УДК 621.396:004.7

Є. В. Прокопенко, Д. А. Мул

ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СУМІСНОСТІ СУБ'ЄКТІВ СИЛ ОБОРОНИ УКРАЇНИ В УМОВАХ ЗАСТОСУВАННЯ ГЕТЕРОГЕННИХ СИСТЕМ ЗВ'ЯЗКУ

Анотація. *У тезах обґрунтовано підхід до забезпечення інформаційно-комунікаційної сумісності суб'єктів Сил оборони України в умовах одночасного застосування різнорідних військових і цивільних систем зв'язку. Запропоновано розглядати взаємодію не як створення єдиної інформаційно-комунікаційної системи, а як об'єднання автономних комунікаційних сегментів, поєднаних міжнародно стандартизованими інтерфейсами, інтеграційними шлюзами, узгодженими форматами обміну даними та спільними правилами безпеки. Визначено технічний, інформаційний, організаційний і безпековий рівні сумісності та запропоновано послідовність їх оцінювання під час планування міжвідомчої взаємодії.*

Ключові слова: *гетерогенна система зв'язку; інформаційна сумісність; Сили оборони України; комунікаційна мережа; взаємодія.*

Annotation. *The paper substantiates an approach to ensuring information and communication interoperability among the entities of the Defence Forces of Ukraine under conditions of the simultaneous use of heterogeneous military and civilian communication systems. It is proposed to consider interoperability not as the creation of a single information and communication system, but as the integration of autonomous communication segments connected through internationally standardized interfaces, integration gateways, harmonized data exchange formats, and common security rules. The technical, information, organizational, and security levels of interoperability are identified, and a sequence for their assessment during the planning of interagency interaction is proposed.*

Keywords: *heterogeneous communication system; information interoperability; Defence Forces of Ukraine; communication network; interoperability.*

Повномасштабна війна росії проти України істотно прискорила розвиток засобів управління, зв'язку, ситуаційної обізнаності та оброблення даних у Силах оборони України. Водночас розвиток відбувався нерівномірно: різні складові Сил оборони використовують власні системи зв'язку, інформаційно-комунікаційні системи, програмно-апаратні комплекси, радіомережі, супутникові та наземні канали передачі даних, а також ресурси цивільних операторів зв'язку. З одного боку, така технологічна різнорідність підвищує загальну живучість, однак, з іншого, ускладнює взаємодію під час спільного виконання завдань, коли інформаційні повідомлення мають своєчасно передаватися між органами управління, бойовими порядками, розвідувальними засобами та вогневими платформами.

Проблема полягає не стільки у відсутності окремих каналів зв'язку, скільки у різних підходах до побудови мереж, адресації, ідентифікації користувачів, форматів даних, правил маршрутизації, кіберзахисту та пріоритетності інформаційних потоків. Тому формування задачі у фізичному об'єднанні всіх наявних мереж в одну інтегровану інформаційно-комунікаційну мережу є недоцільною. Більш перспективним є підхід, за якого кожний суб'єкт зберігає керування власними мережами та сервісами, але забезпечує взаємодію через попередньо погоджені профілі сумісності. Такий принцип відповідає концепції NATO Federated Mission Networking, де федерація розглядається як поєднання автономних учасників на основі узгоджених процедур, стандартів, інформаційних сервісів і технічних профілів [1].

Практичну доцільність такого підходу підтверджує український досвід. Під час навчань NATO CWIX 2024 бойова система DELTA успішно інтегрувалася з польською системою управління артилерійським вогнем TOPAZ, забезпечивши обмін даними та підтвердивши сумісність за кількома стандартами взаємосумісності [2]. У 2025 році DELTA була впроваджена на всіх рівнях Сил оборони України, що додатково підкреслює значення спільного цифрового простору для обміну інформацією між різними рівнями та складовими системи управління [3]. Організація Північноатлантичного договору, своєю чергою, визначає федеративну

взаємосумісність і захищеність цифрових платформи одним із базових напрямів цифрової трансформації Альянсу [4].

