

ФУНКЦІЇ, ЗАВДАННЯ ТА ЗОНИ ВІДПОВІДАЛЬНОСТІ ЧАСТИН І ПІДРОЗДІЛІВ ЗВ'ЯЗКУ З УРАХУВАННЯМ ЧОТИРЬОХ ІНФОРМАЦІЙНИХ ДОМЕНІВ ЗБРОЙНИХ СИЛ УКРАЇНИ ТА ОСОБЛИВОСТЕЙ ВІЙСЬКОВО-МОРСЬКИХ СИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

Коновець В. І.

*кандидат технічних наук, старший науковий співробітник,
провідний науковий співробітник
Науково-дослідного центру «Державний океанаріум»
Інституту Військово-Морських Сил
Національного університету «Одеська морська академія»
ORCID: 0000-0002-5354-4234*

Дем'яненко Г. В.

*старший науковий співробітник
Науково-дослідного центру «Державний океанаріум»
Інституту Військово-Морських Сил
Національного університету «Одеська морська академія»
ORCID: 0000-0001-5408-1721*

Лазута Р. Р.

*начальник науково-дослідного відділу
Наукового центру зв'язку та інформатизації
Військового інституту телекомунікацій та інформатизації імені Героїв Крут
ORCID: 0000-0003-3254-9690*

Анотація. Основою управління військами є рішення командира, що розробляється на основі інформації, яка отримується від різних джерел у єдиному інформаційному просторі, зокрема з використанням сумісних систем / мереж зв'язку та інформаційних систем. Своєю чергою поняття «мережа» в сучасних війнах охоплює різні складники, які раніше розглядалися лише окремо та між якими постійно повинен здійснюватися інформаційний обмін, наприклад: бойові одиниці (бойові машини, озброєння, підрозділи тощо), системи зв'язку, інформаційне забезпечення операцій, різноманітні джерела розвідки, логістичні та медичні інформаційні системи тощо. Тобто для ведення сучасних війн та отримання переваги над противником збройні сили повинні використовувати єдиний інформаційний простір, побудований на сумісних мережах / системах зв'язку, які забезпечують захищений обмін інформацією між ними, для підвищення загальної ситуаційної обізнаності та управління військами (силами) [1].

Розвиток інформаційних технологій прямо впливає на систему зв'язку, що своєю чергою є основним елементом системи управління військами. Збільшення пропускної здатності, упровадження спеціалізованого програмного забезпечення, застосування елементів штучного інтелекту значно розширює можливості управлінських процесів та збільшує інструментарій ситуаційної обізнаності, сприяє проведенню розрахунків, моделюванню ситуації та ефективному прогнозуванню розвитку обстановки. Об'єднана, цілісна, стійка й надійна інформаційно-комунікаційна система в сучасному конфлікті безпосередньо дає змогу застосувати модель мережево-центричної війни, орієнтованої на досягнення інформаційної переваги за допомогою об'єднання військових об'єктів в інформаційну мережу.

Ключові слова: домен зв'язку, базові сервіси, функціональні сервіси, ядро сервісу, транспортна мережа, абонентські програми.

Konovets V. I., Demianenko H. V., Lazuta R. R. FUNCTIONS, TASKS AND AREAS OF RESPONSIBILITY OF COMMUNICATION PARTS AND SUBDIVISIONS TAKING INTO ACCOUNT THE FOUR INFORMATION DOMAINS OF THE ARMED FORCES OF UKRAINE AND THE FEATURES OF THE NAVY OF THE ARMED FORCES OF UKRAINE

Abstract. The basis of troop management is the commander's decision, developed on the basis of information received from various sources in a single information space, including using interoperable communication systems / networks and information systems. In turn, the concept of "network" in modern wars covers various components that

were previously considered only separately, and between which information exchange must be carried out constantly, for example: combat units (combat vehicles, weapons, units, etc.), communication systems, information operations support, disparate sources of intelligence, logistics and medical information systems, etc. That is, in order to conduct modern wars and gain an advantage over the enemy, the armed forces must use a single information space built on interoperable networks / communication systems that provide secure exchange of information between them, to increase general situational awareness and control of troops (forces) [1].

The development of information technologies has a direct impact on the communication system, which is, after all, the main element of the military management system. Increasing bandwidth, implementing specialized software, and using elements of artificial intelligence significantly expands the capabilities of management processes and increases the toolkit of situational awareness, calculations, situation modeling, and effective forecasting of the situation. A unified, integral, stable and reliable information and communication system in the modern conflict directly allows the application of the model of network-centric warfare, focused on achieving an information advantage by means of combining military objects into an information network.

Key words: communication domain, basic services, functional services, service core, transport network, subscriber programs.

