УДК 351/354+328
DOI: 10.35432/tisb292023289498

НАГАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СИСТЕМИ ВІЙСЬКОВОГО УПРАВЛІННЯ

Горб Володимир Вікторович
здобувач
Інститут публічної служби та управління
Національний університет «Одеська політехніка»,
співробітник Служби безпеки України
https://orcid.org/0009-0003-8919-6790

Згідно з статтею 4 Кодексу адміністративного судочинства України публічна служба – це діяльність на державних політичних посадах, професійна діяльність суддів, прокурорів, військова служба, альтернативна (невійськова) служба, дипломатична служба, інша державна служба, служба в органах влади Автономної Республіки Крим, органах місцевого самоврядування [1].

Вищенаведена дефініція є надширокою, однак дозволяє розглядати публічну службу як систему, основними елементами якої являються види публічно-службової діяльності, що її складають.

Стаття 2 Закону України «Про військовий обов'язок і військову службу» визначає, що військова служба є державною службою особливого характеру, яка полягає у професійній діяльності придатних до неї за станом здоров'я і віком громадян України, іноземців та осіб без громадянства, пов'язаній із обороною України, її незалежності та територіальної цілісності [2].

В умовах воєнного стану особливо актуальним є дослідження системи управління сектору оборони та безпеки як складової системи державного управління. Являючись одним з визначальних елементів для здобуття перемоги у війні з російськими окупантами, вона потребує розв'язання комплексу нагальних проблемних питань.

Військова наука визначає управління військами як процес цілеспрямованого впливу командувачів (командирів), штабів на війська, що здійснюється для підтримки готовності військ до виконання завдань за призначенням, їх підготовки та успішного виконання ними завдань у ході ведення операції (бойових дій). Організація управління військами полягає у створенні і розгортанні системи управління, визначенні завдань та порядку роботи штабу під час підготовки і в ході ведення військових операцій (бойових дій) та забезпечення стійкої і безперервної роботи пунктів управління, засобів зв'язку і АУВ для своєчасного і якісного виконання завдань управління [3].

Наразі обумовлена війною перебудова управлінської вертикалі відбувається із значним випередженням процесів організації зв'язку та інформатизації управління зокрема. Адже швидкоплинність таких трансформацій потребує не тільки достатньої кількості інтероперабельних технічних та програмних засобів, а й наявність резерву для маневрів сил. В умовах сьогодення дефіцит взаємодії особливо відчутний на тактичному рівні управління. Діючи в умовах крайньої необхідності, компенсація згаданої нестачі здійснюється за рахунок повсюдного використання мобільних застосунків (додатків) для смартфонів, планшетів, персональних комп'ютерів. Найбільш поширені в силу належності до країни-розробника софту та особливостей безпекових сервісів – WhatsApp, Signal, Telegram. Рівень комунікації силових структур через застосування вищеперелічених програм сьогодні можна констатувати як тотальний. Основною організаційною формою взаємодії зацікавлених учасників є групи, керовані одним чи декількома адміністраторами. У даному контексті до загроз, що вже набули реалізації та тих, які потенційно можуть настати можна впевнено

віднести виток важливої інформації (в тому числі з обмеженим доступом), втрату взаємодії та управління у критичні моменти функціонування, порушення достовірності, цілісності, актуальності даних. Найбільшої гостроти названа проблема набула після ракетних ударів ворога по об'єктах енергосистеми нашої країни. Внаслідок планових та аварійних відключень світла звичні системи зв'язку стандарту GSM та протоколи обміну даними 3G, 4G LTE, Wi-Fi в одних випадках не забезпечували стабільну роботу, а в інших не працювали взагалі.

Для пошуку причин такого стану справ доречно провести ретроспективний аналіз розвитку нормативно-правової бази та впровадження інформаційно-телекомунікаційних технологій в діяльність МОУ, СБУ, МВС.

Так, «Основні напрямки розвитку озброєння та військової техніки на довгостроковий період», схвалені розпорядженням КМУ від 14 червня 2017 р. № 398-р [4], серед інших, декларують наступні цілі у сфері зв'язку та автоматизації:

- удосконалення стаціонарної та мобільної складової системи зв'язку Збройних Сил, інших військових формувань сектору безпеки і оборони шляхом створення єдиних систем адресації та маршрутизації;
- створення системи захищеного супутникового зв'язку в інтересах ЗС України як основи для подальшого створення системи супутникового зв'язку сектору безпеки і оборони.
- створення автоматизованих мереж захищеного радіозв'язку на платформі програмованих радіозасобів «Software-Defined Radio» та розгортання мереж широкосмугового високошвидкісного радіодоступу;
- формування Єдиної автоматизованої системи управління Збройних Сил (C4ISR) та інтеграція до неї автоматизованих систем усіх видів та спеціальних військ.