З урахуванням цього пропонується формувати міжвідомчу взаємодію на чотирьох взаємопов'язаних рівнях. Технічний рівень, має забезпечувати фізичну та протокольну можливість передавання даних між мережами з використанням шлюзів, маршрутизаторів, сервісних шин та інших інтеграційних засобів. Інформаційний рівень, передбачає узгодження структури, семантики, форматів і правил актуалізації даних. Організаційний рівень, визначає повноваження, процедури, відповідальність і порядок доступу до інформаційних ресурсів. Безпековий рівень, установлює єдині мінімально необхідні вимоги до автентифікації, розмежування доступу, криптографічного захисту, системне журналювання та реагування на інциденти.

У практичному плануванні взаємодії пропонується така послідовність. На першому етапі визначаються потреби та перелік сервісів, які необхідно надати суб'єктам інформаційного обміну: ситуаційна обізнаність, обмін координатами, повідомленнями, відео, телеметрією, цілевказанням, логістичною та іншою службовою інформацією. На другому етапі проводиться інвентаризація доступних військових і цивільних транспортних ресурсів: тактичного радіозв'язку, радіорелейних і відомчих IP-мереж, супутникових каналів, приватних LTE/5G та публічних мобільних мереж. На третьому етапі для кожної пари систем визначається спосіб інтеграції: прямий стандартизований обмін, взаємодія через шлюз або надання окремого сервісу через федеративну мережу.

На четвертому етапі формується профіль взаємодії, у якому фіксуються інтерфейси, формати даних, правила ідентифікації, пріоритети трафіку, політики безпеки та вимоги до якості обслуговування. Доцільно максимально використовувати відкриті та узгоджені стандарти, а не прив'язувати взаємодію до одного виробника або конкретного типу апаратури. Такий підхід відповідає NATO Interoperability Standards and Profiles, які формують набір стандартів і профілів для забезпечення сумісності сервісів і комунікацій у федеративних мережах [5].

П'ятий етап передбачає випробування взаємодії до бойового застосування. За аналогією з підходом NATO CWIX, де перевіряється здатність командно-штабних та інформаційних систем обмінюватися оперативними даними, доцільно створювати національні міжвідомчі платформи перевірки взаємосумісності [6]. Основним результатом таких випробувань має бути не лише факт встановлення з'єднання, а підтвердження коректного обміну даними, збереження їх семантики, виконання часових вимог, стійкості до відмов і дотримання політик безпеки.

В умовах війни окремого значення набуває транспортна незалежність інформаційних сервісів. Один і той самий сервіс ситуаційної обізнаності або обміну службовими повідомленнями повинен, за можливості, використовувати різні транспортні середовища без зміни логіки роботи користувача. Це передбачає відокремлення прикладного рівня від конкретного виду зв'язку та наявність механізмів вибору доступного маршруту з урахуванням пріоритету інформації, стану мережі та вимог безпеки. У такому випадку втрата одного транспортного сегмента не обов'язково означає втрату самого інформаційного сервісу.

Водночас федеративна модель не передбачає безконтрольного взаємного доступу між мережами. Інтеграційний шлюз має виконувати функції не лише протокольного перетворення, а й політики довіри: автентифікацію учасників, перевірку інформації з обмеженим доступом, фільтрацію інформаційних потоків, системне журналювання подій та, за потреби, перетворення рівнів представлення даних. Це дає змогу підключати нові комплекси поступово, не змінюючи внутрішню архітектуру всіх інших систем. Особливо важливо, щоб правила доступу і формат обміну були визначені до початку спільного застосування, а не формувалися ситуативно вже під час виконання бойового завдання.