Мета статті – сформулювати структуру системи зв'язку як елемента системи управління Військово-Морських Сил (далі – ВМС) Збройних Сил України (далі – ЗСУ) через сервіс-орієнтовану архітектуру з урахуванням рекомендацій Агентства з питань обслуговування систем інформації та зв'язку НАТО (NATO Communications and Information Agency).

До уваги читачів будуть представлені:

а) структура інформаційного домену на основі сервіс-орієнтованої архітектури;

б) концепція інформаційного простору ВМС ЗСУ з огляду на СЗ Таханому, FMN та розподіл інформаційних доменів у ЗСУ в сервіс-орієнтованій архітектурі.

В умовах російсько-української війни у процесі функціонування інформаційно-комунікаційної системи Військово-Морських Сил України сформувалися рішення щодо забезпечення її основних характеристик (спроможності, сумісності, гнучкості, масштабованості, стійкості, надмірності, живучості, сервісної орієнтації, автономності, своєчасності, готовності, безпеки), а також чітке формулювання системи через чотири основні домени з розділенням їм за трьома ключовими рівнями функціонування.

Відповідно до стратегічних принципів зв'язку та інформаційних систем планування, забезпечення й експлуатація систем зв'язку та інформаційних систем повинні бути сформульовані з позиції сервісів. Сервіси мають визначати спроможності систем зв'язку та інформаційних систем, які надаються користувачеві, при цьому повинна

виключатися необхідність розуміння технічних аспектів функціонування цих сервісів. СЗ-таксономією (інформація, яку наведено в додатку 1 до Доктрини «Зв'язок та інформаційні системи» [1]) мають бути описані такі категорії сервісів:

1) *сервіси зв'язку*, що мають поєднувати системи й механізми передавання вибірко-вих даних між точками доступу або через них відповідно до узгоджених параметрів якості та без зміни форми чи змісту даних, які надсилаються та отримуються. Сервіси зв'язку поділяються на сервіси доступу до телекомунікацій, транспортні сервіси та сервіси передачі;

2) *базові сервіси*, які повинні забезпечувати універсальне, незалежне від груп користувачів і технічної функціональності сервіс-орієнтоване середовище з використанням інфраструктурних, архітектурних та інших необхідних складових елементів. Базові сервіси, що забезпечують ці складові елементи, є універсальними, загальні спроможності яких не повинні бути реалізовані окремими програмами чи іншими сервісами. Базові сервіси поділяються на інфраструктурні сервіси, платформенні сервіси та сервіси підтримки робочих процесів;

3) *сервіси, орієнтовані на конкретні інтереси (функціональні сервіси)*, які мають забезпечувати функціонал, що потрібний окремим спеціалізованим спільнотам користувачів у підтримці операцій сил оборони, навчань і заходів повсякденної діяльності, наприклад окремим структурним підрозділам органів військового управління (підрозділам розвідки, планування вогневого ураження, логістики тощо);

4) *клієнтські програми*, що повинні виконувати технічні сервіси для забезпечення спроможностей, орієнтованих на користувача. Клієнтські програми мають надавати інтерфейс користувачеві, який об'єднує технічні сервіси в підтримку визначеного військового процесу;

5) *домени зв'язку та інформації* – спосіб розподілу спроможностей систем зв'язку та інформаційних систем відповідно до ступеня обмеження доступу до інформації, яка буде цими системами оброблятися, зберігатися та пересилатися. У мережах сил оборони має дотримуватися підхід «найвищого рівня безпеки в системі». Це означає, що такий домен безпеки (англ. Security Domain) може містити всі типи інформації аж до секретної інформації, де всі користувачі повинні мати допуск до такого рівня секретної інформації, а підхід «потреби в інформації» реалізується не технічно, а адміністративно. Для введення в експлуатацію систем зв'язку та інформаційних систем у цей домен безпеки повинна здійснюватися акредитація з безпеки. Типовими доменами безпеки Військово-Морських Сил ЗСУ є секретний домен, службовий домен, відкритий домен та інтернет-домен. Кожен із названих доменів може підтримуватися багатомережевою конфігурацією. Обмін інформацією між доменами безпеки повинен здійснюватися з використанням шлюзів обміну інформацією, які забезпечують захищене з'єднання двох чи більше доменів безпеки та контрольований обмін інформацією [1, с. 2].

Структура будь-якого інформаційного домену сформульована в доктрині «Зв'язок та інформаційні системи»: це спосіб розподілу спроможностей систем зв'язку та інформаційних систем відповідно до ступеня обмеження доступу до інформації, яка буде цими системами оброблятися, зберігатися та пересилатися. Такий розподіл має полегшувати фокусування на технічних вимогах, проектуванні, упровадженні й функціонуванні складових систем зв'язку та інформаційних систем. Своєю чергою ступінь обмеження визначає правила розгортання та експлуатації, які повинні бути дотримані для забезпечення обмеження доступу до інформації.

