УДК 621.396:355.4:004.056

В. А. Ушаков

ІНТЕГРАЦІЯ 5G-МЕРЕЖ У СИСТЕМИ ВІЙСЬКОВОГО ЗВ'ЯЗКУ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

У статті розглянуто технічні можливості 5G, що є критичними для військового застосування, зокрема високу пропускну здатність, наднизьку затримку, підвищену надійність, підтримку масового підключення пристроїв та механізми мережевої сегментації (network slicing). Показано потенціал 5G для побудови розподілених сенсорних мереж, підтримки роїв безпілотних та автономних бойових платформ, інтеграції систем штучного інтелекту в контури управління військами й зброєю, а також автоматизації логістичних процесів. Узагальнено міжнародний досвід НАТО, США, держав ЄС і Китаю щодо впровадження корпоративних 5G-мереж оборонного призначення та їх інтеграції з наявними системами зв'язку. Обґрунтовано, що масове використання віртуалізованих компонентів, відкритих інтерфейсів та багатовендорних рішень у 5G призводить до суттєвого зростання площі атаки й формує новий спектр кіберзагроз, проблем сумісності з іншими системами зв'язку та ризиків технологічної залежності від іноземних постачальників. Сформульовано основні підходи до поетапної інтеграції 5G у системи військового зв'язку сил оборони України, включно з вимогами до архітектури корпоративних мереж, організації кіберзахисту та управління постачальницькими ризиками.

Ключові слова: *5G, військовий зв'язок, тактичні мережі, кібербезпека, автономні бойові платформи, C4ISR-системи, Internet of Military Things (IoMT), корпоративні 5G-мережі, штучний інтелект.*

Постановка проблеми. Досвід широкомасштабної збройної агресії проти України засвідчив різке зростання вимог до систем військового зв'язку: необхідність одночасної підтримки великої кількості розподілених пунктів управління, засобів розвідки й ураження, безпілотних та автономних платформ, а також автоматизованих систем управління в реальному часі. Наявна інфраструктура зв'язку сил оборони сформована переважно на базі технологій попередніх поколінь і розрахована на значно менші обсяги трафіку, інші профілі затримок та більш низький рівень кіберзагроз. Це призводить до перевантаження каналів, нестабільності роботи сервісів управління військами та обмежує можливість повноцінної реалізації мережево-центричних підходів до планування й ведення операцій.

У той же час у низці держав НАТО, США, країн ЄС та Китаї вже сформовано довгострокові стратегії використання технологій мобільного зв'язку п'ятого покоління для потреб оборони, розгортаються експериментальні корпоративні 5G-мережі на полігонах і військових базах, відпрацьовуються сценарії їх застосування у тактичних мережах, логістиці та системах розвідки [2, 3, 6, 8, 9, 14, 15]. Водночас результати цих програм безпосередньо не можуть бути перенесені в українські реалії через відмінності в структурі сил оборони, стані наявної інфраструктури, обмеження в ресурсах та специфічний характер загроз з боку противника. Додатково ситуацію ускладнює високий рівень невизначеності щодо кібербезпеки 5G-мереж, сумісності з існуючими засобами зв'язку та ризиків технологічної залежності від іноземних постачальників.

Таким чином, актуальність цієї теми зумовлена:

– сформованою науково-практичною проблемою обґрунтування підходів до інтеграції технологій 5G у систему військового зв'язку та управління сил оборони України;

– необхідністю визначення вимог до архітектури таких рішень, оцінки їх впливу на стійкість і кіберзахищеність мереж, встановлення обмежень, пов'язаних із взаємодією з наявними системами, а також розробки засад поетапного впровадження 5G-технологій в умовах бойових дій, що тривають, і жорстких ресурсних обмежень.

