗВЗ – засіб військового зв’язку;

ЗСУ – Збройні сили України;

ІКС – інформаційно-комунікаційна система;

РЕБ – радіоелектронна боротьба;

СВЗ – система військового зв’язку;

СТРЗ – система тактичного радіозв’язку;

ШІ – штучний інтелект;

AJP-6 (Allied Joint Publication-6) – стандарт NATO, що визначає ключові принципи інформаційних та комунікаційних систем;

AR (Augmented Reality) – доповнена реальність;

IoT (Internet of Things) – інтернет речей;

JADC2 (Joint All-Domain Command and Control) – стратегія об'єднаного командування та управління всіма доменами;

LiFi (Light Fidelity) – безпроводова технологія передачі даних на основі світла замість радіохвиль;

LTE (Long-Term Evolution) – стандарт мобільного зв'язку 4-го покоління;

MIMO (Multiple Input Multiple Output) – системи зв'язку з кількома входами та кількома виходами;

NATO (North Atlantic Treaty Organization) – Організація Північно-атлантичного договору;

SDR (Software-Defined Radio) – програмно-визначена радіостанція;

SWaP (Size, Weight, and Power) – критичні обмеження для інженерних систем (розмір, вага та потужність).

ВСТУП

В сучасних умовах мережі та засоби зв'язку перестали бути лише допоміжним інструментом, вони стали стратегічним фундаментом забезпечення військових операцій. В інформаційну епоху, коли інформація виступає визначальним ресурсом сили, характер збройних конфліктів дедалі більше зумовлюється рівнем інформаційного домінування, а ефективність військових операцій безпосередньо залежить від функціонування засобів зв’язку.

Використання інформаційно-комунікаційних засобів у військовій сфері за останні роки значно змінилося. Зараз такі засоби є максимально важливими для успіху військових операцій, швидкого прийняття оптимальних рішень та створенні стратегічних переваг.

Ефективність військових операцій значною мірою залежить від надійних, безпечних та адаптивних систем та засобів зв'язку. Сучасні війни стають дедалі більше мережецентричними, де перевага залежить не лише від вогневої потужності чи чисельної переваги, а й від здатності обмінюватися інформацією та діяти на її основі швидше, ніж супротивник. Стратегічною необхідністю сьогодні є здатність передавати інформацію в режимі реального часу через різноманітні сфери (наземну, повітряну, морську, космічну та кіберпростірну). Зараз військові системи зв'язку швидко розвиваються, інтегрують передові радіомережі, супутниковий зв'язок та зашифровану передачу даних, забезпечують безперебійну координацію між розгорнутими силами та командними центрами.

Зростаюча складність та особливості сучасних військових операцій підкреслюють необхідність досліджень та вдосконалень різноманітних засобів зв'язку для створення та впровадження високозахищених та сумісних комунікаційних інфраструктур, які можуть функціонувати в сучасних та

складних умовах. Для України в умовах воєнного стану такі дослідження є особливо актуальними.

Дана кваліфікаційна робота присвячена дослідженню сучасних засобів для організації військового зв’язку. Сучасна військова ситуація в Україні, а також аналіз літературних та інших інформаційних джерел за темою роботи [1 – 31] підтверджують актуальність даної кваліфікаційної роботи.

1 АНАЛІЗ СТАНУ ТА РОЗВИТКУ ВІЙСЬКОВОГО ЗВ’ЯЗКУ

1.1 Основи організації сучасного військового зв’язку

Військовий зв’язок (ВЗ) – це обмін інформацією в системі управління військами (силами) та зброєю [1, 2]. Військовий зв’язок є важливою складовою частиною Збройних сил, що дозволяє виконувати важливі завдання, зокрема забезпечує обмін інформацією, обробку та зберігання даних, а також вирішувати інформаційні задачі в системах управління військовими силами.

Управління військовими силами є основою успіху під час виконання будь-якого бойового чи навчального завдання. Забезпечити надійне управління можливо лише шляхом впровадження сучасних цифрових захищених засобів військового зв'язку [3] та постійного вдосконалення засобів зв'язку та всіх інформаційно-комунікаційних процесів.

Роль систем зв'язку в сучасних військових операціях є надзвичайно важливою. Надійний та безпечний військовий зв'язок є важливим для командування та управління, координації та ситуаційної обізнаності. Інтегровані мережі зв'язку покращують оперативну швидкість та точність військового зв’язку.

Український досвід ведення бойових дій останніх років підтвердив необхідність створення систем управління на сучасних принципах і новітніх технологіях. Сьогодні розвиток інфокомунікаційних систем та автоматизації управління силових структур України має стійку тенденцію до всебічної модернізації, переоснащення підрозділів новими засобами зв’язку та переходу на сучасні цифрові технології [3]. Сучасна система зв'язку має інтегрувати функції коммунікацій, навігації, орієнтування та управління військами, зброєю, розвідкою, радіоелектронною боротьбою; вона має створюватися та розвиватися відповідно до прийнятої у країнах NATO концепції управління військами на основі побудови єдиного інформаційного простору.

Військовий зв’язок безпосередньо пов'язаний з автоматизацією управління військами (АУВ). ВЗ та АУВ реалізують та забезпечують війська зв’язку. Війська зв’язку призначені спеціально для створення, впровадження та експлуатації систем ВЗ та АУВ. Основні завдання військ зв’язку визначено в [1, 2] та наведено на рис. 1.1.

Рисунок 1.1 – Основні завдання військ зв’язку

Структура ВЗ містить в собі багато різних елементів: польові вузли зв’язку, відділення, центри, вузли, станції, пункти, групи, взводи, полки, заводи, бази, склади різного призначення, навчальні заклади та наукові установи [1]. Всі ці елементи мають функціонувати згідно з суворою організацією єдино, комплексно та узгоджено. Структура ВЗ та призначення її елементів наведено на рис. 1.2.

Рисунок 1.2 – Структура та призначення ВЗ

Організація сучасного військового зв'язку має свої особливості (рис.1.3), що спричиняють суттєве ускладнення завдань зв'язку для забезпечення безперервного та надійного управління під час військових дій.

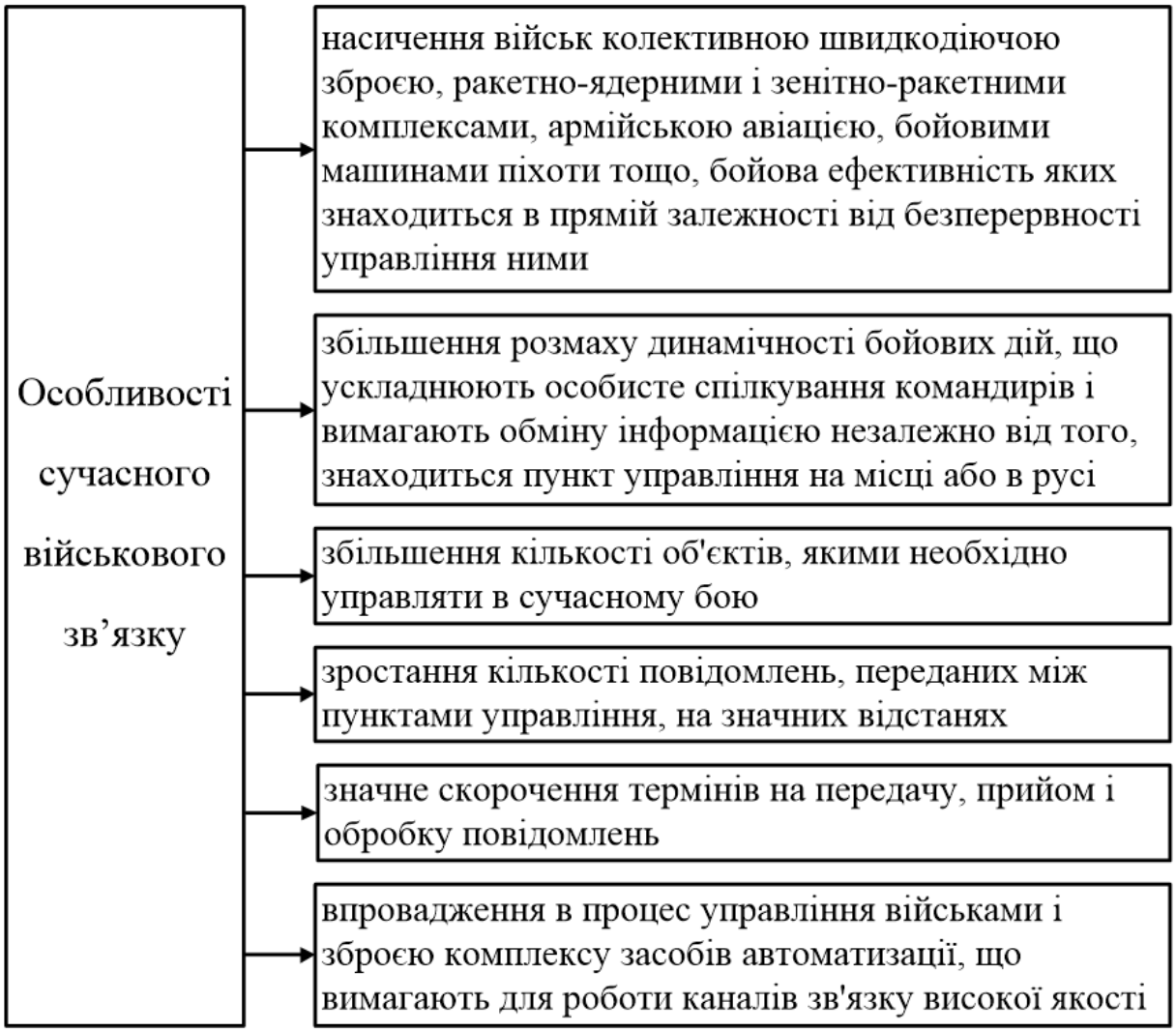

Рисунок 1.3 – Особливості сучасного ВЗ

У сучасних війнах, де поле бою є мінливим, а підрозділи часто розосереджені, зв'язок у режимі реального часу є особливо важливим. Сучасні мобільні та безпечні системи дозволяють координувати дії в русі, швидко адаптуватися до мінливих загроз та уникати зайвого ризику.

Операції на складній місцевості або в міському середовищі часто залежать від децентралізованого прийняття рішень. Це можливо лише за умови надійності систем зв'язку на всіх рівнях, від взводу до командування театру бойових дій. Без такої зв'язності навіть технологічно розвинені підрозділи можуть бути ізольованими та нездатними ефективно реагувати [4].

1.2 Основні вимоги до сучасного військового зв’язку

Сучасний зв'язок є основою командування та управління. Ефективне командування та управління неможливе без надійних та швидко реагуючих систем зв'язку. Мережі зв'язку забезпечують потік наказів, розвідувальних даних та оновлень між командними центрами та бойовими підрозділами. Коли цей потік швидкий і точний, то операції синхронізовані та адаптивні [4].

Системи зв'язку все частіше стають мішенню для засобів радіоелектронної боротьби та кібератак. Глушіння, підміна сигналів та перехоплення сигналів можуть порушити координацію в критичні моменти. Ці збої не лише впливають на тактичні операції, але й можуть мати стратегічні наслідки, якщо командні структури втрачають ситуаційну обізнаність або здатність контролювати свої сили.

З розвитком комунікаційних технологій системи зв’язку стають більш потужними, але також і складнішими. Передові системи тепер включають зашифровану передачу даних, геолокацію в режимі реального часу, відеоканали та багатодоменну інтеграцію. Однак, розширена функціональність має бути збалансована з простотою використання. Занадто складні системи можуть стати перешкодою, якщо користувачі не пройшли належного навчання або якщо технічна підтримка недоступна під час роботи.

Системи, які є інтуїтивно зрозумілими та легко адаптуються під тиском, мають більше шансів бути ефективно використані в реальних бойових ситуаціях [4]. Простота інтерфейсу та надійність у польових умовах так само важливі, як і технічні характеристики на папері.

Результати аналізу літератури [1 – 5] вказують на низку суттєвих вимог до систем зв'язку (рис. 1.4) в сучасних та майбутніх військових операціях. Вони повинні бути достатньо швидкими для підтримки циклів прийняття рішень, достатньо безпечними, щоб витримувати електронні атаки, та достатньо простими, щоб функціонувати в стресових ситуаціях. Це поєднання має

вирішальне значення для підтримки ініціативи та координації на ранніх стадіях конфлікту високої інтенсивності.

Рисунок 1.4 – Вимоги до сучасного ВЗ

Однією з ключових вимог військового зв'язку є оперативна сумісність - здатність, що забезпечує безперебійний обмін інформацією між різними видами збройних сил та багатонаціональними коаліціями. Для забезпечення складних спільних операцій різні комунікаційні мережі повинні ефективно працювати в рамках єдиної системи [5].

Вимоги безпеки, достовірності та секретності передачі даних є також дуже актуальними, оскільки останнім часом кількість кібератак та інших цифрових інформаційних злочинів зростає та має великий негативний вплив на результати військових операцій.

Крім того, планування комунікацій має бути повністю інтегроване в оперативний план, а не розглядатися як допоміжний елемент. Сили, які не надають пріоритетів комунікаційній інфраструктурі та навчанню, ризикують втратити здатність ефективно діяти в складних та конфліктних умовах.

1.3 Сучасний стан та тенденції розвитку військового зв’язку

Ключовим аспектом сучасного військового зв'язку є забезпечення надійного мережного з'єднання та безперервний потік інформації, незважаючи на кіберзагрози, атаки радіоелектронної боротьби (РЕБ) та порушення навколишнього середовища.

Військові доктрини підкреслюють важливість маневреності, резервування та живучості в мережах зв'язку, забезпечуючи збереження оперативної готовності сил навіть за умови порушення роботи основних каналів [5].

Сучасні фундаментальні принципи підтримки сигналів включають сумісність, стійкість мережі та стратегії кібербезпеки, необхідні для успіху військових операцій. Ці принципи мають вирішальне значення у великомасштабних бойових операціях, де здатність підтримувати командування та управління визначає успіх операцій.

В наш час у всьому світі відбувається перехід від традиційного зв’язку до сучасних військових інфокомунікаційних платформ, що характеризуються новими можливостіми, зокрема значним зростанням швидкості передачі даних, управлінням мережами за допомогою штучного інтелекту (ШІ) та використанням новітніх автоматизованих протоколів шифрування [5]. В табл. 1.1. наведено порівняння традиційних та сучасних військових систем зв’язку.