Будь-який інформаційний домен повинен мати таку структуру (див. рис. 1):

– транспортна мережа – зв'язки між елементами;

– ядро інформаційного домену – сукупність серверних частин систем базових і функціональних;

– споживачі інформації та сервісів – сукупність абонентів інформаційного домену.

У Військово-Морських Силах Збройних Сил України реалізовані та активно використовуються в повсякденній діяльності й під час воєнного стану такі основні інформаційні домени:

1) секретний домен (Мережа 001), представлений апаратурою засекречення, терміналами засекреченого зв'язку, сервісами обробки користувачами інформації з грифом обмеження доступу «таємно», нормами та правилами користування й функціонування;

2) службовий домен (Мережа 002), представлений апаратурою криптографічного захисту, терміналами спеціального зв'язку, сервісами обробки інформації з грифом «для службового користування», нормами та правилами функціонування;

3) відкритий домен (Мережа «Дніпро»), представлений апаратурою утворення ізольованих каналів, обладнанням кіберзахисту й кібербезпеки, терміналами зв'язку, сервісами обробки інформації, нормами та правилами функціонування;

4) інтернет-домен, представлений апаратурою доступу до мережі Інтернет, обладнанням кіберзахисту та кібербезпеки, терміналами зв'язку, сервісами обробки інформації, нормами та правилами функціонування.

Окремо варто зауважити, що у Військово-Морських Силах Збройних Сил України через специфіку складу сил (військ) для зв'язку з кораблями, катерами, літаками, гелікоптерами та суднами забезпечення здебільшого застосовується радіозв'язок на коротких хвилях (далі – КХ) й ультракоротких хвилях (далі – УКХ), що створює окремі потужні інформаційні домени зі своєю специфічною інфраструктурою. Тому необхідно виділити ще два специфічні домени:

1) радіозв'язок дальньої дії (КХ), представлений апаратурою радіозв'язку КХ для утворення радіомереж і радіоканалів, абонентських терміналів КХ радіозв'язку, інформаційними сервісами, нормами та правилами функціонування;