Аналіз останніх досліджень і публікацій. У міжнародній практиці питання застосування технологій 5G у військовій сфері розглядається передусім у стратегічних та доктринальних документах. Стратегії Міністерства оборони США визначають 5G як ключовий елемент модернізації інфраструктури зв'язку, зосереджуючись на корпоративних мережах для військових баз, полігонів та експериментальних зон, а також на підтримці нових сервісів C4ISR і логістики [2, 3]. Документи НАТО STO формують бачення ролі 5G у майбутніх операціях, описують потенціал мережевого сегментування, підтримки тактичних підрозділів та інтеграції з наявними системами зв'язку, проте здебільшого обмежуються рамковими архітектурними підходами й окремими демонстраційними проєктами [9]. При цьому специфіка бойових дій високої інтенсивності, характерна для України, у цих документах практично не деталізується.

Значний внесок у формування науково-аналітичної бази роблять дослідження, присвячені сценаріям військового застосування 5G. У роботах НАТО C2COE (Центр передового досвіду НАТО з командування та управління), європейських авторів та аналітичних центрів розглянуто можливості 5G для тактичних мереж, взаємодії платформ, морських і наземних застосувань, наголошено на важливості корпоративних мереж та інтеграції з системами управління [7, 10, 15]. Окремі публікації демонструють перспективи використання 5G для підтримки операцій сухопутних військ та формування *цифрового поля бою*, однак здебільшого оперують сценаріями з обмеженим застосуванням засобів РЕБ та кібернападів [6]. Аналітичні огляди щодо Китаю показують, що ця держава розглядає 5G як платформу для побудови інтегрованих військово-цивільних мереж, підтримки автономних систем та інформаційного протистояння [14], але питання протидії таким рішенням, а також можливості асиметричної відповіді з боку інших держав залишаються мало опрацьованими.

Проблематика кібербезпеки 5G та її застосування в IoT/IoMT відображена в низці міжнародних рекомендацій і систематичних оглядів. Документи ЄС та ENISA (Агентство Європейського Союзу з питань мережевої та інформаційної безпеки) пропонують *набір інструментів* для управління ризиками, пов'язаними з постачальниками, віртуалізацією, відкритими інтерфейсами та ланцюгами поставок [4, 5], тоді як ITU (Міжнародний союз електрозв'язку) та NIST NCCoE (Національний центр кібербезпеки Національного інституту стандартів і технологій США) фокусуються на загальних моделях загроз і технічних заходах захисту для операторських мереж [12]. Наукові огляди з питань 5G-IoT підкреслюють складність забезпечення конфіденційності, цілісності й доступності даних у масових сенсорних мережах та мобільних пристроях, звертаючи увагу на вразливості, пов'язані з протоколами доступу, керуванням ключами та гетерогенністю обладнання [11, 13]. Водночас більшість робіт орієнтована на цивільних операторів і не враховує специфіку бойового середовища, коли противник одночасно застосовує РЕБ, кіберзасоби та кінетичний вплив по елементах інфраструктури.

Окремий напрям становлять дослідження інтеграції штучного інтелекту в тактичні мережі та системи зв'язку, де 5G розглядається як один із ключових транспортних рівнів. Сучасні огляди демонструють значний потенціал використання ШІ для адаптивного керування ресурсами мережі, динамічного маршрутизаційного та радіопланування, а також для підтримки прийняття рішень у реальному часі [8]. Проте питання сумісності таких рішень із наявними системами зв'язку, їх стійкості до цілеспрямованих атак на моделі ШІ та практичні аспекти впровадження в умовах обмежених обчислювальних ресурсів у польових вузлах розкриті лише фрагментарно.

Узагальнюючи, можна констатувати, що розглянуті дослідження дають розгорнуте бачення потенціалу 5G у військовому зв'язку, окреслюють базові архітектури корпоративних мереж, моделі загроз і загальні підходи до кіберзахисту [2–7, 9, 10–13]. Водночас недостатньо опрацьованими залишаються питання адаптації цих рішень до умов тривалих бойових дій високої інтенсивності, інтеграції 5G з наявною інфраструктурою зв'язку сил оборони, оцінювання стійкості 5G-мереж до комбінованого радіоелектронного та кібернетичного впливу, а також визначення безпечних моделей взаємодії з іноземними постачальниками обладнання і програмного забезпечення. Саме заповненню цих прогалин у контексті потреб і обмежень оборонного сектору України присвячено подальші розділи статті.