Таблиця 1.1 – Порівняння традиційного та сучасного ВЗ

№	Функції	Традиційний зв’язок	Сучасний зв’язок
1	Вид передачі	Аналогові сигнали	Зашифровані цифрові мережі
2	Швидкість передачі даних	Низькі швидкості	Високошвидкісний широкосмуговий доступ
3	Безпека	Вразливість до перехоплення	Наскрізне шифрування та безпека на основі використання ШІ
4	Сумісність	Обмежена	Повна інтеграція зі спільними / багатонаціональними операціями
5	Адаптивність	Системи з фіксованою частотою	Програмно-визначені та частотно-гнучкі системи
6	Надійність у бою	Схильність до глушіння	Висока стійкість до РЕБ та кіберзагроз

Через існуючі військові конфлікти світовий ринок військового зв'язку останнім часом суттєво зростає. Згідно з дослідженням [6] ринок військового зв'язку у 2025 році становить 34,28 млрд доларів США та прогнозується що, до 2032 року він досягне 55,77 млрд доларів США, що демонструє сукупний річний темп зростання (CAGR) 7,2% з 2025 по 2032 рік [6].

На ринку військового зв’язку зараз спостерігається сильна увага до інтеграції передових технологій, таких як 5G, штучний інтелект та кіберзахищені комунікаційні мережі, для підвищення операційної ефективності та ситуаційної обізнаності. Також більше уваги приділяється супутниковому зв'язку, тактичним радіостанціям та шифруванню даних для підтримки зв'язку в режимі реального часу на полі бою. Перехід до мережецентричної війни та оперативної сумісності між союзними силами сприяє інноваціям та впровадженню комунікаційних рішень наступного покоління [6]. Аналіз сучасного стану військового зв’язку наведено в табл. 1.2.

Таблиця 1.2 – Аналіз сучасного стану військового зв’язку

Сфера	Події, що впливають на розвиток військового зв’язку	Наслідки та тенденції розвитку військового зв’язку
1	*2*	*3*
Геополітична	1. Збільшення оборонного бюджету NATO через російсько-українську війну	– різке зростання закупівель безпечних систем зв’язку в режимі реального часу, особливо серед країн Східної Європи та союзників NATO
	2. Зростання напруженості в Індо-Тихоокеанському регіоні (США, Китай, Тайванська протока)	– прискорення переходу регіональних військових на супутникові та зашифровані платформи зв’язку; – підвищення попиту на системи на основі ШІ та кіберзахищені системи
	3. Санкції проти китайських оборонно-технологічних компаній	– обмеження доступу до компонентів; – вимушена переорієнтація західних військових на власних або союзних постачальників; – збільшення інвестицій у власні можливості військового зв’язку
Економічна та інфраструктурна	1. Збільшення витрат на модернізацію оборони після COVID	– країни надають пріоритет цифровізації та зв'язку на полі бою; – підвищення попиту на тактичні радіостанції, супутниковий зв'язок та інтегровані системи

Продовження табл. 1.2

1	*2*	*3*
	2. Зростання інтелектуальних військових баз та оборонних екосистем, що підтримуються штучним інтелектом	– підвищення попиту на інтегровані комунікаційні мережі, що здатні підтримувати автономні операції, спостереження та безпечне командування та управління

Сьогодні на ринку військового зв’язку перше місце займає сегмент повітряного зв'язку з часткою 39,2%, а друге місце займає сегмент військових супутникових систем з часткою 34,2% [6].

Повітряний зв'язок зараз став критичним сегментом на світовому ринку військового зв'язку, він лідирує завдяки покращеному зв'язку на полі бою та зростаючому акценту на повітряному спостереженні. Сучасні військові операції потребують миттєвої передачі даних між повітряними засобами, наземними військами, військово-морськими суднами та командними центрами, що створює попит на надійні та безпечні системи повітряного зв'язку.

На ринку спостерігається зростаюча інтеграція передових технологій, таких як високочастотні радіостанції, супутникові канали та протоколи безпечного шифрування даних, спеціально розроблені для використання в повітрі. Крім того, розширення сучасної тактики ведення війни, що зосереджується на мережецентричних операціях, створює потребу в безперебійному повітряному зв'язку, який може передавати відеопотоки, радіолокаційну інформацію та командні інструкції з мінімальною затримкою.

Ще однією важливою тенденцією є збільшення використання дронів та дистанційно керованих апаратів для розвідки, спостереження та рекогносцювання. Поширення безпілотних літальних апаратів (БПЛА) у різних військових застосуваннях (від патрулювання кордонів до бойової підтримки) відповідно посилило попит на передові технології повітряного зв'язку,

призначені для подолання обмежень пропускної здатності та розширення оперативної дальності. Наприклад, у рамках стратегії Об'єднаного командування та управління JADC2 (Joint All-Domain Command and Control) ВПС США розгортають Розширену систему управління боєм ABMS (Advanced Battle Management System) для покращення повітряного зв'язку та інтеграції даних у режимі реального часу на кількох військових платформах [6].

Військові супутникові системи, які займають приблизно 34,2% частки у 2025 р., виділяються також як домінуючий сегмент на ринку військового зв'язку. Супутникові системи дозволяють збройним силам підтримувати безперервні канали зв'язку на величезних відстанях, включаючи віддалені та складні умови, де традиційні комунікаційні мережі недоступні або вразливі. Сучасні військові місії часто охоплюють кілька театрів військових дій і вимагають сумісних каналів зв'язку, які можуть долати географічні обмеження. Супутникові мережі сприяють зв'язку за межами прямої видимості та забезпечують постійний контакт командних центрів з розгорнутими підрозділами незалежно від їхнього місцезнаходження (на суші, морі або в повітрі). Зростаюча складність супутникових технологій, таких як високопродуктивні супутники (HTS), лазерні канали зв'язку та супутникові угруповання на низькій навколоземній орбіті (LEO), значно збільшує пропускну здатність, зменшує затримку та підвищує стійкість до загроз радіоелектронної війни. Міркування безпеки ще більше підсилюють домінування супутникових систем.

Військові супутникові платформи забезпечують стандартизовані комунікаційні рамки, що дозволяють безперебійний обмін даними між різноманітними системами зв'язку, розгорнутими різними країнами. Уряди надають пріоритет покращенню своїх супутникових комунікаційних ресурсів для підтримки цих критично важливих оборонних функцій у рамках ширших зусиль з модернізації військової галузі. Космічні сили США у співпраці з Агентством з розвитку космосу (SDA) та оборонними підрядниками, такими як Boeing, Lockheed Martin та Northrop Grumman, просувають програму

захищеного тактичного супутникового зв'язку (PTS) для розробки безпечних, захищених від перешкод та високопродуктивних систем супутникового зв'язку для військових операцій.

Основні перспективні напрямки науково-технологічного розвитку ВЗ наведено на рис. 1.5. Основні сучасні технологічні рішення у різних сферах розвитку ВЗ [7] показано на рис. 1.6.

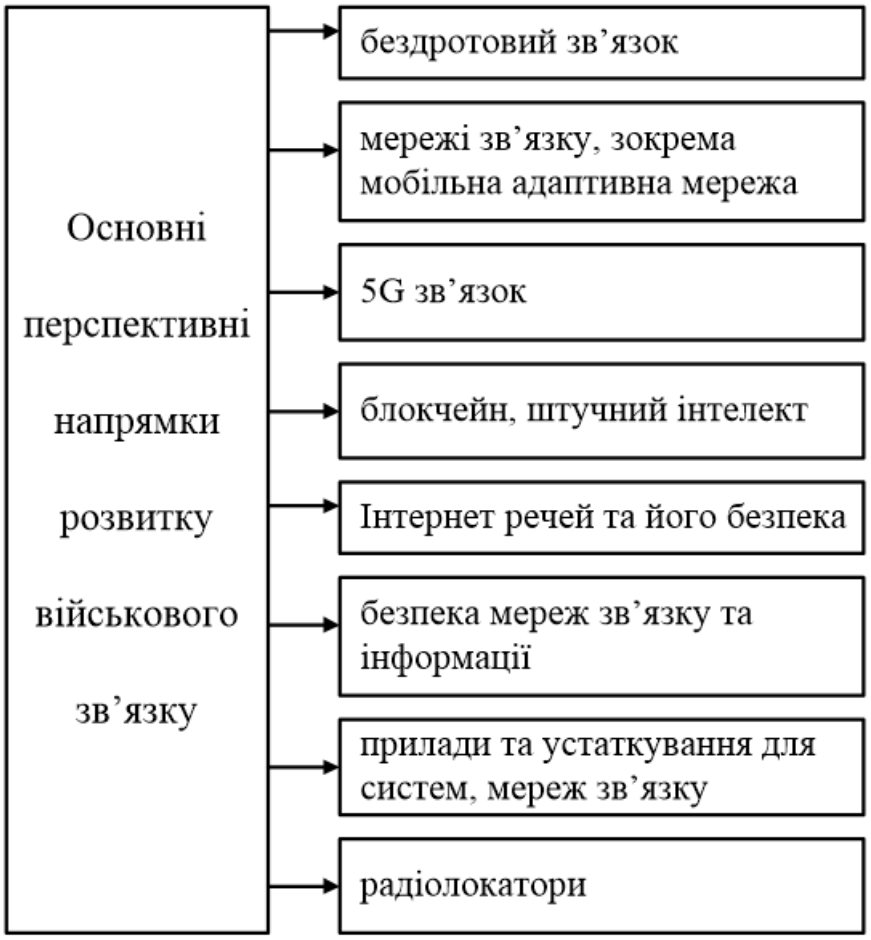

Рисунок 1.5 – Перспективні напрямки розвитку ВЗ

Сьогодні на ринок військового зв'язку великий вплив має впровадження штучного інтелекту. ШІ суттєво трансформує військові системи зв'язку, забезпечуючи швидше, безпечніше та автономніше прийняття рішень. Інструменти на базі ШІ все частіше використовуються для сигнальної розвідки, перекладу мов у режимі реального часу, виявлення загроз та оптимізації

мережі, що дозволяє силам оборони швидко аналізувати величезні набори даних та гнучко реагувати. В умовах бою ШІ покращує ситуаційну обізнаність, інтегруючи вхідні дані датчиків, автоматизуючи обробку даних та допомагаючи в операціях командування та управління.

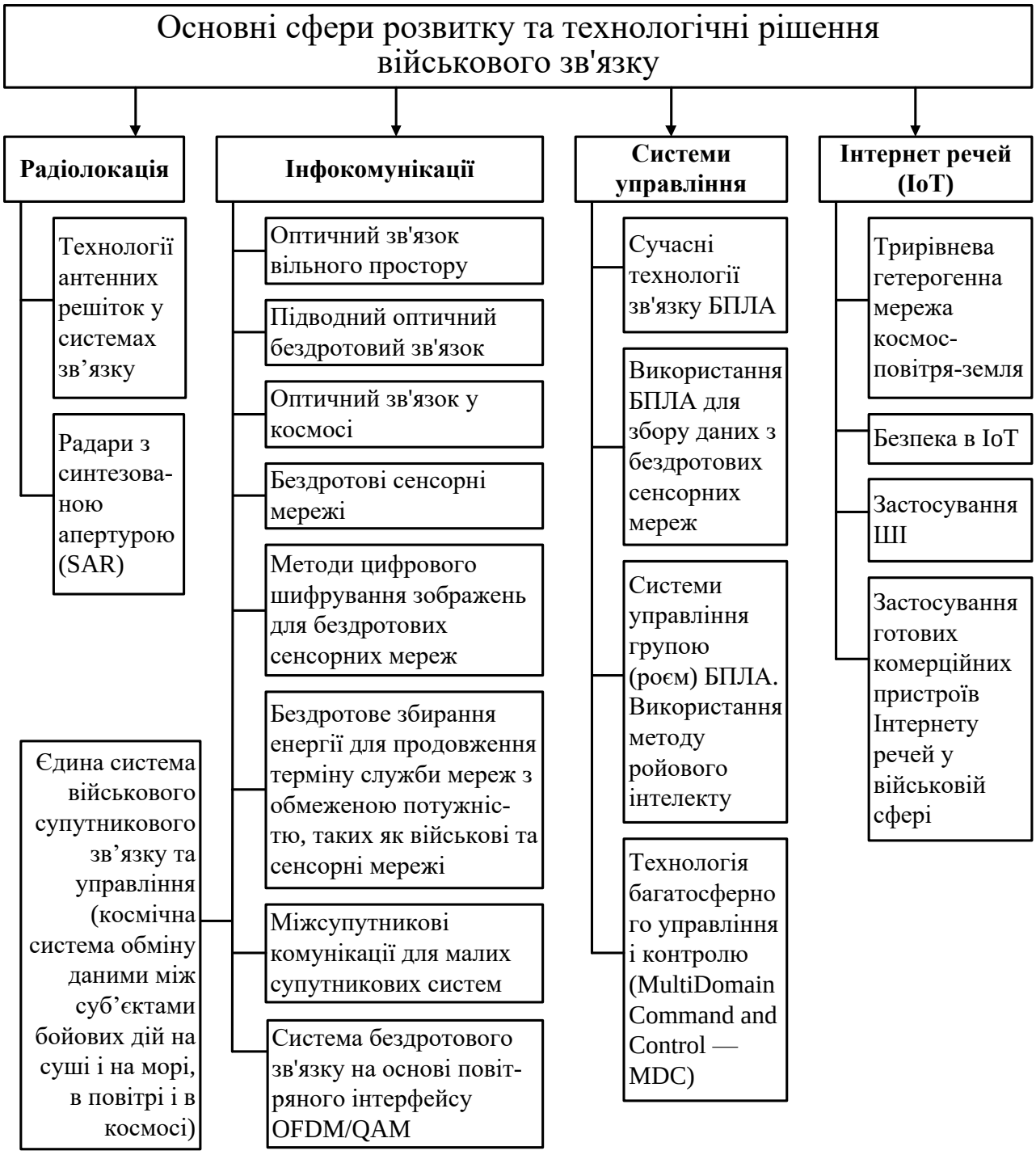

Рисунок 1.6 – Сучасні технологічні рішення у різних сферах розвитку ВЗ

Помітним прикладом з реального світу є програма Об'єднаного командування та управління всіма доменами (JADC2) Міністерства оборони США, яка інтегрує системи на базі штучного інтелекту в наземній, повітряній, морській, кібер- та космічній сферах. У випробуванні 2023 року ВПС США продемонстрували використання алгоритму ШІ, який автономно та миттєво аналізував супутникові та безпілотні знімки, передавав координати цілей через захищені тактичні мережі та запускав автономні дії безпілотників [6].

2 СИСТЕМИ ТА ЗАСОБИ ВІЙСЬКОВОГО ЗВ’ЯЗКУ

2.1 Структура систем військового зв’язку

Система військового зв’язку (СВЗ) – це сукупність взаємозв’язаних, сумісних та узгоджених за завданнями вузлів і ліній військового зв’язку, орендованих каналів передачі, групових трактів та утворених на їх основі систем і мереж, що призначені для вирішення задач забезпечення управління військовими силами, зброєю в мирний час, під час їх приведення у вищі ступені бойової готовності, підготовки та веденні бойових дій [1, 2].