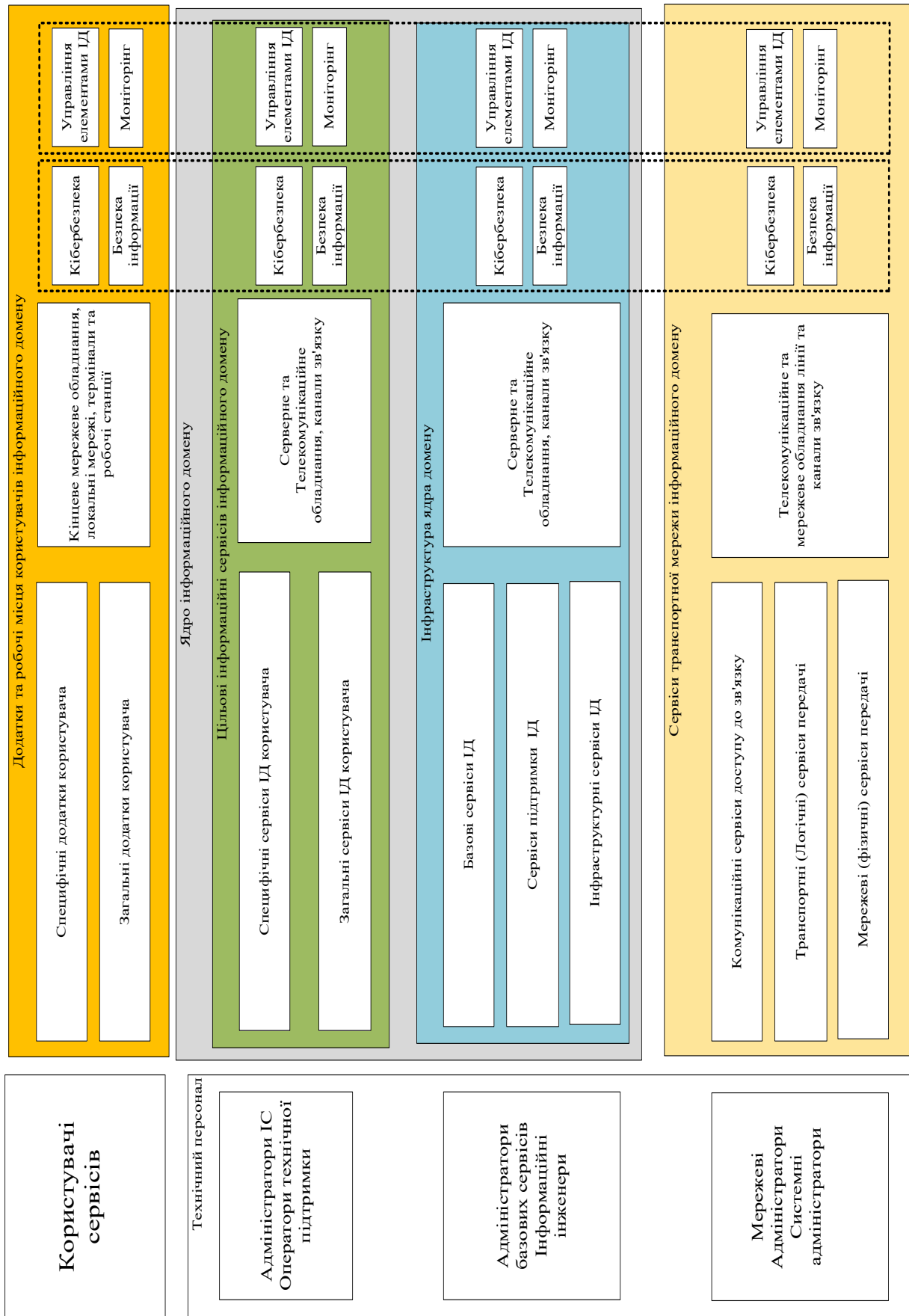


Рис. 1. Структура інформаційного домену на основі COA (C4ISR)

2) радіозв'язок ближньої дії (УКХ), представлений апаратурою радіозв'язку УКХ для утворення радіомереж і радіоканалів, абонентських терміналів УКХ радіозв'язку, інформаційними сервісами, нормами та правилами функціонування.

Фактично інформаційний простір ВМС ЗСУ представлений чотирма основними інформаційними доменами та двома специфічними доменами радіозв'язку.

Таким чином, зоною відповідальності частин і підрозділів зв'язку Військово-Морських Сил України є інформаційний простір, представлений сукупністю інформаційно-комунікаційних систем усіх видів інформаційних доменів Збройних Сил України (транспортних мереж, ядер усіх інформаційних доменів та пунктів управління органів управління, з'єднань, частин та окремих підрозділів ВМС ЗСУ).

Частина (підрозділ) зв'язку виду повинна забезпечувати такі функції:

- функціонування (розгортання, нарощування) інформаційно-комунікаційних сервісів системи управління (з подальшим розвитком до моделі С4 ISR) Військово-Морських Сил України, контроль і моніторинг їх ефективності;
- генерацію та видачу сервісів зв'язку елементам польових мереж зв'язку, літакам та кораблям, у разі необхідності – іншим складовим елементам сил оборони через їх відповідні точки присутності;
- забезпечення захисту інформації та кіберзахисту інформаційно-комунікаційних сервісів системи зв'язку Військово-Морських Сил України, що ним розгортаються та обслуговуються;
- забезпечення технічної, інформаційної підтримки та надання сервісів зв'язку й інформаційних систем загального та спеціального призначення посадовим особам органів управління, з'єднань частин та окремих підрозділів ВМС ЗСУ.

Через збройну агресію російської федерації, а також з огляду на вимоги Закону України «Про електронні комунікації» від 16 грудня 2020 р. № 1089-ІХ, положення доктрини «Зв'язок та інформаційні системи» (ВКП 6-00(01).01) від 1 липня 2021 р. [1] та напрям розвитку Військ зв'язку й кібербезпеки Збройних Сил України [11], враховуючи впрова-

дження Концепції розвитку ІТ-інфраструктури Міністерства оборони України та Збройних Сил України від 3 листопада 2021 р. [10] та Концепції побудови електронної комунікаційної мережі Збройних Сил України (ВКП 6-26(01).01) від 6 вересня 2021 р. [12], сформувалася концепція інформаційного простору ВМС ЗСУ з огляду на С3 Таханому, FMN та розподіл інформаційних доменів у ЗСУ в сервіс-орієнтованій архітектурі, що описує середовище (див. рис. 2).

У процесі розгляду структури інформаційного простору ВМС ЗСУ (рис. 2) можна зробити висновок, що для формування колективу персоналу для його обслуговування є два шляхи:

- а) лінійний – поділ за доменами;
- б) функціональний – поділ за функціями та специфікою кожного рівня.

У разі застосування лінійного принципу формування підрозділів є низка недоліків, зокрема й дублювання функцій технічного персоналу в кожному інформаційному домені. Наприклад, мережеві адміністратори інтернет-домену, відкритого, спеціального та секретного доменів – це однаково навчені спеціалісти з невеликими відмінностями щодо специфіки обладнання. З огляду на те, що транспортні мережі пов'язані одна з одною та є первинними в одних випадках і вторинними в інших, функції мережевих адміністраторів однакові: налаштування комунікаційного обладнання для утворення мереж і каналів, їх маршрутизація та контроль за станом зв'язку.