Мета статті полягає в обґрунтуванні підходів до інтеграції технологій 5G у систему військового зв'язку та управління сил оборони України шляхом аналізу можливостей 5G, кіберзагроз, проблем сумісності та формуванні рекомендацій щодо їх поетапного впровадження.

Виклад основного матеріалу.

1. Ключові характеристики 5G, релевантні для військового зв'язку.

Технологія мобільного зв'язку п'ятого покоління поєднує три основні класи сервісів: eMBB (enhanced Mobile Broadband), URLLC (Ultra-Reliable Low-Latency Communications) та mMTC (massive Machine-Type Communications) [1]. Для військового застосування найбільший інтерес становлять URLLC та mMTC, оскільки вони забезпечують наднизьку затримку (одиниці мілісекунд) при високій надійності каналу, а також можливість одночасного підключення великої кількості сенсорів, платформ та вузлів управління [1, 2]. Додатковою перевагою є мережеве сегментування (network slicing), яке дозволяє створювати логічно ізольовані *зрізи* мережі для критичних та некритичних сервісів з гарантованими параметрами якості обслуговування [9].

Особливістю 5G є широке використання віртуалізації мережевих функцій, програмно-конфігурованих мереж та відкритих інтерфейсів, що дає змогу гнучко перерозподіляти ресурси між сервісами, швидко розгортати нові функції й адаптувати конфігурацію мережі до змін обстановки [2]. Для військових систем зв'язку це відкриває можливість створення адаптивних тактичних мереж, у яких ресурси автоматично перерозподіляються між напрямками із найбільш критичним навантаженням, наприклад, у районі масованого застосування безпілотних систем або під час ведення інтенсивних вогневих дій.

2. Можливості 5G для IoMT та автономних платформ.

Дослідження NATO C2COE, RAND («Research ANd Development» аналітичний центр США) та низки європейських авторів демонструють, що 5G є гармонійною транспортною основою для концепції Internet of Military Things, яка охоплює сенсорні мережі розвідки, системи спостереження, безпілотні літальні апарати, наземні й морські автономні платформи [6, 7, 15]. Висока щільність підключень у поєднанні з URLLC дозволяє формувати розподілені мережі спостереження й ураження, де дані з численних сенсорів та платформ агрегуються і передаються в центри обробки майже в реальному часі.

У морській та береговій сфері 5G розглядається як доповнення до супутникових і традиційних радіосистем для забезпечення високошвидкісних каналів між кораблями, береговою інфраструктурою та безпілотними морськими платформами [15]. Для сухопутних військ ключовою є можливість підтримки *роїв* БпЛА та наземних роботизованих платформ, де мережа 5G забезпечує обмін телеметрією, відео та командами управління, а також взаємодію між платформами на рівні «машина – машина» [6, 14].

3. Інтеграція 5G та штучного інтелекту в тактичних мережах.

Сучасні дослідження зосереджені на тому, як використання штучного інтелекту в поєднанні з 5G може підвищити ефективність тактичних мереж зв'язку. Зокрема, показано перспективність застосування алгоритмів ШІ для динамічного планування радіоресурсу, адаптивної маршрутизації, виявлення аномалій трафіку й підтримки прийняття рішень командуванням [8]. 5G у цьому разі виступає як високошвидкісний і низьколатентний транспортний рівень, що дозволяє розміщувати частину інтелектуальних функцій ближче до *краю* мережі (edge computing) та зменшувати час реакції системи, це є особливо важливим для систем чутливих до часу відгуку, таких як Internet of Military Things.

Для сил безпеки та оборони України це створює передумови для побудови розподілених систем управління, де окремі блоки аналітики, заснованої на ШІ, можуть розміщуватися безпосередньо у вузлах тактичного рівня, аналізуючи потоки даних від сенсорів, БпЛА та систем розвідки й автоматично формуючи рекомендації для командирів. Водночас інтеграція таких рішень потребує чітко визначених вимог до обчислювальних ресурсів, захисту моделей ШІ від компрометації та забезпечення їх стійкості до цілеспрямованих атак [8].

4. Кібербезпекові аспекти застосування 5G у військових мережах.