СВЗ в провідних країнах світу будуються на основі класичної трирівневої схеми (рис. 2.1) з використанням нових інформаційних технологій та інтеграцією послуг у військових цифрових мережах, що забезпечують передачу різноманітних видів повідомлень (голос, дані, відео тощо) з гарантованою якістю обслуговування.

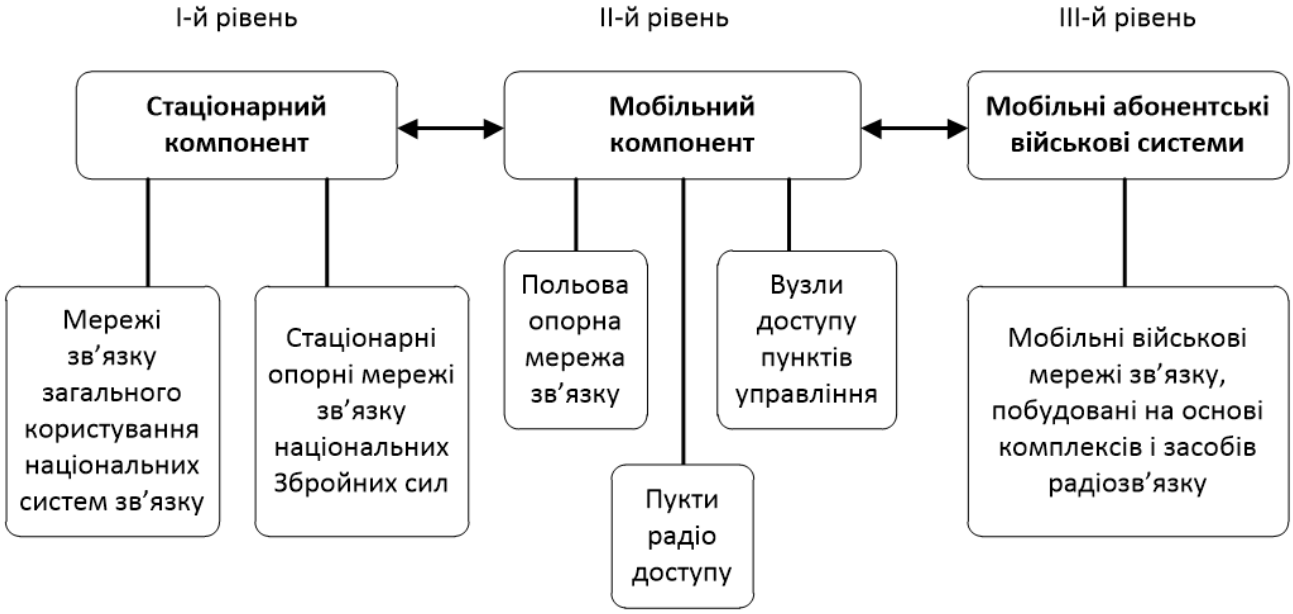

Рисунок 2.1 – Класична схема побудови СВЗ

Стаціонарний компонент - це I рівень СВЗ. Він базується на національних мережах зв'язку загального користування та на стаціонарних опорних мережах зв'язку Збройних сил.

Мобільний компонент - це II рівень СВЗ. Він базується на польовій опорній мережі зв'язку, вузлах доступу пунктів управління та пунктах радіодоступу.

Мобільні військові абонентські системи доступу до кожного військового на полі бою - це III рівень СВЗ. Ці мобільні мережі ВЗ будуються на основі різноманітних комплексів і засобів радіозв'язку.

Дана схема побудови системи військового зв'язку (рис. 2.1) дає можливість використовувати єдине транспортне середовище для інформаційного обміну між військовими в інтересах усіх військових сил незалежно від підпорядкування та оперативної належності (від окремого військового до штабів стратегічного рівня).

Сучасна СВЗ являє собою суміш мобільних та динамічних гетерогенних мереж у широкому спектрі носіїв, які не обов'язково належать до однієї й тієї ж області безпеки. З'єднання реагує на операційні вимоги та охоплює низькі та високі швидкості передачі даних з періодичними періодами мовчання, звідси й різноманітні протоколи в інформаційних технологіях (IT) та аналогових мережах [8].

Стандарт NATO AJP-6 [9] визначає стратегічні і тактичні СВЗ. Існує 3 класи мереж: стратегічні, оперативні та тактичні, для підтримки командних, бойових або інформаційно-комунікаційних систем (ІКС), підключених на цьому рівні і які забезпечують підтримку трьох командних середовищ. Це посилюється вимогами до обміну комунікаційною інформацією, що розподіляються відповідно до бойового порядку та структури командування ієрархічно від стратегічного до тактичного, причому можливості та пропускна здатність зменшуються при наближенні до тактичного краю, для підтримки ієрархічних інформаційних потоків. Через необхідність, можливості та

розвиток технологій, розроблені стратегічні ІКС та шлюзи використовуються на тактичному рівні та можуть взаємодіяти безпосередньо через мережу.

Сьогодні дуже важливу роль у ВЗ відіграє тактичний радіозв'язок. Система тактичного радіозв'язку (СТРЗ) включає 4 основні рівні, що зображено на рис. 2.2 [3]. В табл. 2.1 наведено характеристики основних рівнів СТРЗ.

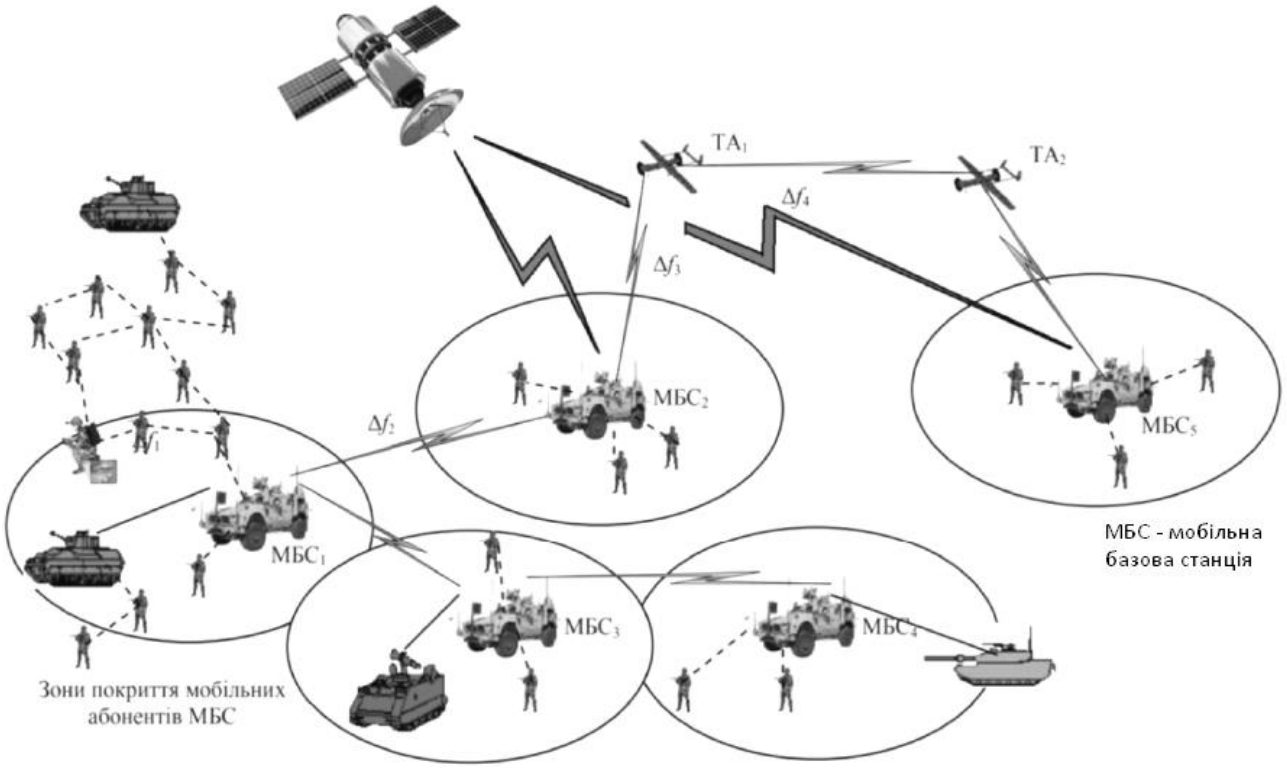

Рисунок 2.2 – Архітектура системи тактичного радіозв'язку

СТРЗ завдяки своїй єдиній багаторівневій архітектурі, що містить взаємосумісні системи, створює єдиний інформаційний простір та забезпечує захищений обмін даними між цими системами (на відміну від розрізнених систем ВЗ, що використовувалися раніше). Система управління в ЗСУ сьогодні будується на основі стандартів NATO та прийнятої в країнах NATO концепцією мережецентричного управління військами [3]. Технологічною основою системи управління стає єдина автоматизована система військового зв'язку, що об'єднує в собі різні засоби зв'язку, програми, радіоелектронну боротьбу, розвідувальні, навігаційні та інші бойові комунікаційні засоби.

Таблиця 2.1 – Основні характеристики рівнів СТРЗ

Рівень	Склад	Задачі	Розмірність	Динаміка змін топології
I	бойові радіомережі	зв’язок між солдатами, управління низового рівня	сотні абонентів	дуже висока
II	мобільна високо-швидкісна транспортна мережа	формування зони радіодоступу мобільним абонентам і надання їм необхідних сервісів	кожна МБС обслуговує до 200 військових та до 30 бойових машин [3]	середня, можливий розподіл на підмережі
III	повітряна транспортна мережа (реалізована на ТК аеро-платформах (БПЛА, дрони тощо)	функції додаткової високошвидкісної транспортної мережі, формування зони радіодоступу мобільним абонентам	велика	може бути як високою так і низькою
IV	супутникова мережа	забезпечення ефективних, захищених, інтерактивних ліній зв'язку високої якості	велика	мінлива

Основні принципи організації сучасних систем військового зв’язку наведені на рис. 2.3.

Рисунок 2.3 – Принципи організації СВЗ

Сьогодні системи військового зв’язку в Україні будують за принципами та стандартами NATO, відбувається всебічний розвиток та модернізація СВЗ, впроваджують новітні технології, війська оснащують все більш сучасними засобами зв’язку.

2.2 Основні характеристики систем військового зв’язку

Зв'язок у військовій сфері є аспектом життєво важливого значення для координації та контролю операцій, передачі інформації (голосу, даних, відео), необхідної для отримання адекватного сприйняття навколишнього середовища та ситуації. Зв'язок необхідний військовослужбовцям на всіх рівнях та в різних середовищах, таких як під водою, на землі, в повітрі та в космосі. Військовий зв'язок повинен характеризуватися гнучкістю, адаптивністю та керованістю такими характеристиками, як частота, пропускна здатність, швидкість передачі

інформації та час реагування, а також гарантувати безперервність зв'язку, незважаючи на різні середовища, які можуть виникнути [9].

Для ефективного та результативного виконання своїх стратегічних принципів, СВЗ повинна відповідати низці загальних характеристик. Основні характеристики систем ВЗ визначені у виданнях зброєю [1, 2], а більш детально описані в стандарті NATO AJP-6 [10]. На основі аналізу даної інформації створено рис. 2.4, в якому представлено характеристики систем ВЗ.

Рисунок 2.4 – Основні характеристики СВЗ

СВЗ має бути специфікована, розроблена, впроваджена та експлуатуватися таким чином, щоб відповідати внутрішнім вимогам командування. Щоб уникнути погіршення або уповільнення процесів прийняття рішень, слід подбати про те, щоб забезпечити достатню функціональність СВЗ для підтримки інформаційних процесів командира, а також про те, щоб пов'язані з нею потужності були масштабовані таким чином, щоб вони відповідали сукупності внутрішніх вимог.

Ефективні спільні та багатонаціональні операції вимагають сумісності СВЗ, що дозволяють командуванню об'єднаних сил та підпорядкованим командирам здійснювати ефективне управління між елементами сил. У порядку зростання рівнів стандартизації – це сумісність, взаємозамінність та спільність.

Гнучкість забезпечує динамічну реакцію СВЗ на зміни в масштабах зусиль, оперативному темпі, поставі та перебоях. Це необхідно для реагування на зміни з мінімальними збоями або затримками. Гнучкість досягається шляхом розробки та відпрацювання планів дій у надзвичайних ситуаціях.

Масштабованість стосується здатності СВЗ адаптуватися до змін необхідного розміру та якості. Масштабованість також необхідна в межах однієї місії, оскільки операції часто масштабуються на етапах розгортання та виконання.

Стійкість – це здатність відновлюватися після небажаних змін та збоїв. Стійкість СВЗ є важливою для забезпечення безперервності та своєчасності процесів управління та контролю. Стійкість СВЗ досягається завдяки поєднанню резервування та здатності витримувати заданий рівень навантаження або вимог без погіршення стану або втрати функціональності при випадкових подіях та атаках [10].

Автономність СВЗ – це здатність працювати незалежно від наявності, контролю та впливу зовнішніх СВЗ та будь-якої вже існуючої логістики та інфраструктури (наприклад, енергопостачання та розміщення), а також операційних учасників.

Готовність СВЗ стосується рівня задоволення негайних потреб. Різні штаб-квартири, підрозділи, агентства та інші органи перебувають у розпорядженні на різних рівнях готовності, що відповідає їхній ролі в процесі управління та контролю. Їхні відповідно виділені СВЗ повинні мати подібний рівень готовності, щоб вони могли відповідно виконувати свої функції [10].

Безпека та ефективність зв'язку є дуже важливими, і у військовій сфері вони повинні враховувати катастрофічні ситуації, перешкоди, збої в енергетичних системах та руйнування локальних комунікаційних мереж [9].

Належна безпека СВЗ гарантує необхідний рівень конфіденційності, цілісності та доступності послуг, систем та інформації, що відповідають вимогам місії. Для того, щоб правила безпеки СВЗ були ефективними та результативними, вони повинні бути невід'ємною частиною консультацій, планування, виконання та оцінки місії, і повинні забезпечуватися шляхом збалансованого поєднання проектування, постійної оцінки гарантій та контрзаході [10].

2.3 Аналіз сучасних систем військового зв’язку

Згідно військових стандартів, зокрема ВСТ 01.112.001 [11], військовий зв'язок має види і роди зв’язку. Класифікація ВЗ за видами і родами представлена на рис. 2.5.