Для більш раціонального застосування ІТ-спеціалістів необхідно враховувати їх специфіку та групувати в невеликі групи для вирішення однотипних завдань (функціональний підхід), а ці групи варто підпорядковувати одному керівнику, який буде відповідати за напрям (за схожим функціоналом у різних інформаційних доменах). Такими напрямками є:

- 1) комунікаційний – побудова транспортних магістральних мереж, керування та моніторинг стану зв'язку, маршрутизація та надання доступу до певних елементів інформаційних доменів. Основним завданням цього напрямку є створення й підтримка транспортного середовища ВМС ЗСУ та надання доступу групам користувачів (пунктам управлінь, окремим підрозділам тощо);

Відкрита складова загального інформаційного простору ВМС ЗС України				Закрита складова інформаційного простору ВМС ЗС України		Середовище радіозв'язку ВМС ЗС України	
Інтернет-домен (Публічний домен)	Відкритий домен (Внутрішня мережа – Дипро)	Службовий домен (Мережа ЗСУ 002)	Секретний домен (Мережа ЗСУ 001)	Радіозв'язок Близької Дії (УКХ)	Радіозв'язок Дальньої Дії (КХ)		
Абонентські пристрої	Абонентські пристрої	Абонентські пристрої	Абонентські пристрої	Радіо винос (за необхідності)	Радіо винос (за необхідності)		
Внутрішня мережа ПУ	Внутрішня мережа ПУ	Внутрішня мережа ПУ	Внутрішня мережа ПУ	Абонентські радіопристрої	Вхідне абонентське з'єднання та криптозахист		
Вхідне абонентське з'єднання	Вхідне абонентське з'єднання	Вхідне абонентське з'єднання та криптозахист	Вхідне абонентське з'єднання та криптозахист		Абонентські радіопристрої		
Загальні та спеціальні сервіси	Загальні та спеціальні сервіси	Загальні та спеціальні сервіси	Загальні та спеціальні сервіси		Загальні та спеціальні сервіси		
Базові сервіси	Базові сервіси	Базові сервіси	Базові сервіси		Базові сервіси		
Інфраструктурні сервіси	Інфраструктурні сервіси	Інфраструктурні сервіси	Інфраструктурні сервіси		Інфраструктурні сервіси		
Авторизація і доступ	Авторизація і доступ	Авторизація і доступ	Авторизація і доступ		Авторизація і доступ		
Логічні з'єднання	Логічні з'єднання	Криптозахист та логічні з'єднання	Криптозахист та логічні з'єднання		Логічні з'єднання радіоканалів та радіомереж	Логічні з'єднання	Криптозахист та логічні з'єднання
Зовнішня магістральна мережа	Зовнішня магістральна мережа (Відокремлена)				Радіомережі УКХ-діапазону		

Абонентські сервіси
(пункти управління
ВМС ЗС України)

Технічні та базові
сервіси
(Сервіси ядра систем,
ЦОД, технологічні
майданчики, віртуальне
середовище)

Сервіси зв'язку
(Транспортні сервіси
магістральної мережі
ВМС ЗС України)

Рис. 2. Концепція інформаційного простору ВМС ЗСУ з огляду на С3 Таханоту, FMN та розподіл інформаційних доменів у ЗСУ в сервіс-орієнтованій архітектурі функціонування частин і підрозділів зв'язку, яка повинна забезпечити безперерйне та надійне існування інформаційно-комунікаційної системи Військово-Морських Сил України

2) інфраструктурний – побудова, підтримка та супроводження апаратно-програмних середовищ для розміщення цільових функціональних сервісів загального й спеціального призначення, налаштування та супроводження інфраструктурних сервісів рівня ядра;

3) інформаційний – забезпечення функціонування інформаційних сервісів загального та спеціального призначення, їх налаштування, підтримка та супроводження. Сервіси орієнтовані на користувачів і мають певний рівень захисту від кібервпливу ззовні;

4) абонентський – забезпечення функціонування внутрішніх абонентських мереж, налаштування клієнтського обладнання та програмного забезпечення, надання інформаційно-технічної підтримки під час експлуатації сервісів операторами та користувачами.

З огляду на принципи однорідності процесів, які функціонують у середовищі інформаційно-комунікаційної системи ВМС ЗСУ, можна виділити такі зони відповідальності її складників (див. рис. 3):

- інформаційно-технічна підтримка пунктів управління (для кожного пункту управління повний склад підтримки сервісів);

- складник управління й забезпечення функціонування інформаційних систем, базових і функціональних сервісів, програмний складник ядра інформаційно-комунікаційної системи ВМС ЗСУ;

- комунікаційний складник, що включає в себе інфраструктурні сервіси центрів обробки даних, фактично апаратно-програмний комплекс ядра інформаційно-комунікаційної системи ВМС ЗСУ;

- інформаційно-комунікаційний радіо-складник, що фактично поєднує специфічні сервіси радіозв'язку та канало-мережеутворювальну апаратуру.