Європейський *набір інструментів* з кібербезпеки 5G, рекомендації ENISA, ITU та NIST NCCoE показують, що розгортання 5G супроводжується суттєвим розширенням поверхні атаки через віртуалізацію, хмарну інфраструктуру, відкриті інтерфейси та використання компонентів різних постачальників [4, 5, 12]. У наукових оглядах, присвячених безпеці 5G-IoT, підкреслюються вразливості протоколів доступу, проблеми управління ключами, оновлення прошивок для масових пристроїв та ризики компрометації *кінцевих точок* [11, 13].

Для військових мереж це означає необхідність застосування принципів *нульової довіри*, жорсткої сегментації та мікросегментації, багаторівневого контролю доступу й безперервного моніторингу аномалій трафіку. Додатково необхідно враховувати можливість поєднання кібератак із застосуванням засобів РЕБ та фізичним ураженням окремих вузлів, що вимагає проєктування мережі з надлишковістю ключових елементів, використанням декількох незалежних маршрутів і сценаріїв деградованого режиму роботи [5, 12].

5. Сумісність із наявною інфраструктурою та постачальницькі ризики.

Документи США, НАТО та ЄС підкреслюють важливість інтеграції 5G з наявними системами зв'язку, включно з тактичними радіомережами, супутниковими каналами та застарілими проводовими системами [2, 3, 7, 9]. Пропонуються різні варіанти шлюзів і проміжних рівнів, які забезпечують взаємодію IP-базованих 5G-мереж із системами, що використовують інші протоколи й стандарти. У той же час значна увага приділяється питанню вибору постачальників, оцінюванню ризиків ланцюгів поставок, наявності небезпечних залежностей від окремих держав та можливості прихованого впливу на мережеву інфраструктуру [4, 5, 14].

Для України актуальними є як технічні, так і політико-економічні аспекти цієї проблеми. Значна частина наявної інфраструктури військового зв'язку базується на обладнанні різних поколінь і стандартів, що ускладнює побудову єдиного інформаційного простору. Вибір рішень 5G повинен здійснюватися з урахуванням вимоги до повного контролю над програмним забезпеченням, прозорості ланцюгів поставок, можливості локального виробництва або принаймні розгортання елементів мережі силами вітчизняних підприємств оборонно-промислового комплексу [3, 5, 14].

6. Міжнародний досвід інтеграції 5G у військових системах зв'язку.

Досвід США демонструє переважно експериментально-демонстраційний підхід до інтеграції 5G у військову інфраструктуру. Стратегія та плани впровадження передбачають створення низки пілотних майданчиків на базах та полігонах, де відпрацьовуються сценарії застосування корпоративних 5G-мереж для підтримки логістики, тактичних операцій, виробничих процесів оборонних підприємств, а також взаємодії з наявними системами зв'язку [2–4]. При цьому основна увага приділяється побудові ізольованих, контрольованих оператором оборонного відомства мереж із чітко визначеними вимогами до кібербезпеки, контролю ланцюгів постачання та можливості масштабування рішень у майбутньому.

У рамках НАТО проведено низку дослідницьких програм та експериментів, присвячених використанню 5G для підтримки операцій Альянсу, включно з опрацюванням архітектур корпоративних мереж, застосуванням механізмів network slicing і забезпеченням взаємодії з наявними C4ISR-системами [7, 9]. У публікаціях та технічних звітах наголошується на важливості стандартизованих інтерфейсів, можливості розгортання 5G як у стаціонарних, так і в мобільних конфігураціях, а також на потребі тісної координації між державами-членами при виборі постачальників і визначенні вимог до кіберзахисту [4, 5]. Досвід європейських країн доповнюється проєктами із використання 5G у морській сфері, де технологія застосовується для забезпечення зв'язку між кораблями, портовою інфраструктурою та безпілотними морськими платформами [15].

Китайський підхід характеризується глибокою інтеграцією цивільної та військової сфер, високою щільністю розгортання 5G-мереж та реалізацією концепції «військово-цивільного злиття» у галузі телекомунікацій [14]. 5G розглядається як базова платформа для побудови інтегрованих мереж розвідки, спостереження та управління, підтримки автономних систем і високошвидкісного обміну даними між різнорідними платформами. Водночас існують суттєві відмінності в нормативно-

правовій базі, структурі управління та ресурсних можливостях, що ускладнює пряме перенесення моделі китайських рішень в українські реалії.