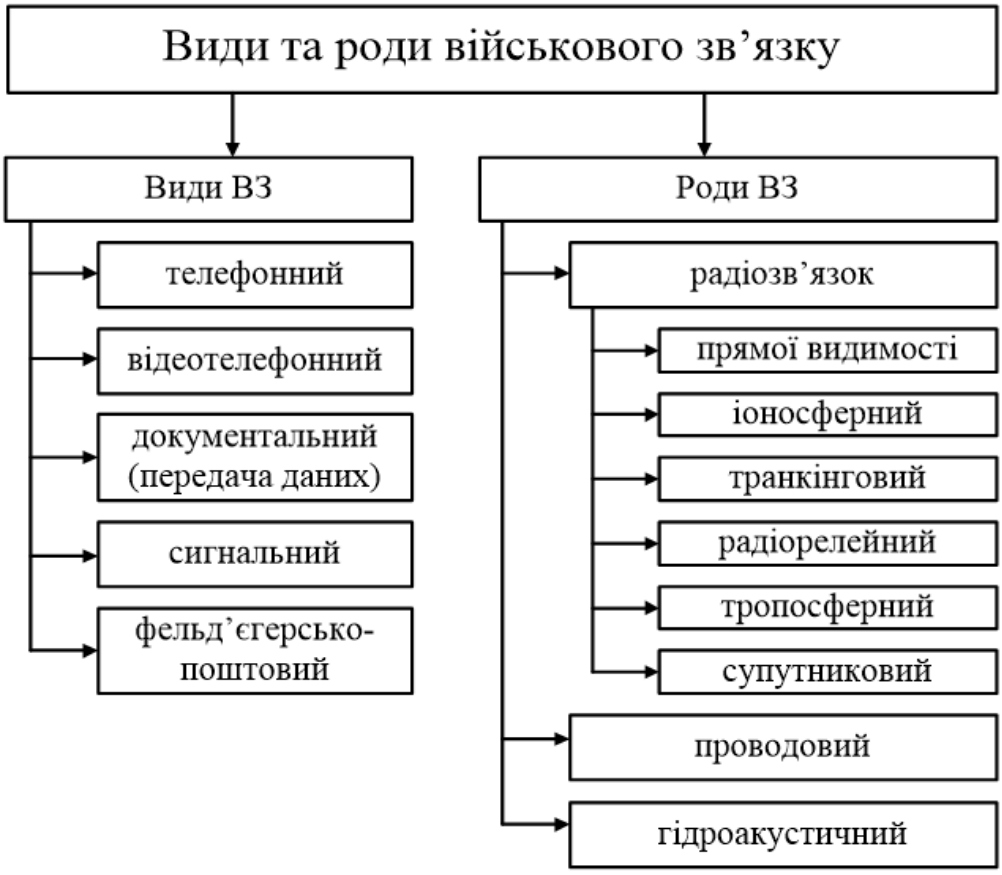

Рисунок 2.5 – Класифікація військового зв’язку

Сьогодні війна в Україні слугує сучасним полігоном для випробування військових комунікаційних стратегій. Розглянемо системи ВЗ, що застосовуються на українському полі бойових дій та виконаємо дослідження їхніх переваг, проблем та перспектив розв’язання цих проблем. Результати такого дослідження є критично важливими для військових стратегів, які планують майбутні операції в складному електромагнітному середовищі, де ефективна комунікація може визначити успіх або поразку [12].

2.3.1 Системи LTE

Системи LTE підтримують додатки, що працюють з великими обсягами даних, необхідними для розвідки та координації в режимі реального часу. Ці системи сприяють безперешкодній інтеграції між військовими та цивільними системами. Багато співробітників вже знайомі з технологією LTE, що скорочує час і витрати, пов'язані з навчанням.

Мережі LTE схильні до глушіння і перехоплення, що ставить під загрозу операційну безпеку. Залежність від фізичної інфраструктури робить мережі LTE вразливими до цілеспрямованих атак. У міських районах перевантаження цивільної мережі може перешкоджати військовим операціям.

Тактичні LTE-системи виявилися неоціненними в районах зі скомпрометованою інфраструктурою. Поєднання LTE із супутниковим зв'язком (наприклад, Starlink) підвищує відмовостійкість мережі. Захист мереж LTE від кіберзагроз та радіоелектронної війни має першорядне значення.

2.3.2 Системи супутникового зв’язку

Супутникові послуги відіграють ключову роль у військовій галузі та сфері оборони завдяки системам навігації, визначення часу та позиціонування, покриття у віддалених районах та безпечному підключенні [13, 14].

Супутникові мережі надають можливості зв'язку навіть у віддалених районах. Ці мережі залишаються працездатними навіть тоді, коли наземна інфраструктура зруйнована. Такі системи, як Starlink, пропонують значну пропускну здатність, підтримуючи передачу великих обсягів даних.

До основних проблем, з якими стикається космічний сектор, можна віднести перевантаженість та різноманітні проблеми безпеки (глушіння, спуфінг, викрадення, проникнення, компрометація тощо). Космічна сфера дедалі більше перевантажена. Кількість робочих супутників на орбіт навколо Землі дуже швидко зростає, що зменшує кількість орбіт, придатних для використання в оперативних цілях (таких як навігація чи спостереження), та збільшує ризик зіткнення, що може перешкодити наданню космічних послуг. [13]. Складні засоби глушіння і кібератаки можуть порушити супутниковий зв'язок. Затримки в передачі сигналу можуть вплинути на своєчасність прийняття важливих рішень. Крім того, витрати на системи та послуги супутникового зв'язку можуть бути непомірно високими.

Використання декількох супутникових провайдерів забезпечує безперервність зв'язку. Швидка підготовка до розгортання та зручні інтерфейси мають важливе значення для ефективного супутникового зв'язку. Розробка надійних засобів захисту від перешкод має вирішальне значення для підтримки цілісності супутникової мережі.

2.3.3 Тактичні радіомережі

Тактичні радіомережі мають надійне шифрування та стійкістю до перешкод створені для умов бойових дій. Вони розроблені спеціально для роботи в суворих умовах та мають забезпечувати надійність під час обстрілу.

Тактичні радіомережі мають меншу пропускну здатність порівняно з комерційними системами. Інтеграція цих мереж з іншими комунікаційними системами може бути складною. Постійна боротьба з ворожими засобами радіоелектронної боротьби вимагає безперервних інновацій.

Програмно-визначені радіостанції (SDR) забезпечують адаптивність в умовах радіоелектронної боротьби. Технології стрибкоподібної зміни частоти та розширення спектру є життєво важливими для забезпечення безпечного зв'язку. Постійні інвестиції в технології, стійкі до заторів, мають вирішальне значення для підтримання експлуатаційних можливостей.

2.3.4 Mesh-мережі

Mesh-мережі є децентралізованими, що робить їх менш вразливими до окремих точок відмови. Ці мережі автоматично адаптуються до мінливих умов, забезпечуючи безперервний зв'язок. Mesh-мережі чудово працюють у міському середовищі, де інші сигнали можуть бути заблоковані.

Окремі вузли мають обмежений радіус дії, що вимагає ретельного планування Mesh-мережі. Зі збільшенням розміру мережі управління нею стає дедалі складнішим.Електромагнітні випромінювання від mesh-мереж можуть збільшити ризик виявлення.

Mesh-мережі забезпечують критично важливий резервний зв'язок у міських бойових сценаріях. Розширення корисності mesh-мереж шляхом їх інтеграції з системами більшого радіусу дії має важливе значення. Впровадження суворих протоколів контролю викидів мінімізує ризики виявлення.

2.3.5 Стільникові мережі

Стільникові мережі пропонують в населених пунктах широко розгалужену інфраструктуру, яка може бути використана у військових цілях. Ці мережі підтримують швидку передачу великих обсягів даних. Цивільне населення знайоме з мобільними мережами, що робить їх корисними для поширення інформації.

Стільникові мережі дуже вразливі до фізичного руйнування та кібератак. Під час криз ці мережі можуть бути легко перевантажені. Існує ризик того, що супротивники можуть використовувати цивільні мережі для збору розвідувальної інформації.

Мобільні вежі, що розгортаються, є життєво важливими для швидкого відновлення інфраструктури. Забезпечення захисту стільникових мереж від перехоплення та підміни є критично важливим. Ефективні протоколи управління перевантаженням мережі під час кризових ситуацій необхідні для операційного успіху.

2.3.6 Програми для безпечного обміну повідомленнями

Програми для безпечного обміну повідомленнями забезпечують надійне шифрування конфіденційних повідомлень. Ці програми, як правило, прості у використанні, що сприяє швидкому освоєнню їх персоналом. Широко доступні на комерційних смартфонах, що робить їх доступними в більшості середовищ.

Ці програми покладаються на комерційну інфраструктуру, яка не завжди може бути безпечною або доступною. Безпека пристроїв може бути слабким місцем. Помилки користувачів можуть призвести до значних порушень операційної безпеки.

Впровадження суворих протоколів операційної безпеки має важливе значення при використанні комерційних додатків. Існує потреба у перевірці або розробці спеціальних платформ безпечного обміну повідомленнями для військових. Ці додатки цінні для швидкого, неформального спілкування та цивільної координації.

2.3.7 Порівняльний аналіз сучасних систем військового зв’язку

Результати порівняння сучасних систем військового зв’язку представлені в табл. 2.2.

Таблиця 2.2 – Порівняльний аналіз сучасних систем військового зв’язку

Вид системи	Переваги	Проблеми	Перспективи
1	*2*	*3*	*4*
Системи LTE	- висока пропускна здатність; - інтероперабельність; - мінімум витрат на навчання	- вразливість (схильність до глушіння та перехоплення); - інфраструктурна залежність; - перевантаження	- гнучкість в умовах пошкодженої інфраструктури; - супутникова інтеграція; - зміцнення мережі і її захисту
Системи супутникового зв’язку	- глобальне покриття; - стійкість; - висока пропускна здатність	- вразливість до глушіння; - затримка сигналу; - висока вартість	- надмірність через диверсифікацію; - швидке розгортання; - зручні інтерфейси; - заходи проти перешкод
Тактичні радіомережі	- військово-специфічний дизайн; - міцність; - надійне шифрування	- обмеження пропускної здатності; - складність інтеграції; - боротьба з РЕБ	- підвищення гнучкості та адаптивності; - інвестиції у передові технології
Mesh-мережі	- стійкість; - самоформування та самозцілення; - міська ефективність	- обмеження по дальності дії; - складність управління; - ризик виявлення	- резервний зв'язок; - інтеграція з системами більшої дальності; - контроль та мінімізація ризиків виявлення

Продовження табл. 2.2.

1	*2*	*3*	*4*
Стільникові мережі	- вже існуюча інфраструктура; - висока пропускна здатність і низька затримка; - мінімум витрат на навчання	- фізична та кібернетична вразливість; - перевантаження; - ризк експлуатації ворогом	- швидке відновлення; - захист мереж; - протоколи управління перевантаженнями
Системи з використанням програм для безпечного обміну повідомленнями	- наскрізне шифрування; - зручність для користувачів; - доступність	- інфраструктурна залежність; - вразливості пристроїв; - ризики операційної безпеки	- впровадження суворих протоколів; - розробка військово-специ-фічних платформ; - утиліта для неформального спілкування

Застосування описаних в табл. 2.2 систем військового зв’язку визначається різними умовами та можливостями, але для максимальної ефективності рекомендується застосовувати всі можливі системи комплексно.

2.4 Засоби для організації військового зв’язку

Засоби військового зв’язку – це засоби, що призначені для передавання та (або) приймання інформації, доставки секретних та поштових відправлень в системі військового зв’язку і автоматизації [1]. Класифікація засобів зв’язку відповідно до [1, 2] представлено на рис. 2.6.

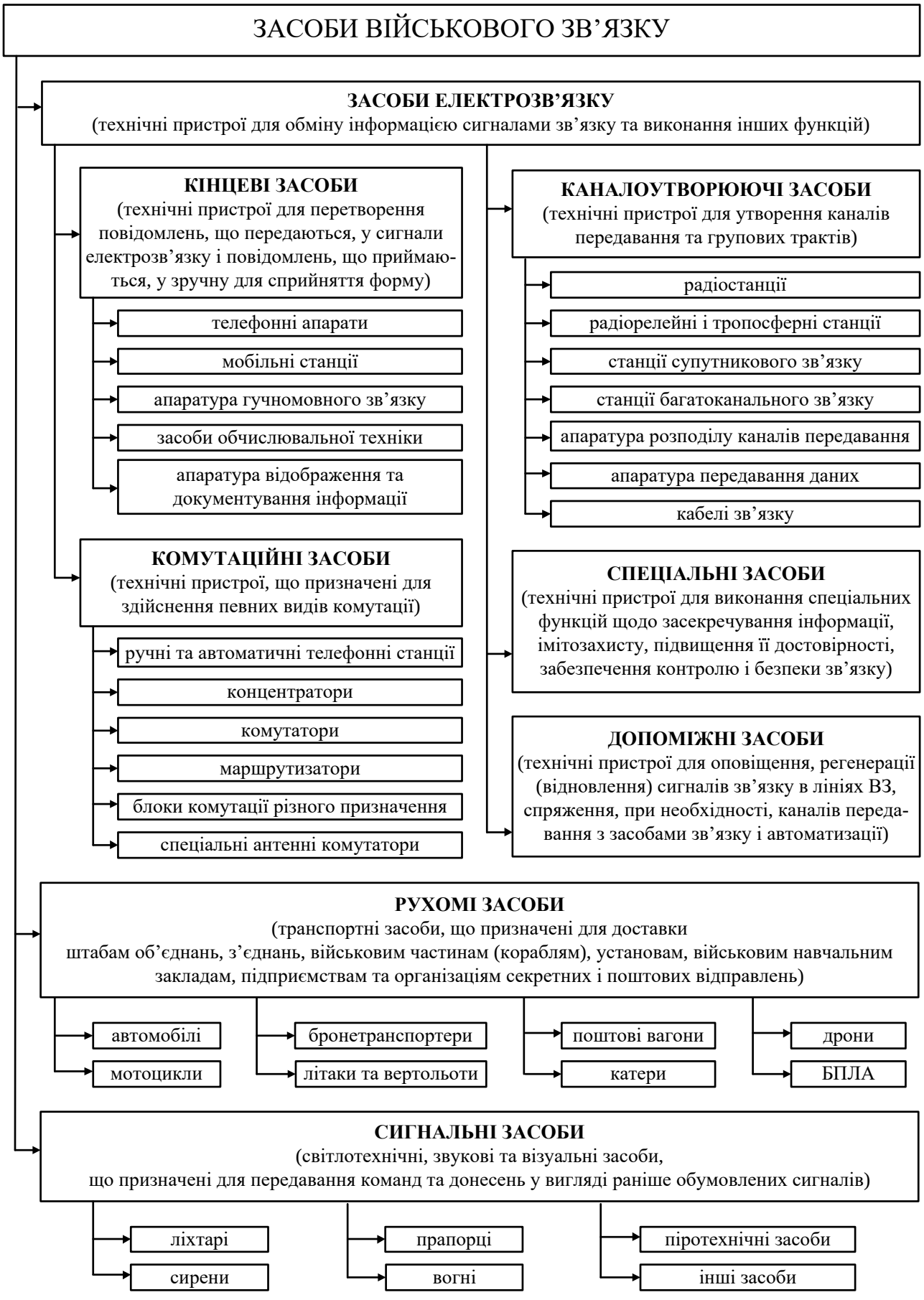

Рисунок 2.6 – Класифікація засобів військового зв'язку

Значення і роль засобів військового зв'язку, визначаються їхніми тактико-технічними даними, що змінюються в залежності від характеру бойових дій та обставин, що складаються. Основними засобами зв'язку є ті засоби, що в конкретних умовах найбільш повно забезпечують необхідні вимоги та потреби управління військами.