Для Сил оборони України доцільно передбачити декілька типових профілів взаємодії. Перший профіль, обмін даними ситуаційної обізнаності між різними системами управління. Другий профіль, передавання цілевказання та результатів розвідки до систем планування і вогневого ураження за чітко визначеними форматами та правилами підтвердження даних. Третій профіль, забезпечення службового зв'язку й обміну повідомленнями через різні військові та цивільні транспортні мережі. Четвертий профіль, підключення сенсорів різних типів, безпілотних і роботизованих платформ до спільного інформаційного контуру. \

Запропонований підхід дає змогу перейти від інтеграції окремих пар систем до керованого процесу нарощування взаємосумісності. Якщо новий комплекс підтримує затверджений профіль, його підключення зводиться до перевірки відповідності інтерфейсів, даних, процедур та політик безпеки. У перспективі доцільним є створення каталогу національних профілів міжвідомчої взаємодії та постійного випробувального середовища, у якому нові зразки озброєння, військової техніки, програмно-апаратні комплекси та інформаційні системи перевірятимуться на сумісність ще до масового постачання до складових Сил оборони України.

Таким чином, перспективним напрямом розвитку систем зв'язку Сил оборони України є не уніфікація всіх засобів до одного технічного рішення, а створення керованої федерації гетерогенних мереж і сервісів. Кожний суб'єкт зберігає власні спроможності та автономність, а взаємодія забезпечується стандартними профілями, інтеграційними шлюзами, узгодженими моделями даних і єдиними мінімальними вимогами до безпеки. Це дозволяє зменшити залежність від окремого виробника або виду зв'язку, прискорити включення нових систем і комплексів у спільний контур управління та підвищити ефективність бойового застосування різнорідних сил і засобів.

Список використаних джерел:

1. Federated Mission Networking / NATO Allied Command Transformation. URL: https://www.act.nato.int/activities/federated-mission-networking/ (дата звернення: 14.10.2026).
2. Українська бойова система DELTA успішно інтегрувалася з польською системою управління артилерійським вогнем TOPAZ / Міністерство оборони України. 01.07.2024. URL: https://mod.gov.ua/news/ukrainska-bojova-sistema-delta (дата звернення: 14.10.2026).
3. Бойова система DELTA впроваджена на всіх рівнях Сил оборони України / Міністерство оборони України. 06.08.2025. URL: https://mod.gov.ua/news/bojova-sistema-delta-vprovadzhena-na-vsih-rivnyah-sil-oboroni-ukrayini (дата звернення: 14.10.2026).
4. Alliance Digital Strategy / NATO. 13.01.2026. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/01/13/alliance-digital-strategy (дата звернення: 14.10.2026).
5. NATO Interoperability Standards and Profiles (NISP) : ADatP-34. NATO Interoperability Profiles Capability Team. URL: https://nhqc3s.hq.nato.int/apps/nisp/NISP_index.htm (дата звернення: 14.10.2026).
6. Federated Interoperability / NATO Allied Command Transformation. URL: https://www.act.nato.int/activities/federated-interoperability/ (дата звернення: 14.10.2026).

Прокопенко Євгеній Володимирович *– кандидат технічних наук, доцент, начальник кафедри зв'язку та інформаційних систем Національної академії Державної прикордонної служби України імені Б. Хмельницького (в/ч 9960), м. Хмельницький, e-mail: mydocent@gmail.com, ORCID https://orcid.org/0000-0002-6825-2357.*

Мул Дмитро Анатолійович *– кандидат технічних наук, доцент, доцент кафедри зв'язку та інформаційних систем Національної академії Державної прикордонної служби України імені Б. Хмельницького (в/ч 9960), м. Хмельницький, e-mail: dmitry.mul@gmail.com, ORCID https://orcid.org/0000-0003-2662-4770.*

Yevhenii Volodymyrovych Prokopenko *– Candidate of Technical Sciences (Ph.D.), Associate Professor, Head of the Department of Communications and Information Systems, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine (Military Unit 9960), Khmelnytskyi, Ukraine, e-mail: mydocent@gmail.com, ORCID: https://orcid.org/0000-0002-6825-2357.*

Dmytro Anatoliiovych Mul *– Candidate of Technical Sciences (Ph.D.), Associate Professor, Associate Professor of the Department of Communications and Information Systems, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine (Military Unit 9960), Khmelnytskyi, Ukraine, e-mail: dmitry.mul@gmail.com, ORCID: https://orcid.org/0000-0003-2662-4770.*