Зіставлення зазначених прикладів дозволяє виділити спільні риси міжнародного досвіду: переважно поетапний характер інтеграції 5G (від експериментальних полігонів до критичних об'єктів), фокус на корпоративних мережах оборонного призначення, жорсткі вимоги до кібербезпеки й контролю постачальників, а також орієнтацію на інтеграцію з наявною інфраструктурою, а не її повну заміну [2–7, 9, 14, 15]. Водночас майже всі наведені рішення розроблялися в умовах відсутності тривалих бойових дій високої інтенсивності, що обумовлює необхідність їх адаптації до специфіки українського театру воєнних дій та ресурсних обмежень оборонного сектору України.

7. Пропонована модель поетапної інтеграції 5G у систему військового зв'язку України.

На підставі аналізу міжнародного досвіду та наукових досліджень пропонується модель поетапного впровадження 5G у систему військового зв'язку сил оборони України.

Перший етап – експериментальні корпоративні мережі. Розгортання ізольованих корпоративних 5G-мереж на полігонах, у навчальних центрах та на окремих стаціонарних об'єктах тилу для відпрацювання типових сценаріїв застосування: підтримка БпЛА, сенсорних мереж, логістичних процесів і елементів C4ISR [2, 3, 6, 7]. На цьому етапі формується національна нормативна база, моделі загроз та вимоги до архітектури захищених 5G-рішень.

Другий етап – розгортання у критичних тилових вузлах. Інтеграція корпоративних 5G-мереж у логістичні хаби, пункти управління оперативно-стратегічного рівня, об'єкти з підвищеними вимогами до пропускної здатності й надійності. Передбачається взаємодія з наявними волоконно-оптичними та радіорелейними системами, впровадження розширених механізмів мережевого сегментування й засобів моніторингу кібербезпеки [3, 5, 7, 9].

Третій етап – інтеграція з тактичними мережами та бойовими платформами. Розгортання мобільних або транспортованих 5G-рішень у районах ведення бойових дій для підтримки тактичних підрозділів, *роїв* БпЛА, розподілених сенсорних мереж і систем підтримки прийняття рішень у реальному часі [6, 7, 14, 15]. На цьому етапі критичними стають питання стійкості до РЕБ, можливості швидкого розгортання/згортання мережі, а також інтеграції з алгоритмами ШІ для автоматизованого керування ресурсами [8].

Четвертий етап – довгострокова перспектива інтеграції з наступними поколіннями мереж. З урахуванням глобальних трендів передбачається поступовий перехід до інтегрованих архітектур 5G/6G, у яких опорна мережа та сервіси обробки даних поєднують наземні, повітряні й космічні сегменти, забезпечуючи стале інформаційне середовище для сил оборони [9, 10].

Запропонована модель може бути використана як основа для розроблення відомчих концепцій розвитку систем військового зв'язку, програм модернізації інфраструктури та планів дослідно-конструкторських робіт у сфері 5G-рішень оборонного призначення.

Висновки

Проведене дослідження показало, що технологія мобільного зв'язку п'ятого покоління є одним з ключових чинників трансформації систем військового зв'язку та управління сил оборони. Характерні для 5G висока пропускна здатність, наднизька затримка, підтримка масового підключення пристроїв і розвинуті механізми мережевої сегментації створюють передумови для побудови розподілених сенсорних мереж, підтримки *роїв* безпілотних і автономних платформ, інтеграції систем штучного інтелекту в контури управління та автоматизації логістичних процесів.

Водночас встановлено, що широке використання віртуалізації, хмарних технологій, відкритих інтерфейсів і багатовендорної інфраструктури суттєво розширює поверхню атаки й породжує новий спектр кіберзагроз, проблем сумісності з наявними засобами зв'язку та ризиків технологічної залежності від іноземних постачальників. Міжнародний досвід США, НАТО, країн ЄС і Китаю підтверджує доцільність поетапного переходу до корпоративних 5G-мереж оборонного

призначення, однак не дає готових рішень для умов тривалих бойових дій високої інтенсивності, в яких перебуває Україна.