3 ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ВЗ

3.1 Огляд сучасних засобів військового зв’язку

Сучасні засоби військового зв’язку (ЗВЗ) розроблені для роботи в найскладніших умовах та сценаріях. Деякі ключові характеристики сучасних ЗВЗ роблять їх винятковими та максимально популярними. До таких характеристик сьогодні відносяться: шифрування та безпека, взаємосумісність, надійність, висока швидкість передачі та інтеграція з передовими технологіями [15].

Сучасні військові операції вимагають стійких засобів зв'язку, проте такі загрози, як кібератаки, радіоелектронна війна та складна місцевість, створюють значні перешкоди [16]. Системи оборонного зв'язку повинні шифрувати всі повідомлення, щоб запобігти перехопленню та несанкціонованому доступу противника. Це вимагає захисту даних як у стані спокою, так і під час передачі, використовуючи передові криптографічні методи, що відповідають стандартам військового рівня. З огляду на чутливий характер армійського зв'язку, сучасні військові пристрої для зв'язку оснащені передовими протоколами шифрування, які запобігають прослуховуванню та несанкціонованому доступу.

Сучасні ЗВЗ можуть безперебійно працювати на різних платформах та в різних підрозділах. Ця сумісність з різними системами та стандартами є вирішальною для координації.

Військові пристрої створені для роботи в екстремальних умовах, таких як суворі погодні умови, електромагнітні перешкоди та фізичний вплив. Лінії армійського зв'язку повинні залишатися відкритими навіть за несприятливих обставин.

Швидка та ефективна передача даних є важливою частиною прийняття рішень у режимі реального часу. Військові комунікаційні пристрої все частіше

використовують технології, які пропонують вищу пропускну здатність та меншу затримку.

Інтеграція інтеграція з передовими технологіями (штучний інтелект, машинне навчання, LiFi тощо) пропонує нові можливості, такі як автоматизована підтримка рішень та краща безпека [15].

Згідно джерелу [15] найкращими сучасними ЗВЗ у 2024 – 2025 роках є засоби, що наведенві на рис. 3.1.

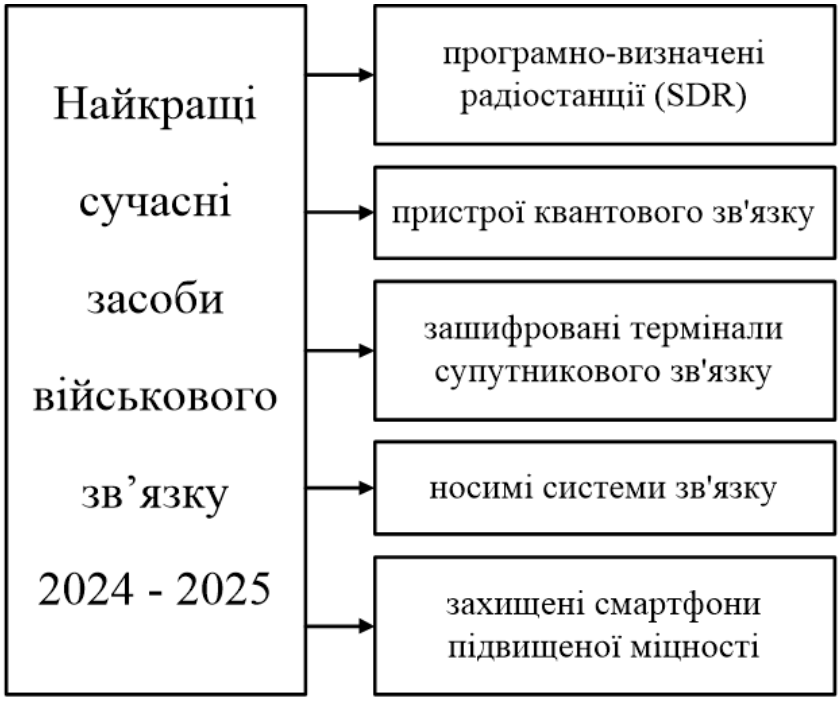

Рисунок 3.1 – Найкращі сучасні ЗВЗ

Програмно-визначені радіостанції (SDR) це універсальні комунікаційні пристрої, які можна легко налаштувати для роботи на різних частотах і протоколах. Ці радіостанції використовують програмне забезпечення для керування функціями зв'язку. Така гнучкість робить їх ідеальними для різних вимог місій та середовищ. У армійському зв'язку SDR важливі, оскільки вони можуть шифрувати повідомлення, обробляти сигнали та ефективно передавати дані. SDR можуть взаємодіяти через різні мережі та з іншими пристроями. Вони підходять для спільних операцій за участю кількох видів збройних сил та

військ. Гнучкість SDR дозволяє їм швидко адаптуватися до нових частот і режимів. Вони можуть протидіяти радіоелектронним перешкодам і забезпечувати безперервний армійський зв'язок. SDR можуть бути розгорнуті в постраждалих від стихійного лиха районах для створення військових мереж зв'язку. Це сприяє координації між військовими частинами, неурядовими організаціями та місцевою владою.

Засоби квантового зв'язку використовують принципи квантової механіки для досягнення надбезпечної передачі даних. Ці військові комунікаційні пристрої використовують квантовий розподіл ключів (QKD) для створення практично незламних ключів шифрування. Якщо робиться спроба перехопити зв'язок, квантовий стан даних змінюється, негайно попереджаючи користувачів про порушення. Засоби квантового зв'язку можна використовувати для безпечної передачі конфіденційних даних між командними центрами та польовими підрозділами. Вони захищають дані навіть від найскладніших кіберзагроз. Завдяки цій технології у військових супутниках можна встановити безпечні канали зв'язку для міжконтинентального зв'язку. Це ідеально підходить для стратегічних операцій, що вимагають високого рівня конфіденційності [15].

Зашифровані термінали супутникового зв'язку оснащені суворим шифруванням, забезпечують безпечні та надійні канали зв'язку на великих відстанях. Ці військові пристрої для зв'язку захищають від несанкціонованого доступу, що робить їх незамінними для підтримки безпечних ліній зв'язку як у віддалених, так і у ворожих середовищах. Ці термінали розроблені, щоб витримувати екстремальні погодні умови та засоби радіоелектронної боротьби, щоб зв'язок залишався безперебійним. Вони ідеально підходять для місій, що виходять за межі можливостей наземних систем зв'язку, таких як розвідувальні та спостережні операції. Ці термінали забезпечують безпечну передачу конфіденційної інформації до центрального командування та з нього, навіть через континенти. У разі збою наземної мережі супутниковий зв'язок слугує надійною резервною копією для підтримки безперервного зв'язку.

Носимі системи зв'язку розроблені для забезпечення солдатів надійним та вільним від рук способом зв'язку на полі бою. Ці системи інтегрують комунікаційні пристрої в шоломи, жилети чи інше спорядження. Це дозволяє їм легко спілкуватися за допомогою голосу, відео та обміну даними. Найновіші досягнення в цій галузі включають дисплеї доповненої реальності (AR) та біометричні датчики для повної ситуаційної обізнаності [15]. Носимі системи допомагають кожному солдату підтримувати зв'язок зі своїм підрозділом та командуванням. Така координація та швидке реагування є критично важливими під час місій. Завдяки носимим ЗВЗ з підтримкою доповненої реальності, солдати можуть переглядати карти в режимі реального часу, позиції противника та цілі місії безпосередньо у своєму полі зору. Крім того, інтегровані біометричні датчики можуть відстежувати показники здоров'я солдатів. Ці дані передаються медикам для надання оперативної медичної допомоги за потреби.

Захищені смартфони підвищеної міцності спеціально розроблені для армійського зв'язку, мають міцний корпус та можливості шифрування. Вони створені для того, щоб витримувати екстремальні температури, занурення у воду, пил та фізичні удари. Окрім міцного корпусу, ці пристрої забезпечують безпечний зв'язок та передачу даних. Це робить їх непроникними для злому та прослуховування. Вони пропонують гнучкість комерційних смартфонів, водночас задовольняючи вимоги військового рівня. Ці пристрої ідеально підходять для використання в польових умовах, забезпечуючи солдатам безпечні канали зв'язку та доступ до критично важливих програм. Вони дозволяють обмінюватися зображеннями, відео та іншими даними в режимі реального часу. Це допомагає швидко приймати рішення та бути обізнаним з ситуацією як на полі, так і поза ним. Так само як і інші носимі ЗВЗ в них інтегровані біометричні датчики для відстеження показників здоров'я та реалізована можливість передавати дані медикам.

3.2 Порівняльний аналіз SDR

Програмно-визначені радіостанції (SDR) революціонізували методи проектування та впровадження радіосистем. Завдяки своїй гнучкості та універсальності, ці приймально-передавальні системи стають дедалі поширенішими в різних радіочастотних застосуваннях, включаючи телекомунікації, тестування пристроїв, станції 5G, інтернет речей (IoT) тощо. Зокрема, високопродуктивні SDR стали важливим інструментом у критично важливих оборонних застосуваннях, таких як радар, моніторинг спектру, радіорозвідка, радіоелектронна боротьба та супутниковий зв'язок [17].

SDR – це такі системи радіозв'язку, в яких всі або деякі функції фізичного рівня, як правило реалізовані на аналоговому обладнанні (наприклад змішувачі, фільтри тощо), але визначаються та виконуються за допомогою програмного забезпечення на програмованих процесорах, таких як універсальні комп'ютери, цифрові сигнальні процесори або програмовані польовими елементами вентильні матриці [18]. Такий підхід забезпечує можливість реконфігурації, багаторежимну роботу в різних діапазонах частот та адаптацію до різних бездротових стандартів без необхідності модифікації обладнання, що робить SDR важливими для застосування в ізних галузях, зокрема у військовому зв’язку. Важливою перевагою SDR є можливість отримання багатьох функцій і сервісів в одному компактному корпусі [19].

Перелік SDR охоплює різноманітний спектр апаратних платформ, від недорогих USB-адаптерів, що використовуються для радіоприйому, до складних продуктивних SDR, які підтримують високошвидкісну роботу в повнодуплексному режимі. Недорогі приймачі (такі як наприклад RTL-SDR) здобули популярність для спектрального аналізу та моніторингу сигналів завдяки своїй доступності. Професійні пристрої (такі як наприклад Ettus Research USRP X410) забезпечують високу пропускну здатність та вихідну потужність та широко використовуються в промислових умовах для створення передових безпроводових систем [18].

Порівняльний аналіз доступних апаратних платформ для SDR з відкритим кодом представлено в табл. 3.1. Дані для порівняння взято з [20].

Таблиця 3.1 – Порівняння доступних апаратних платформ для SDR з відкритим кодом

SDR	USRP B210	LimeSDR	HackRF One	ADALM Pluto	RTL-SDR
Радіочастотний діапазон	70 МГц – 6 ГГц	100 кГц – 3,8 ГГц	1 МГц – 6 ГГц	325 МГц – 3,8/6 ГГц	500 кГц – 1,766 ГГц
Пропускна здатність, МГц	61,44	61,44	20	20	2,4
АЦП, біт	12	12	8	12	8
MIMO	2×2	2×2	немає	немає	немає
ПЛІС	Xilinx Spartan-6	Altera Cyclone IV	немає	Xilinx Zynq Z-7010	немає
Дуплекс	повний	повний	напів-дуплекс	повний	тільки приойм
Середня вартість, грн	30000	20000	15000	11000	2000

Доступні SDR чудово підходять для освітнього та рекреаційного використання, наприклад для відстеження сигналів з літаків для моніторингу польотів у режимі реального часу та виконання базового спектрального аналізу для візуалізації заповненості сигналу. Деякі доступні SDR широко використовуються в установках, що забезпечують надійний прийом до 200

морських миль за допомогою простої антени [18]. Їхня доступність сприяє розвитку різних проектів, де немає необхідності використання функції передачі.

Професійні платформи охоплюють високоякісні приймально-передавальні SDR, розроблені для вимогливих застосувань, зокрема в оборонній промисловості, з акцентом на масштабованості, надійності та інтеграції з передовими можливостями обробки [18]. Такі системи підтримують повнодуплексний режим роботи та широкі діапазони частот, обслуговуючи військовослужбовців та телекомунікаційні компанії, яким потрібна надійна продуктивність для масштабних розгортань.

Потужні SDR характеризуються своїми апаратними можливостями та критичними параметрами продуктивності, такими як діапазон налаштування, кількість каналів, пропускна здатність, цифровий транспортний канал тощо. Оцінюючи ці показники, розробники можуть вибрати оптимальний варіант SDR для своїх застосувань, оскільки жодне рішення не може відповідати всім можливим варіантам використання [17].

При виборі SDR для систем радіоелектронної боротьби та оборони важливими є 4 ключові показники: діапазон налаштування, кількість каналів, смуга пропускання дискретизації та цифровий транспортний канал. Ці параметри є вирішальними для визначення здатності SDR ефективно працювати в цих застосуваннях.

Діапазон налаштування визначає діапазон частот, на яких SDR може приймати та передавати сигнали з номінальним посиленням. Широкий діапазон налаштування є важливим для таких застосувань, як моніторинг спектру та радіоелектронна боротьба, де здатність автоматично налаштовуватися та швидко перемикатися між різними частотами є критично важливою для точності, безпеки та працездатності. Наприклад, SDR з широким діапазоном налаштування в системах радіоелектронної боротьби може швидко виявляти ворожі радіолокаційні системи та автоматично налаштовувати ланцюг передачі

для генерації сигналів перешкод. Аналогічно, радари можуть використовувати протоколи стрибкоподібної зміни частоти, щоб уникнути перешкод.