Відповідно до обраного Україною курсу на євроатлантичну інтеграцію одним із пріоритетних завдань оборонної реформи є створення єдиної автоматизованої системи управління ЗСУ архітектури C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, тобто командування, контроль, зв'язок, комп'ютери, розвідка, спостереження та рекогностування), як основи системи управління силами оборони держави [5]. В той же час, незважаючи на окремі позитивні напрацювання та технічні розробки, фактичний стан справ засвідчує про відсутність на озброєнні навіть систем нижчого рівня С4, С2, Battle management system (BMS).

Функціонування об'єднаної автоматизованої інформаційної системи у сфері боротьби з тероризмом в процесі антитерористичного забезпечення об'єктів можливого терористичного посягання передбачено чинною Концепцією боротьби з тероризмом в Україні (53/2019) [6], а також Планом заходів з її реалізації (7-2021-р) [7].

Підтвердження солідарності ідеї інформатизації у секторі національної безпеки знаходить своє відображення у Положенні про Антитерористичний центр та його координаційні групи при регіональних органах СБУ. Однак в реальності як організаційні та правові, так і будівельно-технічні заходи з впровадження у діяльність суб'єктів боротьби з тероризмом галузевої системи перебувають в стадії зародження.

Концепція програми інформатизації системи Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2021-2023 роки [8], являється новою галузевою програмою інформатизації системи МВС та підшефних їй структур. Вона зосереджена на розбудові публічних сервісів єдиної інформаційної системи МВС, упровадженні та модернізації національних електронних інформаційних ресурсів як складових єдиної інформаційної системи МВС, створенні інноваційної інфраструктури органів системи МВС. Серед галузевих проєктів інформатизації, реалізація яких закріплена у розпорядженні Кабінету Міністрів України від 17 лютого 2021 р. № 365-р [9], схвалено такі проєкти цифрової трансформації системи МВС України на період до 2023 року, як «Безпечна країна», «Система 112», «Єдиний реєстр зброї», «Реєстр відомостей про статус особи у кримінальному провадженні та судимості», «Єдиний сервіс ідентифікації фізичних осіб», «Система планування та управління об'єднаними силами із забезпечення громадської

безпеки та ліквідації надзвичайних ситуацій» та інші (усього 14 проєктів).

Законодавчо закріплені в період суспільного усвідомлення найбільшої терористичної загрози – агресивної політики Російської Федерації та спрямовані на подолання нових викликів, що постали перед воєнною організацією України і водночас частково або повністю не реалізовані правові норми, концепції, нажаль, є відображенням дійсного стану справ з реалізації права законодавчих ініціатив визначеними суб'єктами.

До вдалих впроваджених проєктів з цифровізації сфери службової діяльності слід віднести Єдину інформаційну систему МВС – інтеграційної платформи, що використовується для різноманітних Е-послуг. Досягнутий успіх є результатом виконання аналогічної галузевої програми інформатизації на 2018 - 2020 роки. Прикладом запозичення іноземних розробок являється система електронної взаємодії національних електронних інформаційних ресурсів «Трембіта». Побудована на базі естонської платформі обміну даними «X-road» вона являється системою архітектури інтероперабельності [10]. У військовій сфері частково запроваджена мобільна автоматизована система бойового управління силами та засобами авіації, протиповітряної оборони ЗСУ «Ореанда-ПС», у лютому поточного року українська армія повідомила про запровадження системи управління військами «Дельта».

В умовах війни гідний внесок у боротьбу з окупантами зроблено компанією «SpaceX» у вигляді постачання комплектів глобальної супутникової системи «Starlink». Здійснений запуск модулю інформаційно-аналітичної системи для моніторингу постачання Україні озброєння «СОТА», мобільного додатку для сповіщення про ворожі повітряні атаки «єППО». Напрацюваннями з автоматизації комунікацій є офіційні Telegram-боти «@stop_russian_war_bot» (СБУ), «StopRussia», «Народний месник» (Кіберполіція) та інші.

Таким чином, сьогоденна реальність воєнного стану України закладає нові камені у фундамент її державотворення. Форсований війною принцип розвитку, притаманний базовій діалектичній ідеї, наразі особливо характерний для перебудови системи воєнного управління. В той же час, спостерігається асинхронність у протіканні інших законів діалектики – загального зв'язку, детермінізму, системності, об'єктивності. Тобто, виникнення нових військових і правоохоронних об'єднань та з'єднань, не супроводжується одночасною інформатизацією таких організмів.