Окремо необхідно виділити систему моніторингу стану системи загалом та систему кібербезпеки й кіберзахисту, яка включає в себе сенсори на всіх рівнях системи (бази даних, бази знань та аналітичні інструменти) для виявлення, реагування й упередження кіберінцидентів в інформаційно-комунікаційній системі ВМС ЗСУ.

Таким чином, концепція ведення мережецентричної війни передбачає збільшення бойової

потужності угруповання об'єднаних сил шляхом утворення інформаційно-комутаційної мережі, яка поєднує джерела інформації (розвідки), органи управління та засоби ураження (придушення), що забезпечує доведення до учасників операцій достовірної та повної інформації про обстановку практично в реальному часі. Завдяки цьому досягається прискорення процесу управління силами та засобами, підвищення темпу операцій, збільшення ефективності ураження сил супротивника, живучості своїх військ та рівня самосинхронізації бойових дій.

Основною особливістю мережецентричної війни є переведення інформаційних переваг, властивих окремим інформаційним технологіям, у конкурентну перевагу шляхом об'єднання в робастну (стійку) мережу інформаційно добре забезпечених та географічно розосереджених сил. Ця мережа, поєднана з відмінними технологіями, організацією процесів і людей, може сприяти новим формам організаційної поведінки.

Перспективним напрямом є концепція інтеграції інформаційної та сенсорної підсистем мережецентричного ведення бойових дій у єдину інформаційно-сенсорну підсистему з перетворенням інформаційної компоненти на інформаційно-сенсорну решітку.

Тому перспективою подальшого розвитку в цьому напрямі є реалізація принципів ведення мережецентричної війни через нарощування та трансформацію інформаційно-комунікаційної системи, а саме:

- об'єднання сил (військ) надійними мережами для покращеного обміну інформацією та досягнення інформаційної переваги над ворогом;

- збільшення корисного і якісного обміну інформацією для загальної ситуаційної поінформованості та обізнаності;

- зменшення часу на отримання інформації, її аналіз та обробку, формулювання на її основі ефективного рішення та доведення до виконавців у зрозумілому вигляді;

- нарощування якісної загальної ситуаційної обізнаності для забезпечення співробітництва й самосинхронізації, підвищення стійкості та швидкості команд і розпоряджень із метою різкого підвищення ефективності управління.