Кількість каналів SDR є ще одним важливим параметром, який стосується кількості незалежних радіоланцюгів, які може підтримувати SDR. У таких застосуваннях, як радіолокація та розвідувальна система розвідки, велика кількість каналів дозволяє одночасно обробляти кілька сигналів, що також називається роботою з кількома входами та кількома виходами (MIMO). Наприклад, у радіолокаційних застосуваннях MIMO SDR може одночасно обробляти численні радіолокаційні сигнали, що дозволяє точніше відстежувати цілі, ідентифікувати їх, а також використовувати методи формування/керування променем за допомогою антенних решіток [17].

Ширина смуги пропускання визначає максимальний діапазон частот, який SDR може дискретизувати, зрештою обмежуючи діапазон миттєвого виявлення частоти на канал. Висока смуга пропускання дискретизації є важливою для таких застосувань, як радіолокаційний та спектральний моніторинг, де захоплення та обробка великих обсягів даних є критично важливими. Наприклад, у застосуваннях спектрального моніторингу SDR з високою смугою пропускання дискретизації може одночасно захоплювати значну частину радіочастотного спектру, збільшуючи ймовірність перехоплення сигналу.

Цифровий зворотний зв'язок стосується здатності SDR передавати та приймати дані через цифровий інтерфейс. Ця характеристика особливо важлива в таких застосуваннях, як електронна війна, де здатність швидко обробляти та аналізувати великі обсяги даних є важливою. SDR з високошвидкісним цифровим зворотним зв'язком може швидко передавати дані до інших систем для подальшого аналізу, обробки та зберігання з мінімальними втратами інформації.

В даній роботі для порівняння був обрані найбільш потужні SDR, що використовуються для військового зв’язку. Порівняльний аналіз представлено в табл. 3.2.

Таблиця 3.2 – Порівняння високопродуктивних SDR

SDR	Per Vices Cyan	NI USRP X410	Herrick Labs HTLw
Ядро	Однокристальна система Intel Stratix 10 / ARM Cortex-A53 MPCore	Xilinx Zynq Ultrascale+ ZU28DR РЧ-система / 4-ядерний ARM Cortex-A53	Невизначена FPGA з ядрами ARM9/ співпроцесори NEON
Діапазон налаштування	майже постійний струм до 18 ГГц	від 1 МГц до 8 ГГц	від 20 МГц до 18 ГГц
Роздільна здатність	32-бітний	12-бітний АЦП, 14-бітний ЦАП	–
Дінамічний діапазон	60 дБ	–	80 дБ
Кількість каналів	16 передав. /прийм.	4 передав., 4 прийм.	4 передав., 4 прийм.
Пропускна здатність	3 ГГц на канал	400 МГц на канал	1 ГГц на канал
Цифровий зворотний зв'язок	4x 40/100 Гбіт/с qSFP+	2x 10/100 GbE qSFP28	2x 10GbE Ethernet
Габарити	48,26 x 40,2 x 13,3 (см), 6,2 кг	28,5 × 22,2 × 4,4 (см), 2,5 кг	–

Кожна з порівняних SDR (Per Vices Cyan, NI USRP X410 та Herrick Labs HTLw) демонструє виняткові апаратні можливості за аналізованими параметрами та широкий діапазон застосування в цільовій галузі.

Всі розглянуті SDR – це універсальні та потужні інструменти, що добре підходять для широкого спектру застосувань в оборонній промисловості, що робить їх сильними конкурентами на ринку високопродуктивних SDR.

З таблиці видно, що Per Vices Cyan має найвищу миттєву пропускну здатність та найбільшу кількість каналів з усіх трьох, що робить її дуже придатною для радіолокацій, моніторингу спектру, обладнання для розвідки та радіоелектронної боротьби, постановників перешкод, протидії перешкодам та загальних пристроїв радіоелектронної боротьби. Висока пропускна здатність також робить її корисною для обробки великих обсягів даних у режимі реального часу, що додатково забезпечується потужним зворотним каналом на основі qSFP+ [17]. Однак, це може бути не найкращим варіантом для застосувань з обмеженнями розміру, ваги та потужності (SWaP). Herrick Labs HTLw забезпечує аналогічні частотні характеристики зі значно меншими габаритами за рахунок меншої кількості каналів та пропускної здатності цифрового зворотного каналу, що робить його кращим для застосувань, які потребують дуже низького SWaP та високочастотної продуктивності. HTLw забезпечує вищий динамічний діапазон, що чудово підходить для підвищення точності та надійності. Однак швидкість зворотного каналу нижча, ніж у інших розглянутих SDR, що може бути обмеженням для високошвидкісних застосувань з величезними обсягами даних. Хоча NI USRP X410 забезпечує дещо меншу загальну продуктивність з точки зору частоти, її малі габарити та архітектура з відкритим вихідним кодом роблять її чудовим вибором для швидкого прототипування та некритичних застосувань, оскільки вона пропонує більше вбудованої розробки.

Аналіз результатів порівняння найпродуктивніших SDR показав, що всі три SDR забезпечують вражаючі можливості та функції. Хоча кожна SDR має свої переваги та недоліки, розуміння параметрів продуктивності та їхніх переваг для конкретних застосувань є вирішальним при виборі оптимального рішення для конкретного випадку використання.

3.3 Порівняння та вибір оптимального військового смартфону

Військовий смартфон (або смартфон військового класу) – це міцний, довговічний мобільний пристрій, розроблений для роботи в екстремальних умовах навколишнього середовища та жорсткого поводження, який часто використовують військовослужбовці, правоохоронні органи та фахівці у складних галузях, таких як будівництво, гірничодобувна промисловість та дослідження довкілля [21]. Ці телефони створені відповідно до військових стандартів міцності, водонепроникності та ударостійкості або навіть перевищують їх. Смартфони військового класу доводять свою цінність у певних операційних умовах, де стандартні пристрої повністю виходять з ладу. Основні характеристики смартфонів військового класу наведено на рис. 3.2.

Рисунок 3.2 – Основні характеристики військових смартфонів

Військові підрозділи потребують повної інтеграції безпеки, де апаратне шифрування, протоколи безпечного зв'язку та фізичне посилення працюють як єдині системи. Захист військового рівня означає довговічність та поєднує міцне

обладнання з передовими функціями безпеки, яких вимагають військові та оборонні установи. Сертифікація MIL-STD-810H – це військовий стандарт для смартфонів, що працюють в екстремальних умовах, проходять тестування на падіння, екстремальні температури та вологу (в 28 різних умовах навколишнього середовища). Смартфони військового класу пропонують високу обчислювальну потужність та додають спеціалізовані рівні міцності, вони поєднують тактичну довговічність із практичною повсякденною функціональністю [22].

Для виконання вибору оптимального військового смартфону були проаналізовані 12 найкращих моделей смартфонів військового класу у 2025 році згідно [22 – 24]:

1) Oukitel WP39 Pro,
2) Doogee V Max Pro,
3) Samsung Galaxy XCover 7 Pro,
4) AGM H6,
5) Caterpillar Cat S75,
6) AGM Glory G1S,
7) Caterpillar Cat S62 Pro,
8) Blackview BV9900 Pro,
9) Ulefone Armor 11T 5G,
10) Doogee S97 Pro,
11) Ulefone Power Armor 16 S,
12) JCB Toughphone.

Обрані військові смартфони були порівняні за 15 параметрами: характеристики дисплея, роздільна здатність, процесор, оперативна пам'ять, вбудована пам'ять, основна камера, фронтальна камера, акумулятор, вага, захист від пилу та води, захист від ударів та падінь, матеріал корпусу, захист скла, наявність спеціальних функцій та вартість. Результати порівняння представлено в табл. 3.3.

Таблиця 3.3 – Порівняння найкращих моделей військових смартфонів

	Oukitel WP39 Pro	Doogee V Max Pro	Samsung Galaxy XCover 7 Pro	AGM H6	Caterpillar Cat S75	AGM Glory G1S
Дисплей	6,6"	6,58"	6,6 "	6,56"	6,6"	6,53"
Роздільна здатність	2408x1080	2408x1080	2408x1080	1612 x 720	2160 x 1080	2160 x 1080
Процесор	Dimensity 6300	Dimensity 7050	Qualcomm Snapdragon 7S Gen 3	Unisoc T606	MediaTek Dimensity D930 2,2 ГГц	Qualcomm Snapdragon 480 5G
Оперативна пам'ять, Гб	12	12	6	16	6	8
Вбудована пам'ять, Гб	512	512	128	256	128	128
Основна камера, Мп	64 +8 +2, нічне бачення	108 + 20 +8, нічне бачення	50 + 8	50 + 2	50 + 8 + 2	48 + 20 + 2, нічне бачення
Фронтальна камера, Мп	32	16	13	8	8	16
Акумулятор, мАг	11 000	22000	4350	4900	5000	5500
Вага, г	368	536	240	240	268	315
Захист від пилу та води	IP68, IP69K	IP68, IP69K	IP68	IP68, IP69K	IP68, IP69K	IP69K
Захист від ударів, падінь	MIL-STD-810H	MIL-STD-810H	MIL-STD-810H	MIL-STD-810G	MIL-STD-810H	так
Корпус	Метал, пластик	Алюміній, метал, пластик, полікарбонат, гума	Пластик, шкіра	Пластик, полікарбонат, термо-пластичний поліуретан	Пластик, алюміній	Прогумо-ваний пластик
Захист скла	Corning Gorilla Glass 5	Corning Gorilla Glass 7	Corning Gorilla Glass Victus+	Corning Gorilla Glass	Gorilla Glass Victus	Corning Gorilla Glass 5
Спеціальні функції	Компас, гіроскоп, датчик наближення, акселерометр	Датчик освітленості, датчик наближення, гіроскоп, компас	Датчик наближення, датчик освітлення, гіроскоп, акселерометр	Датчик наближення, датчик світла, акселерометр, компас	Тепловізор, акселерометр, датчик наближення, гіроскоп	Тепловізор
Вартість, грн	10000	15000	14000	8500	16000	25000

Продовження табл. 3.3

	Caterpillar Cat S62 Pro	Blackview BV9900 Pro	Ulefone Armor 11T 5G	Doogee S97 Pro	Ulefone Power Armor 16 S	JCB Toughphone
Дисплей	5.7"	5.84"	6.1"	6.39"	5.93"	5.7 "
Роздільна здатність	2160 x 1080	2280x1080	1560x720	1560 x 720	720x1440	1520x720
Процесор	Qualcomm Snapdragon 660	Helio P90	MediaTek Dimensity 800	MediaTek Helio G95	Tiger T616	Helio G85
Оперативна пам'ять, Гб	6	8	8	8	8	6
Вбудована пам'ять	128	128	256	128	128	128
Основна камера, Мп	12	48 + 5 + 2	48 + 5 + 2 + 2	48 + 8 + 2 + 2	50+2	20
Фронтальна камера, Мп	8	16	16	16	8	20
Акумулятор, мАг	4000	4380	5200	8500	9600	4050
Вага, г	248	273	293	346	406	204
Захист від пилу та води	IP68, IP69	IP68, IP69	IP68, IP69K	IP68	IP68, IP69K	IP68
Захист від ударів, падінь	MIL-STD-810H	MIL-STD-810H	MIL-STD-810G	так	MIL-STD-810H	MIL-STD-810
Корпус	Високоміцн. алюміній	Метал, пластик	Метал, пластик	Метал, пластик	Пластик	Пластик
Захист скла	Corning Gorilla Glass 6	Corning Gorilla Glass 5	Corning Gorilla Glass 5	Corning Gorilla Glass 5	Gorilla Glass	Gorilla Glass v3
Спеціальні функції	Тепловізор	Тепловізор, акселерометр, барометр, гіроскоп, датчик освітлення, датчик наближення, компас	Акселерометр, барометр, гіроскоп, датчик освітлення, датчик наближення, компас	Гіроскоп, датчик освітлення, датчик наближення, компас, лазерний дальномер	Датчик освітлення	Датчик освітлення, компас
Вартість, грн	19000	28000	11000	9000	8000	12000

Порівняння великої кількості альтернатив за великою сукупністю параметрів (показників якості) є складною задачею, саме тому для коректності та об’єктивності результатів порівняння необхідно застосовувати методи багатокритеріальної оптимізації та прийняття рішень.

Вибір оптимального варіанту з множини допустимих альтернатив з урахуванням сукупності показників якості виконується згідно методики та методів, що детально описана в джерелах [25 – 29]. Дані методи широко використовуються в останні роки для вирішення багатокритеріальних задач в інформаційно-комунікацій галузі.

Послідовність етапів виконання вибору оптимального варіанту на основі багатокритеріального аналізу наведено на рис. 3.3.

Рисунок 3.3 – Етапи вибору оптимального варіанту

Постановка задачі – визначити оптимальний військовий смартфон. Множина допустимих варіантів – 12 моделей військових смартфонів, представлена в табл. 3.3.

Вибір показників якості виконано шляхом визначення найбільш важливих характеристик з параметів, що описані в табл. 3.3. Таким чином для вибору оптимального варіанту порівняємо моделі смартфонів (табл. 3.4) за такими параметрами (показниками якості): розмір дисплея (k_1), оперативна пам'ять (k_2), вбудована пам'ять (k_3), основна камера (k_4), акумулятор (k_5), вага (k_6), захист від пилу та води (k_7), захист від ударів та падінь (k_8), кількість спеціальних функцій (в тому числі наявність нічного бачення, тепловізора тощо) (k_9) та вартість (k_{10}).

Таблиця 3.4 – Показники якості для кожного військового смартфону

№	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
	max	max	max	max	max	min	max	max	max	min
1	6,6	12	512	64	11000	368	3	3	5	10000
2	6,58	12	512	108	22000	536	3	3	4	15000
3	6,6	6	128	50	4350	240	1	3	4	14000
4	6,56	16	256	50	4900	240	3	2	4	8500
5	6,6	6	128	50	5000	268	3	3	5	16000
6	6,53	8	128	48	5500	315	2	1	2	25000
7	5,7	6	128	12	4000	248	2	3	2	19000
8	5,84	8	128	48	4380	273	2	3	8	28000
9	6,1	8	256	48	5200	293	3	2	6	11000
10	6,39	8	128	48	8500	346	1	1	5	9000
11	5,93	8	128	50	9600	406	3	3	1	8000
12	5,7	6	128	20	4050	204	1	1	2	12000

Спочатку необхідно привести показники якості до стандартного вигляду, а саме: всі значення показників треба нормувати до максимального значення:

$$k_{iн} = \frac{k_i}{k_{\max}}, \tag{3.1}$$

а потім виконати інвертування для тих показників, які потребують максимізації для покращення рішення:

$$k_{ic} = 1 - k_i \ . \tag{3.2}$$

В нашому випадку мінімізації потребують параметри k_6 і $k_{10,}$ а максимізації потребують параметри: k_1, k_2, k_3, k_4, k_5, k_7, k_8, k_9 – саме для них необхідно виконати інвертування. Після виконання дій (3.1) та (3.2) отримано таблицю стандартних показників якості для всіх смартфонів.