Нормативно-правова база, представлена у вигляді концепцій, стратегій, положень тощо у дійсності відображає сучасний і навіть дещо амбіційний вектор цифровізації усієї військової і правоохоронної сфери, однак його релевантність нагальним запитам оборонних та безпекових структур вкрай низька.

Аналіз міжнародного досвіду вказує на закономірність, що спеціалізовані інформаційні системи та мережі на озброєнні сектору безпеки і оборони є з одного боку результатом практичної реалізації положень тих чи інших далекоглядних стратегій і концепцій, а з іншої сторони в процесі експлуатації довели свою виключну ефективність, яка врахована як одна з вихідних умов при визначені напрямів подальшого розвитку цих систем.

Усвідомлення дійсності сучасності, що більшість диверсантів на всій території України це етнічні українці та набуті у ході оперативно-службової діяльності СБУ пізнання засвідчують про активне використання ворогом усіх можливостей ІТ-сфери для проведення підривної роботи на наших землях. Вказане засвідчує на необхідності вжиття симетричних і форсованих дій, спрямованих на ефективну протидію потенційним і реальним диверсійно-терористичним загрозам. Це сигнал для переосмислення застарілих поглядів і підходів, викорінення анахронічних технологій і відмінностей між платформами та рішеннями в різних відомствах, впровадження нових норм і стандартів – інноваційних, гнучких, прогресивних.

Список літератури

1. Кодекс адміністративного судочинства України: Закон України 6 липня 2005 року № 2747-IV. Відомості Верховної Ради України, 2005, № 35-36, № 37, ст.446.

2. Закон України «Про військовий обов'язок і військову службу» від 25 березня 1992

року № 2232-XII. Редакція від 05.02.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2232-12#Text, (дата звернення: 19.03.2023).

3. Матеріали універсальної інтернет-енциклопедії. URL: https://uk.wikipedia.org/wiki/Система_управління_військами (дата звернення: 19.03.2023).

4. Розпорядження Кабінету Міністрів України від 14 червня 2017 р. № 398-р «Про схвалення Основних напрямів розвитку озброєння та військової техніки на довгостроковий період». Редакція від 21.07.2021 р., URL: https://zakon.rada.gov.ua/laws/show/398-2017-%D1%80#Text.

5. Defense Express. «Від С2 до С4ISR: що ховається за цими абревіатурами». URL: https://defence-ua.com/weapon_and_tech/vid_s2_do_s4isr_scho_hovajetsja_za_tsimi_abreviaturami-872.html.

6. Закон України «Про Концепцію боротьби з тероризмом в Україні» від 05.03.2019 року №53/2019. Редакція від 05.03.2019 р. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text, (дата звернення: 25.11.2022).

7. Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України: Указ Президента України від 14.04.1999 р. № 379/99. Редакція від 11.06.2022 р. URL: https://zakon.rada.gov.ua/laws/show/379/99#Text, (дата звернення: 25.11.2022).

8. Розпорядження Кабінету Міністрів України від 5 січня 2021 р. № 7-р «Про затвердження плану заходів з реалізації Концепції боротьби з тероризмом в Україні». Редакція від 05.01.2021 р. URL: https://zakon.rada.gov.ua/laws/show/7-2021-%D1%80#Text, (дата звернення: 25.11.2022).

9. Наказ МВС України від 22 квітня 2021 року № 301 «Про оголошення рішення колегії МВС України». Концепція програми інформатизації системи МВС України та центральних органів виконавчої влади, діяльність яких спрямовується і координується КМУ через міністра внутрішніх справ України, на 2021-2023 роки. URL: https://mvs.gov.ua/uk/press-center/news/rozvitok-cifrovoyi-infrastrukturi-ta-stvorennya-cifrovix-servisiv-dlya-gromadyan-prioritet-programi-informatizaciyi-sistemi-mvs.

10. Розпорядження Кабінету Міністрів України від 17 лютого 2021 р. № 365-р «Деякі питання цифрової трансформації». Редакція від 15.09.2022 р. URL: https://zakon.rada.gov.ua/laws/show/398-2017-%D1%80#Text, (дата звернення: 01.12.2022).

11. Постанова Кабінету Міністрів України від 08 вересня 2016 р. № 606 «Деякі питання електронної взаємодії державних електронних інформаційних ресурсів». Редакція від 01.12.2022 р. URL: https://zakon.rada.gov.ua/laws/show/606-216-%D0%BF#Text, (дата звернення: 01.12.2022).