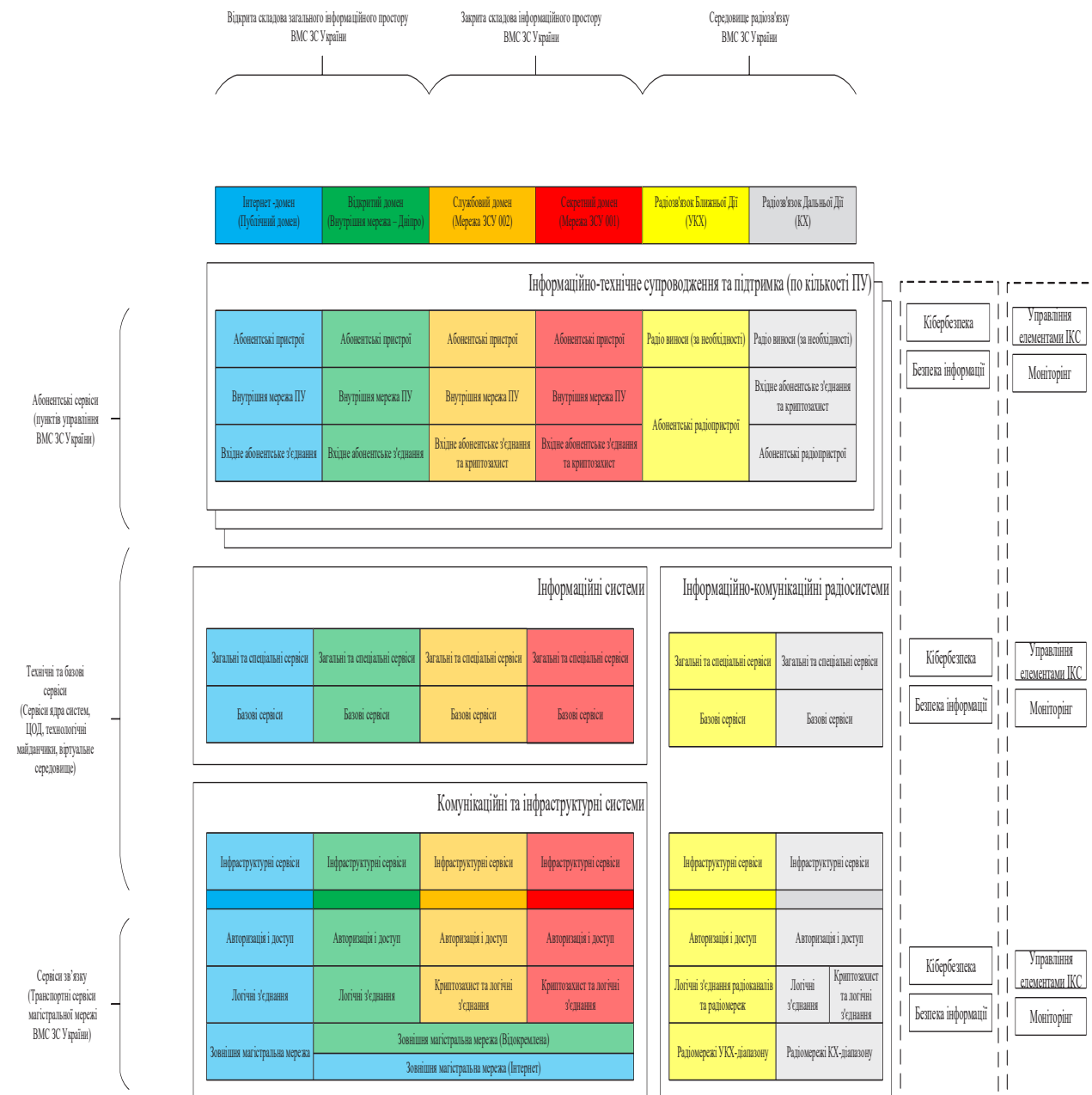


Рис. 3. Зони відповідальності складових частини зв'язку

Література:

1. Доктрина «Зв'язок та інформаційні системи» (ВКП 6-00(01).01), затверджена Головнокомандувачем Збройних Сил України 1 липня 2020 р. № 15841/С. Київ : ГУДП ГШ ЗСУ, 2020. 76 с.
2. Жак А.М. Вимоги та рекомендації щодо вибору та будівельної підготовки території та приміщень для центру обробки даних (ЦОД) : практичний посібник. Датадом, 2010. 90 с.
3. Rubens P. Technical support for the neighbours. *BBC News*. 2005. March 28. URL: http://news.bbc.co.uk/2/hi/uk_news/magazine/4387525.stm.
4. Walker G. IT Problem Management. Upper Saddle River : Prentice Hall, 2001. 167 p.
5. Guru Staff. What Are the Types of Technical Support? *Guru.com*. 2022. March 23. URL: <https://www.guru.com/blog/what-are-the-types-of-technical-support/>.
6. Windley Ph.J. Delivering High Availability Services Using a Multi-Tiered Support Model. URL: <https://www.windley.com/docs/Tiered%20Support.pdf>.

7. Kajko-Mattsson M. Problems within front-end support. *Journal of Software Maintenance and Evolution: Research and Practice*. 2004. Vol. 16. Iss. 4–5. P. 309–329. DOI: <https://doi.org/10.1002/smr.298>.
8. Leung N.K.Y., Lau Sim Kim. Information Technology Help Desk Survey: To Identify the Classification of Simple and Routine Enquiries. *Journal of Computer Information Systems*. 2007. Vol. 47. Iss. 4. P. 70–81.
9. Телекомунікаційні системи та мережі : мультимедійний підручник : у 2 т. / В.В. Поповський, О.В. Лемешко, В.К. Ковальчук, М.Д. Плотніков, Ю.П. Картушин, О.М. Попонін, Д.В. Агєєв, С.О. Сабурова, В.Ф. Олійник, А.В. Персіков, В.А. Лошаков, К.О. Селіванов. Харків : ТОВ «Компанія СМІТ», 2018. Т. 1 : Структура й основні функції.
10. Концепція розвитку IT-інфраструктури Міністерства оборони та Збройних Сил України, затверджена Міністром оборони України 3 листопада 2021 р.
11. Доктрина Військ зв'язку та кібербезпеки Збройних Сил України (БКП 6-00(01).01), затверджена Головнокомандувачем Збройних Сил України 9 лютого 2021 р. Київ, 2021. 51 с. URL: https://shron1.chtyvo.org.ua/Ministerstvo_oborony_Ukrainy/Doktryna_Viisk_zviazku_ta_kiberbezpeky_Zbroinykh_Syl_Ukrainy.pdf?
12. Концепція побудови електронної комунікаційної мережі Збройних Сил України (БКП 6-26(01).01), затверджена Головнокомандувачем Збройних Сил України 6 вересня 2021 р.
13. Науково-дослідна робота «Обґрунтування обрисів автоматизованої системи управління Військово-Морськими Силами Збройних Сил України», реєстраційний номер ЦВНІ ЦНДІ ЗС України № 0321ZS1180.