Наукова новизна роботи полягає у комплексному поєднанні аналізу технічного потенціалу 5G, кібербезпекових, організаційних та постачальницьких ризиків із розробленням структурованої моделі поетапної інтеграції 5G у систему військового зв'язку сил безпеки та оборони України. Запропоновано узгоджену послідовність етапів – від експериментальних корпоративних мереж до інтеграції з тактичними системами й перспективними архітектурами 5G/6G – з урахуванням вимог до стійкості, сумісності та кіберзахищеності. Практичне значення результатів полягає в можливості використання запропонованих підходів під час формування відомчих концепцій розвитку зв'язку, планів модернізації інфраструктури та програм підготовки фахівців.

Перспективи подальших досліджень пов'язані з поглибленою кількісною оцінкою стійкості корпоративних 5G-мереж до комбінованого радіоелектронного та кібернетичного впливу, розробленням методик випробувань у полігонних умовах, створенням моделей довіри до елементів ланцюгів постачання, а також інтеграцією 5G-рішень із національними системами управління військами й озброєнням. Окремим напрямом є розроблення прикладних сценаріїв застосування 5G для конкретних підрозділів і родів військ із урахуванням досвіду поточних бойових дій.

Перелік джерел та посилань

1. 5G Americas. New Services & Applications with 5G Ultra-Reliable Low Latency Communications. *5G Americas*, 2018. URL: https://www.5gamericas.org/new-services-applications-with-5g-ultra-reliable-low-latency-communications/ (дата звернення: 18.06.2025).
2. Department of Defense 5G Strategy. Washington, DC: U.S. Department of Defense, 2020. URL: https://www.cto.mil/wp-content/uploads/2020/05/ DoD_5G_Strategy_May_2020. pdf (дата звернення: 18.06.2025).
3. Department of Defense Chief Information Officer. DoD Private 5G Deployment Strategy. Washington, DC: DoD CIO, 2024. URL: https://dodcio.defense.gov/Portals/0/ Documents/Library/DoD_Private5GDeployment Strategy_508.pdf (дата звернення: 18.06.2025).
4. ENISA. 5G Cybersecurity Standards. *European Union Agency for Cybersecurity*, 2022. URL: https://www.enisa.europa.eu/ publications/5g-cybersecurity-standards (дата звернення: 18.06.2025).
5. European Union. Cybersecurity of 5G Networks – EU Toolbox of Risk-Mitigating Measures. *Brussels: European Commission*, 2020. URL: https://digital-strategy. ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures (дата звернення: 18.06.2025).
6. Gopal V. (2021). Militarisation of 5G: A necessity for the forces (CLAWS Issue Brief No. 291). *Centre for Land Warfare Studies*. URL: https://www.researchgate.net/ publication/351903860_Militarisation_of_5G _A_Necessity_for_the_Forces (дата звернення: 18.06.2025).
7. Lee M., Dimarogonas J., Geist E., Manuel S., Schwankhart R., Downing B. Opportunities and Risks of 5G Military Use in Europe. *Santa Monica: RAND Corporation*, 2023. (Research Report RR-A1351-2). URL: https://www.rand.org/pubs/ research_reports/RRA1351-2.html (дата звернення: 18.06.2025).
8. Monzon Baeza V., Parada R., Concha Salor L., Monzo C. AI Integration in Tactical Communication Systems and Networks: A Survey and Future Research Directions. *Systems*. 2025. Vol. 13, No. 9. Art. 752. DOI: 10.3390/systems13090752. URL: https://doi.org/10.3390/systems13090752 (дата звернення: 18.06.2025).
9. NATO Science and Technology Organization. 5th Generation International Mobile Telecommunications (5G) Technologies Application to NATO Operations. Vol. I: *STO Technical Report TR IST-187. Neuilly-sur-Seine: NATO STO*, 2024. URL: https://www.sto.nato.int/document/5th-generation-international-mobile-telecommunications-5g-technologies-application-to-nato-operations-vol-i/ (дата звернення: 18.06.2025).
10. Van Sambeek, M. (2019). 5G technologies in military communications. *In C2COE Symposium "Get Connected"*, Brussels, Belgium, 26–27 June 2019. URL: https://c2coe.org/wp-content/uploads/2019/10/PDF-5G-Technologies-in-Military-Communications-Mr.-Marcel-van-Sambeek.pdf (дата звернення: 18.06.2025).