Таблиця 3.5 – Показники якості у стандартному вигляді для кожного військового смартфону

№	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
	min	min	min	min	min	min	min	min	min	min
1	0	0,25	0	0,407	0,5	0,687	0	0	0,25	0,357
2	0,003	0,25	0	0	0	1	0	0	0,375	0,536
3	0	0,625	0,75	0,537	0,802	0,448	0,667	0	0,5	0,5
4	0,006	0	0,5	0,537	0,777	0,448	0	0,333	0,5	0,304
5	0	0,625	0,75	0,537	0,773	0,5	0	0	0,375	0,571
6	0,011	0,5	0,75	0,556	0,75	0,588	0,333	0,667	0,625	0,893
7	0,136	0,625	0,75	0,889	0,818	0,463	0,333	0	0,75	0,679
8	0,115	0,5	0,75	0,556	0,801	0,509	0,333	0	0	1
9	0,076	0,5	0,5	0,556	0,764	0,547	0	0,333	0,25	0,393
10	0,032	0,5	0,75	0,556	0,614	0,646	0,667	0,667	0,375	0,321
11	0,102	0,5	0,75	0,537	0,564	0,757	0	0	0,875	0,286
12	0,136	0,625	0,75	0,815	0,816	0,381	0,667	0,667	0,75	0,429

Парето-оптимізація була виконана за формулою:

$$P(Y) = opt_{\geq} Y = \left\{ \vec{f}(x^o) \in Y : \nexists\ \vec{f}(x) \in Y : \vec{f}(x) \geq \vec{f}(x^o) \right\}. \quad (3.3)$$

В результаті виконання Парето-оптимізації виявилося, що за безумовним критерієм переваги всі системи є Парето-оптимальними. Жоден варіант не виявився безумовно гіршим, оскільки сукупність показників якості є дуже великою.

Для вибору єдиного варіанта з множини Парето було використано метод на основі теорії корисності. Для цього для кожного показника якості було задано відносний коефіцієнт корисності (важливості), що наведено в табл. 3.6.

Таблиця 3.6 – Коефіцієнти важливості показників якості

Показник якості	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}
c_j	0,05	0,05	0,05	0,05	0,11	0,15	0,12	0,12	0,15	0,15

Після цього для кожного варіанта військового смартфона було розраховано скалярну цільову функцію за формулою:

$$F(k_1, k_2, ..., k_m) = \sum_{j=1}^{m} c_j k_j, \quad (3.4)$$

де c_j - коефіцієнти відносної важливості показників якості, $\sum_{j=1}^{m} c_j = 1$,

k_j - показники якості у стандартному вигляді [25 – 29].

Результати розрахунків:

$F_1 = 0{,}05 \cdot 0 + 0{,}05 \cdot 0.25 + 0{,}05 \cdot 0 + 0{,}05 \cdot 0{,}407 + 0{,}11 \cdot 0{,}5 + 0{,}15 \cdot 0{,}687 + 0{,}12 \cdot 0 +$
$+ 0{,}12 \cdot 0 + 0{,}15 \cdot 0{,}25 + 0{,}15 \cdot 0{,}357 = 0{,}282$;

$F_2 = 0{,}05 \cdot 0{,}003 + 0{,}05 \cdot 0.25 + 0{,}05 \cdot 0 + 0{,}05 \cdot 0 + 0{,}11 \cdot 0 + 0{,}15 \cdot 1 + 0{,}12 \cdot 0 +$
$+ 0{,}12 \cdot 0 + 0{,}15 \cdot 0{,}375 + 0{,}15 \cdot 0{,}536 = 0{,}293$;

$F_3 = 0{,}05 \cdot 0 + 0{,}05 \cdot 0.625 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}537 + 0{,}11 \cdot 0{,}802 + 0{,}15 \cdot 0{,}448 +$
$+ 0{,}12 \cdot 0{,}667 + 0{,}12 \cdot 0 + 0{,}15 \cdot 0{,}5 + 0{,}15 \cdot 0{,}5 = 0{,}481$;

$F_4 = 0{,}05 \cdot 0{,}006 + 0{,}05 \cdot 0 + 0{,}05 \cdot 0{,}5 + 0{,}05 \cdot 0{,}537 + 0{,}11 \cdot 0{,}777 + 0{,}15 \cdot 0{,}448 +$
$+ 0{,}12 \cdot 0 + 0{,}12 \cdot 0{,}333 + 0{,}15 \cdot 0{,}5 + 0{,}15 \cdot 0{,}304 = 0{,}365$;

$F_5 = 0{,}05 \cdot 0 + 0{,}05 \cdot 0{,}625 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}537 + 0{,}11 \cdot 0{,}773 + 0{,}15 \cdot 0{,}5 +$
$+ 0{,}12 \cdot 0 + 0{,}12 \cdot 0 + 0{,}15 \cdot 0{,}375 + 0{,}15 \cdot 0{,}571 = 0{,}39$;

$F_6 = 0{,}05 \cdot 0{,}011 + 0{,}05 \cdot 0{,}5 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}556 + 0{,}11 \cdot 0{,}75 + 0{,}15 \cdot 0{,}588 +$
$+ 0{,}12 \cdot 0{,}333 + 0{,}12 \cdot 0{,}667 + 0{,}15 \cdot 0{,}625 + 0{,}15 \cdot 0{,}893 = 0{,}609$;

$F_7 = 0{,}05 \cdot 0{,}136 + 0{,}05 \cdot 0{,}625 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}889 + 0{,}11 \cdot 0{,}818 + 0{,}15 \cdot 0{,}463 +$
$+ 0{,}12 \cdot 0{,}333 + 0{,}12 \cdot 0 + 0{,}15 \cdot 0{,}75 + 0{,}15 \cdot 0{,}679 = 0{,}533$;

$F_8 = 0{,}05 \cdot 0{,}115 + 0{,}05 \cdot 0{,}5 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}556 + 0{,}11 \cdot 0{,}801 + 0{,}15 \cdot 0{,}509 +$
$+ 0{,}12 \cdot 0{,}333 + 0{,}12 \cdot 0 + 0{,}15 \cdot 0 + 0{,}15 \cdot 1 = 0{,}4505$;

$F_9 = 0{,}05 \cdot 0{,}076 + 0{,}05 \cdot 0{,}5 + 0{,}05 \cdot 0{,}5 + 0{,}05 \cdot 0{,}556 + 0{,}11 \cdot 0{,}764 + 0{,}15 \cdot 0{,}547 +$
$+ 0{,}12 \cdot 0 + 0{,}12 \cdot 0{,}333 + 0{,}15 \cdot 0{,}25 + 0{,}15 \cdot 0{,}393 = 0{,}381$;

$F_{10} = 0{,}05 \cdot 0{,}032 + 0{,}05 \cdot 0{,}5 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}556 + 0{,}11 \cdot 0{,}614 + 0{,}15 \cdot 0{,}646 +$
$+ 0{,}12 \cdot 0{,}667 + 0{,}12 \cdot 0{,}667 + 0{,}15 \cdot 0{,}375 + 0{,}15 \cdot 0{,}321 = 0{,}5208$;

$F_{11} = 0{,}05 \cdot 0{,}102 + 0{,}05 \cdot 0{,}5 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}537 + 0{,}11 \cdot 0{,}564 + 0{,}15 \cdot 0{,}757 +$
$+ 0{,}12 \cdot 0 + 0{,}12 \cdot 0 + 0{,}15 \cdot 0{,}875 + 0{,}15 \cdot 0{,}286 = 0{,}4442$;

$F_{12} = 0{,}05 \cdot 0{,}136 + 0{,}05 \cdot 0{,}625 + 0{,}05 \cdot 0{,}75 + 0{,}05 \cdot 0{,}815 + 0{,}11 \cdot 0{,}816 + 0{,}15 \cdot 0{,}381 +$
$+ 0{,}12 \cdot 0{,}667 + 0{,}12 \cdot 0{,}667 + 0{,}15 \cdot 0{,}75 + 0{,}15 \cdot 0{,}429 = 0{,}6001$.

Згідно отриманих значень скалярної цільової функції оптимальним рішенням є варіант №1, оскільки у цього варіанта значення F є найменшим. Таким чином оптимальний варіант – це військовий смартфон Oukitel WP39 Pro.

Oukitel WP39 Pro – один із найновіших захищених смартфонів і один із найкращих військових смартфонів на ринку на даний момент. Oukitel WP39 Pro випущений у 2025 році, має оновлений процесор, більше пам’яті, чіткіший екран, пристойні камери, пропонує гарний баланс між габаритами та функціональністю, має потужний акумулятор (11 000 мАг), клас захисту від пилу та води IP68 та IP69K, а також сертифікацію MIL-STD-810H для захисту від ударів та падінь. Цей смартфон можна сміливо рекомендувати військовим.

4 ПЕРСПЕКТИВИ ПОКРАЩЕННЯ ВІЙСЬКОВОГО ЗВ’ЯЗКУ

4.1 Впровадження новітніх технологій у військовий зв’язок

Поле бою продовжує розвиватися та потребує використання найновіших технологій для підвищення якості, стійкості та можливостей систем та засобів військового зв'язку.

Згідно різним джерелам [5, 12, 15, 16, 30] на даний момент такими новітніми технологіями, що потребують впровадження є наступні:

– квантові комунікації,

– нові супутникові сузір'я,

– штучний інтелект,

– технологія LiFi,

– інтегровані оборонні системи на основі IoT,

– технологія доповненої реальності (AR) тощо.

Технологія квантового зв'язку обіцяє створити канали зв'язку, які неможливо зламати за допомогою квантового шифрування. Ця технологія може значно посилити безпеку військового зв'язку, зробивши його несприйнятливим до традиційних форм перехоплення і злому. Дана технологія використовує принципи квантової механіки для створення захищених каналів зв'язку. Квантова заплутаність може уможливити миттєвий, безпечний зв'язок на величезних відстанях без потреби в традиційній інфраструктурі. У поєднанні з існуючими технологіями квантовий зв'язок може забезпечити новий рівень безпеки в середовищах з високими ставками.

Нові супутникові сузір'я, такі як ті, що розробляються компанією SpaceX та іншими комерційними провайдерами, мають розширити можливості глобального зв'язку. Ці сузір'я обіцяють забезпечити високошвидкісний зв'язок з низькою затримкою по всьому світу, в тому числі у віддалених і спірних

районах.Густа мережа низькоорбітальних супутників може забезпечити майже миттєве глобальне покриття, покращуючи зв'язок навіть у найвіддаленіших місцях. Велика кількість супутників може забезпечити надмірність, гарантуючи безперервний зв'язок, навіть якщо деякі супутники вийдуть з ладу. Ці системи можуть бути інтегровані з існуючими військовими мережами, забезпечуючи універсальну і стійку комунікаційну основу.

Штучний інтелект все частіше інтегрується в комунікаційні системи для підвищення їхньої ефективності, безпеки та адаптивності. ШІ може керувати мережним трафіком, виявляти кіберзагрози та реагувати на них у режимі реального часу, а також оптимізувати шляхи зв'язку для швидкості та надійності. ШІ може автономно керувати та оптимізувати комунікаційні мережі, гарантуючи, що пропускна здатність розподіляється там, де вона найбільше потрібна. Системи, керовані штучним інтелектом, можуть виявляти та зменшувати кіберзагрози швидше, ніж люди-оператори, забезпечуючи додатковий рівень захисту. ШІ може дозволити системам зв'язку динамічно пристосовуватися до мінливих умов на полі бою, забезпечуючи безперебійний зв'язок у складних умовах.

Технологія LiFi використовує світло для передачі даних замість традиційних радіочастот. Такий зв'язок є компактний, портативний і може використовуватися в різних умовах для створення високошвидкісних, безпечних мереж зв'язку. Порівняно з радіохвилями, світлові сигнали менш схильні до перешкод, оскільки вони утримуються в певній області. Це пропонує значну перевагу з точки зору безпеки, оскільки дані можуть передаватися за допомогою світлодіодних ламп, які потребують мало енергії та не схильні до електромагнітних перешкод. LiFi набирає обертів у військових застосуваннях завдяки величезній швидкості передачі даних та покращеним функціям безпеки. Його впровадження у військових пристроях зв'язку може призвести до розробки безпечніших та ефективніших мереж зв'язку. Він ідеально підходить для передових операційних баз та командних центрів. Він забезпечує безпечний зв'язок та гарантує захист конфіденційних даних. Оскільки сигнали LiFi не

проникають крізь стіни, вони дуже ефективні в таємних місіях [15]. Це дозволяє здійснювати безпечний зв'язок, який не може бути легко виявлений або перехоплений ворожими силами.

Інтегровані оборонні системи на основі Інтернету речей на полі бою забезпечить сенсорну інтеграцію в режимі реального часу, прогнозну аналітику та автоматизовану розвідку, а використання доповненої реальності (AR) та голографічних інтерфейсів на полі бою покращить ситуаційну обізнаність та координацію місій [5].

4.2 Рекоменації для покращення військового зв’язку

Війна в Україні підкреслює, що жодна система зв'язку не може відповідати вимогам сучасної війни. Багаторівневий підхід з використанням різних технологій необхідний для забезпечення надмірності, гнучкості та стійкості перед обличчям дій противника і хаосу на полі бою. Забезпечення стійкості та якості сучасного військового зв’язку потребує також дотримання певних рекомендацій для планувальників ВЗ.

В роботі були сформульовані рекомендації для покращення ВЗ (рис. 4.1). Необхідно надавати пріоритет різноманітності та надмірності, оскільки використання різних систем зв'язку дозволить забезпечити безперервну роботу; інвестувати в гнучкі системи, оскільки вони (наприклад програмно-визначені системи) дозволяють швидко адаптуватися до мінливих умов; використовувати комерційні технології; посилювати кібербезпеку та розробляти надійні засоби захисту від електронних та кіберзагроз; бути в готовності до забороненого середовища (наприклад у випадках, коли зв'язок може бути порушений або припинений); використовувати найновіші технології: стежити за розвитком квантового зв'язку, супутникових сузір'їв та штучного інтелекту, щоб інтегрувати ці досягнення в майбутні комунікаційні стратегії. Також необхідно проводити безперервне навчання, оскільки це має вирішальне значення для максимізації ефективності комунікаційних інструментів.З розвитком війни

здатність підтримувати стійкі і адаптивні комунікаційні мережі, посилена новими технологіями, стає вирішальним фактором у досягненні військового успіху.