References:

1. Commander-in-Chief of the Armed Forces of Ukraine (2020). *Doktryna "Zviazok ta informatsiini systemy" (BKП 6-00(01).01), zatverdzhena Holovnokomanduvachem Zbroinykh Syl Ukrainy 1 lypnia 2020 r. № 15841/C [The doctrine "Communication and information systems" (BKП 6-00(01).01), approved by the Commander-in-Chief of the Armed Forces of Ukraine on July 1, 2020 № 15841/C]*. Kyiv: HUDP HSh ZSU, 76 p. [in Ukrainian].
2. Zhak, A.M. (2010). *Vymohy ta rekomendatsii shchodo vyboru ta budivelnoi pidhotovky terytorii ta prymyshchen dlia tsentru obrobky danykh (TsOD): praktychnyi posibnyk [Requirements and recommendations for the selection and construction preparation of the territory and premises for the data processing center (DPC): practical guide]*. Datadom, 90 p. [in Ukrainian].
3. Rubens, P. (2005). Technical support for the neighbours. *BBC News*, March 28. Retrieved from: http://news.bbc.co.uk/2/hi/uk_news/magazine/4387525.stm [in English].
4. Walker, G. (2001). *IT Problem Management*. Upper Saddle River: Prentice Hall, 167 p. [in English].
5. Guru Staff (2022). What Are the Types of Technical Support? *Guru.com*, March 23. Retrieved from: <https://www.guru.com/blog/what-are-the-types-of-technical-support/> [in English].
6. Windley, Ph.J. (2002). Delivering High Availability Services Using a Multi-Tiered Support Model. Retrieved from: <https://www.windley.com/docs/Tiered%20Support.pdf> [in English].
7. Kajko-Mattsson, M. (2004). Problems within front-end support. *Journal of Software Maintenance and Evolution: Research and Practice*, vol. 16, iss. 4–5, pp. 309–329. DOI: <https://doi.org/10.1002/smr.298> [in English].
8. Leung, N.K.Y., Lau, Sim Kim (2007). Information Technology Help Desk Survey: To Identify the Classification of Simple and Routine Enquiries. *Journal of Computer Information Systems*, vol. 47, iss. 4, pp. 70–81 [in English].
9. Popovskiy, V.V. Lemeshko, O.V., Kovalchuk, V.K., Plotnikov, M.D., Kartushyn, Yu.P., Poponin, O.M., Ahiev, D.V., Saburova, S.O., Oliinyk, V.F., Persykov, A.V., Loshakov, V.A., Selivanov, K.O. (2018). *Telekomunikatsiini systemy ta merezhi: multymediini pidruchnyk [Telecommunication systems and networks: multimedia textbook]*, in 2 vols., vol. 1: *Struktura y osnovni funktsii [Structure and main functions]*. Kharkiv: TOV "Kompaniia SMIT" [in Ukrainian].
10. Minister of Defense of Ukraine (2021). *Kontseptsiiia rozvytku IT-infrastruktury Ministerstva oborony ta Zbroinykh Syl Ukrainy, zatverdzhena Ministrom oborony Ukrainy 3 lystopada 2021 r. [The concept of IT infrastructure development of the Ministry of Defense and the Armed Forces of Ukraine, approved by the Minister of Defense of Ukraine on November 3, 2021]* [in Ukrainian].
11. Commander-in-Chief of the Armed Forces of Ukraine (2021a). *Doktryna Viisk zviazku ta kiberbezpeky Zbroinykh Syl Ukrainy (BKП 6-00(01).01), zatverdzhena Holovnokomanduvachem Zbroinykh Syl Ukrainy 9 liutoho 2021 r. [Doctrine of Communications and Cyber Security of the Armed Forces of Ukraine (BKП 6-00(01).01), approved by the Commander-in-Chief of the Armed Forces of Ukraine on February 9, 2021]*. Kyiv, 51 p. Retrieved from: https://shron1.chtyvo.org.ua/Ministerstvo_oborony_Ukrainy/Doktryna_Viisk_zviazku_ta_kiberbezpeky_Zbroinykh_Syl_Ukrainy.pdf? [in Ukrainian].
12. Commander-in-Chief of the Armed Forces of Ukraine (2021b). *Kontseptsiiia pobudovy elektronnoi komunikatsiinoi merezhi Zbroinykh Syl Ukrainy (BKП 6-26(01).01), zatverdzhena Holovnokomanduvachem Zbroinykh Syl Ukrainy*

6 veresnia 2021 r. [The concept of building an electronic communication network of the Armed Forces of Ukraine (BKП 6-26(01).01), approved by the Commander-in-Chief of the Armed Forces of Ukraine on September 6, 2021] [in Ukrainian].

13. Naukovo-doslidna robota “Obgruntuvannia obrysu avtomatyzovanoi systemy upravlinnia Viiskovo-Morskymy Sylamy Zbroinykh Syl Ukrainy”, reiestratsiinyi nomer TsVNI TsNDI ZS Ukrainy № 0321ZS1180 [Scientific research work “Justification of the outline of the automated management system of the Naval Forces of the Armed Forces of Ukraine”, registration number of the Center for the Central Research Institute of the Armed Forces of Ukraine № 0321ZS1180] [in Ukrainian].