11. Sousa A., Reis M. J. C. S. 5G Security Features, Vulnerabilities, Threats, and Data Protection in IoT and Mobile Devices: A Systematic Review. *Evolutionary Studies in Imaginative Culture*. 2024. Vol. 8, No. S2. Pp. 414–427. DOI: 10.70082/esiculture.vi.1054 (дата звернення: 18.06.2025).

12. ITU-D Study Group 2, Question 3/2. 5G Cybersecurity. *Geneva: International Telecommunication Union*, 2024. URL: https://www.itu.int/pub/D-STG-SG02.03.2-2024 (дата звернення: 18.06.2025).

13. Valadares D. C. G., Will N. C., Sobrinho Á., Lima A., Morais I., Santos D. Systematic Literature Review on 5G-IoT Security Aspects. *Preprints*. 2023. DOI: 10.20944/preprints202311.0565.v1 (дата звернення: 18.06.2025).

14. Wu H. China's Approach to Military 5G Networks and Related Military Applications. *Tallinn: NATO Cooperative Cyber Defence Centre of Excellence*, 2023. URL: https://ccdcoe.org/library/publications/chinas-approach-to-military-5g-networks-and-related-military-applications/ (дата звернення: 18.06.2025).

15. Zmysłowski D., Skokowski P., Malon K., Maślanka K., Kelner J. Naval Use Cases of 5G Technology. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*. 2023. Vol. 17, No. 3. Pp. 595–603. DOI: 10.12716/1001.17.03.11 (дата звернення: 18.06.2025).

Стаття надійшла до редакції 19.11.2025 р.

UDC 621.396:355.4:004.056

V. Ushakov

INTEGRATION OF 5G NETWORKS INTO MILITARY COMMUNICATION SYSTEMS: PROSPECTS AND CHALLENGES

Modern operations of the defence forces of Ukraine require high-speed, secure and flexible military communication systems capable of supporting massive connectivity of sensors, unmanned and autonomous platforms, decision-support systems and logistics services in real time. Traditional tactical-level networks based on legacy technologies do not provide the required throughput, latency and resilience to cyber threats under conditions of intensive use of electronic warfare means and enemy cyber operations. Fifth-generation mobile communication technology (5G) is considered by the leading armies of the world as a key element in the transformation of C4ISR systems, tactical networks and the Internet of Military Things (IoMT) infrastructure.

The article examines the technical capabilities of 5G that are critical for military use, in particular high throughput, ultra-low latency, increased reliability, support for massive device connectivity and network slicing mechanisms. The potential of 5G for building distributed sensor networks, supporting "swarms" of unmanned and autonomous combat platforms, integrating artificial intelligence systems into the command-and-control and weapon-control loops, as well as automating logistics processes is shown. The international experience of NATO, the USA, EU member states and China in deploying private defence 5G networks and integrating them with existing communication systems is summarised. It is substantiated that the extensive use of virtualised components, open interfaces and multi-vendor solutions in 5G leads to a significant increase in the attack surface and forms a new spectrum of cyber threats, problems of compatibility with legacy communication systems and risks of technological dependence on foreign suppliers. The main approaches to the phased integration of 5G into the military communication systems of the defence forces of Ukraine are formulated, including the requirements for the architecture of private networks, the organisation of cyber defence and the management of supply-chain risks.

Keywords: *5G, military communications, tactical networks, cybersecurity, autonomous combat platforms, Internet of Military Things (IoMT), private 5G networks, artificial intelligence.*

Ушаков Володимир Анатолійович – викладач кафедри військового зв'язку та інформатизації, Національна академія Національної гвардії України

https://orcid.org/0009-0002-9543-4882