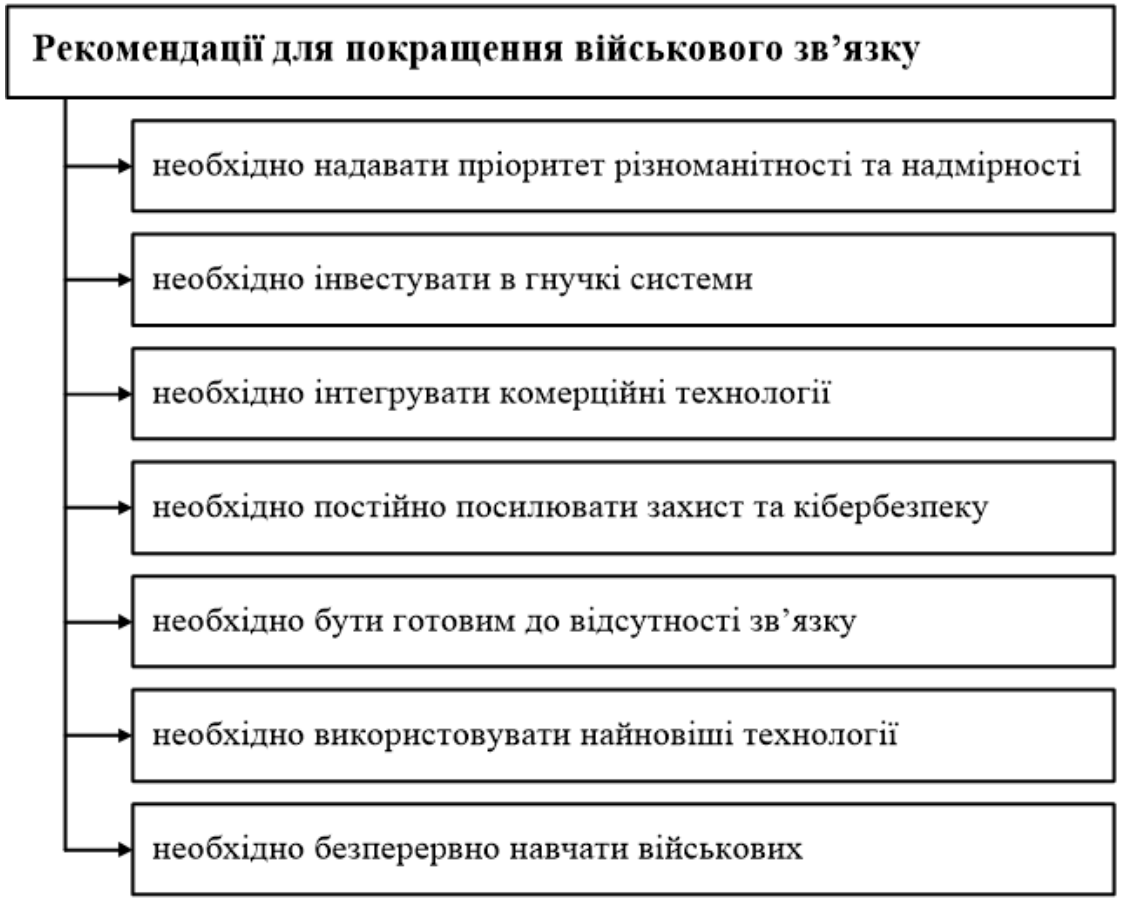

Рисунок 4.1 – Рекомендації для покращення ВЗ

Війна в Україні підкреслює гостру потребу в стійких мережах зв'язку в умовах сучасної війни. Пропонується впроваджувати найсучасніші комунікаційні рішення розроблені для підвищення готовності місії та забезпечення надійного зв'язку в будь-якій ситуації. Рекомендується також використовувати індивідуальні рішення, адаптовані до конкретних оперативних потреб.

ВИСНОВКИ

Сучасні бойові операції фундаментально залежать від зв'язку. Сьогодні військовий зв'язок є центральним елементом досягнення успіху на сучасному полі бою. Надійний, безпечний та своєчасний зв’язок забезпечує ефективне командування та управління, покращує ситуаційну обізнаність та забезпечує скоординовані дії між розосередженими підрозділами.

В роботі було розглянуто та проаналізовано ряд питань, що стосуються систем та засобів військового зв’язку.

В 1-му розділі виконано огляд принципів організації сучасного військового зв’язку та вимог до нього. Виконано аналіз сучасного стану та тенденцій розвитку військового зв’язку.

В 2-му розділі розглянуто структуру та основні характеристики систем військового зв’язку. Виконано порівняльний аналіз сучасних систем військового зв’язку, зокрема системи LTE, системи супутникового зв’язку, тактичні радіомережі, Mesh-мережі, стільникові мережі, системи безпечного обміну повідомленнями.

В 3-му розділі розглянуто сучасні засоби для організації військового зв’язку. Виконано порівняння найпродуктивніших SDR на ринку для критично важливих застосувань радіоелектронної боротьби та оборони, таких як радар, моніторинг спектра та розвідувальна розвідка: Per Vices Cyan, NI USRP X410 та Herrick Labs HTLw. Вони були оцінені за 4 ключовими характеристиками: діапазон налаштування, кількість каналів, смуга пропускання дискретизації та цифровий транспортний канал. Аналіз показав, що всі три SDR забезпечують необхідні можливості та функції. Кожна SDR має свої переваги та недоліки, але при виборі оптимального рішення необхідно враховувати розуміння параметрів продуктивності та їхніх переваг для кожного конкретного випадку застосування.

Також виконано порівняння та вибір оптимального військового смартфону. З 12 смартфонів військового класу (Oukitel WP39 Pro, Doogee V Max Pro, Samsung Galaxy XCover 7 Pro, AGM H6, Caterpillar Cat S75, AGM Glory G1S, Caterpillar Cat S62 Pro, Blackview BV9900 Pro, Ulefone Armor 11T 5G, Doogee S97 Pro, Ulefone Power Armor 16 S, JCB Toughphone) було вибрано оптимальний з урахуванням сукупності 10 показників якості за допомогою методів багатокритеріальної оптимізації. Оптимальним варіантом виявився військовий смартфон Oukitel WP39 Pro, який був випущений в 2025 році та володіє всіма необхідними класами захисту в поєднанні з високими показниками продуктивності, великою кількістю спеціальних військових функцій та доступною вартістю.

В 4-му розділі проведено аналіз перспектив покращення ВЗ, зокрема впровадження новітніх технологій у військовий зв’язок. Також сформовано та запропоновано рекомендації для покращення військового зв’язку.

Впровадження новітніх технологій має вирішальне значення в сучасних військових операціях. Безперешкодна інтеграція різних систем гарантує, що дані і зв'язок можуть безперешкодно передаватися між різними платформами, покращуючи координацію і оперативну ефективність на полі бою.

Щоб відповідати майбутнім викликам, збройні сили повинні інвестувати не лише в передові комунікаційні технології, але й у стійкість систем, навчання користувачів та оперативну інтеграцію. Зв'язок слід планувати, захищати та здійснювати як основну бойову здатність, а не як допоміжну функцію. Побудова безпечних, простих та гнучких комунікаційних мереж є ключем до підтримки ефективності в умовах швидкозмінних, суперечливих ситуацій. У сучасній війні сторона, яка контролює інформацію, часто контролює результат.

Результати кваліфікаційної роботи було апробовано на тринадцятій міжнародній науково-практичній конференції «Проблеми інформатизації» та опубліковано тези доповіді [31] за темою роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Організація військового зв’язку : навчальний посібник / В. Шолудько та ін. Київ: ВІТІ, 2017. 282 с.

2. Глушко А. Організація військового зв’язку: конспект лекцій. Одеса: Одеський державний екологічний університет, 2021. 95 с.

3. Сучасні засоби зв’язку та інфокомунікаційні технології у Збройних Силах України та Національній гвардії України: сьогодення та перспективи застосування / О. Ю. Іохов та ін. *Честь і закон.* 2022. № 4(83). С. 111 – 119. ISSN 2078-7480.

4. Huseynov A. The Strategic Role of Military Communications in Achieving Operational Success in Modern Combat Operations. *Collection of scientific papers «SCIENTIA».* Bern, Swiss Confederation, 2025. Modernization of science and its influence on global processes. С. 68 – 76.

5. Mustafovski R. The Use of Communication Platforms in Military Operations: Enhancing Strategic and Tactical Effectiveness. *Database Systems Journal.* 2025. Vol. XVI. С. 1 – 10.

6. Military Communication Market Size and Share Analysis - Growth Trends and Forecasts (2025 - 2032). *Conerent Market Insights.* 06.08.2025. URL: https://www.coherentmarketinsights.com/industry-reports/military-communication-market.

7. Писаренко Т.В. Аналіз світових технологічних трендів у військовій сфері: монографія [Електронний ресурс] / Т. Писаренко, Т. Кваша, Т. Гаврис та ін., за заг. редакцією Т.В.Писаренко. – К.: УкрІНТЕІ, 2021. – 110 с.

8. Santry P. Military Communications Information Systems Definitions and Policy. *NATO Science and Technology Organization STO-MP-IST-208.* Portsdown West, Fareham, Hampshire, Untited Kingdom, 2025. С. 12-1 – 12-10.

9. Velastegui N. Avances tecnológicos en sistemas y equipos de comunicaciones militares. *Minerva Journal.* 2022. Vol. 3, Issue. 8. P. 61 – 73.

ISSN 2697-3650. URL: https://doi.org/10.47460/minerva.v3i8.65.

10. Nato Standard AJP-6. Allied Joint Doctrine for Communication and Information Systems. Edition A Version 1. February 2017. Published by the Nato Standardization Office. URL: https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDA_V1_E_2525.pdf.

11. ВСТ 01.112.001-2006. Військовий зв'язок та інформаційні системи. Військовий зв'язок. Терміни та визначення. Введ. 03.05.06. – К.: Видавництво стандартів, 2006. – 25 с.

12. Battlefield Communication Networks: Strategic Lessons from Ukraine. *MSSDEFENCE*. 21.08.2024. URL: https://mssdefence.com/blog/battlefield-communication-networks-strategic-lessons-from-ukraine/.

13. Stefano De Luca, Clément Evroux. Satellites: State of play and challenges for the EU. *European Parliament. Briefing.* 29.09.2025. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/777930/EPRS_BRI(2025)777930_EN.pdf.

14. Defense Satcom Systems: The Backbone of Modern Military Communication. A&D. Communication and Electronics. 28.05.2025. URL: https://aviationanddefensemarketreports.com/defense-satcom-systems-the-backbone-of-modern-military-communication/.

15. Best Military Communication Devices (2024-2025). *Oledcomm.* URL: https://www.oledcomm.net/blog/military-communication-devices/ (дата звернення: 11.12.2025).

16. Defense communication system: 5 essential features for modern military operations. *Rocket.Chat.* 17.01.2025. URL: https://www.rocket.chat/blog/defense-communication-system (дата звернення: 11.12.2025).

17. Comparing High-Performance Software-Defined Radios. *COTS Journal. The Journal of Military Electronics & Computing.* 23.03.2023. URL: https://www.cotsjournalonline.com/comparing-high-performance-software-defined-radios/.

18. List of software-defined radios. *Grokipedia*. 08.12.2025. URL: https://grokipedia.com/page/List_of_software-defined_radios.

19. Новітні технології та засоби зв'язку у ЗСУ: шлях трансформації та перспективи розвитку / О. Лаврут та ін. *Ukrainian Military Pages.* 2019. URL: https://www.ukrmilitary.com/2019/04/signal.html#google_vignette.

20. Chaudhari Q. Top 5 Software Defined Radios (SDR) for RF Experimentation. *Wireless Pi*. URL: https://wirelesspi.com/top-5-software-defined-radios-sdr-for-rf-experimentation/ (дата звернення: 13.12.2025).

21. Best military grade phone. *Accio. Business.* 29.11.2025. URL: https://www.accio.com/business/best-military-grade-phone.

22. The Toughest Smartphone in the World: Military-Grade Durability and Extreme Performance. *Vertu. AI & PHONE.* 10.10.2025. URL: https://vertu.com/lifestyle/the-toughest-smartphone-in-the-world-military-grade-durability-and-extreme-performance/?srsltid=AfmBOopShgazqUWMv3__-0TmH-Dbv6ILwXvNujrC-_gB4WhC5doOoFWb.

23. The best rugged phones to buy in 2025 (including Samsung and Oukitel). *Zdnet. Tech.* 28.06.2025. URL: https://www.zdnet.com/article/best-rugged-phone/.

24. Top 5 Military-Grade Phones for Extreme Environments: Your Ultimate 2025 Guide. *Vertu. AI & PHONE*. 04.09.2025. URL: https://vertu.com/guides/top-5-military-grade-phones-for-extreme-environments-your-ultimate-2025-guide/?srsltid=AfmBOoobh2pH2afGidntGDujtnz-y0MbEnqG27ueZA-ZCoHvdTO9uuX9.

25. Безрук В., Буханько О., Чеботарьова Д. Оптимізація та математичне моделювання мереж зв'язку: Навчальний посібник. Харків : Компанія СМІТ, 2014. 194 с.

26. Чеботарьова Д., Безрук В. Автоматизація вибору оптимальних проєктних варіантів систем зв'язку на основі методів багатокритеріальної оптимізації. *Information and communication technologies, electronic engineerin*g. 2021. Vol. 1, № 2. С. 54 – 61.

27. Optimization and mathematical modeling of communication networks : monograph / V. Bezruk та ін. Kharkiv : PC "Technology Center", 2019. 192 с. ISBN 978-617-7319-22-01.

28. Наукоємні технології оптимізації та керування в інфокомунікаційних мережах : монографія / Під загальною редакцією В.М. Безрука, Л.С. Глоби, О.Є Стрижака. – К.: Інститут обдарованої дитини НАПН України, 2019. – 194с.

29. Безрук В., Ємельянов В., Чеботарьова Д. Планування та оптимізація систем стільникового мобільного зв’язку: Навчальний посібник / ред. В. Безрук. Харків : ХНУРЕ, 2024. 337 с.

30. Military communications in hostile environments. *Globalsys. Military communications in hostile environments.* 05.10.2025. URL: https://global-sys.com/news/military-communications-systems/.

31. Стрілка В.Я., Чеботарьова Д.В. Аналіз сучасних інфокомунікаційних засобів для організації військового зв'язку // Тези доповідей тринадцятої міжнародної науково-технічної конференції «Проблеми інформатизації», 27 – 28 листопада 2025 р., Баку – Харків – Бельсько-Бяла. 2025. – Том 1. – С. 102.