УДК 343.341:323.28(477)
DOI https://doi.org/10.32850/sulj.2022.4.1.41

ОБ'ЄДНАНІ АВТОМАТИЗОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОТИДІЇ ДИВЕРСІЙНО-ТЕРОРИСТИЧНИМ ЗАГРОЗАМ

Горб В. В.

Розглянуто проблему перетворення стратегії і тактики дій російських окупаційних військ в Україні шляхом застосування диверсійно-терористичної діяльності як інструменту для досягнення комплексу цілей невоєнного характеру. Окреслено трансформаційні процеси, що зазнає воєнна організація України сьогодні, утворення і розвиток нових військових формувань з протидії диверсіям та терористичним актам зокрема. На рівні концепцій охарактеризовані напрями інформатизації Міністерства оборони України, Служби безпеки України, Міністерства внутрішніх справ України, наведені позитивні напрацювання та технічні розробки в одних відомствах, а також акцентовано увагу на прорахунках і відсутності поступального розвитку інформаційних систем, процесів автоматизації в інших. Досліджено проблемні питання, пов'язані з недостатньою інформатизацією структур секторів безпеки та оборони, які в умовах війни протидіють ворогові, а також обґрунтована необхідність впровадження сучасних технологій, стандартів управління і взаємодії під час реалізації завдань із захисту держави. Виведений висновок про низьку релевантність існуючої нормативно-правової бази сьогоденним запитам визначеного кола суб'єктів боротьби з тероризмом та нагальну потребу повсюдної інформатизації силових структур.

Ключові слова: *воєнна організація держави, диверсійно-терористична діяльність, інформаційна система, автоматизована система, цифровізація, терористичні загрози.*

Horb V. V. Unified automated information systems as a tool for increasing the effectiveness of countering subversive and terrorist threats

The problem of transforming the strategy and tactics of the Russian occupation forces in Ukraine through the use of subversive-terrorist activities as a tool for achieving a set of non-military goals is considered. The transformational processes that the military organization of Ukraine is undergoing today, the formation and development of new military formations to counter sabotage and terrorist acts, in particular, are outlined. At the level of concepts, the directions of informatization of the Ministry of Defense of Ukraine, the Security Service of Ukraine, the Ministry of Internal Affairs of Ukraine are characterized, positive developments and technical developments in some departments are given, and attention is also focused on miscalculations and the lack of progressive development of information systems and automation processes in others. Problematic issues related to insufficient informatization of the structures of the security and defense sectors, which oppose the enemy in conditions of war, as well as the justified need for the introduction of modern technologies, standards of management and interaction during the implementation of state defense tasks, have been studied. The conclusion is drawn about the low relevance of the existing regulatory and legal framework to today's requests of a certain circle of actors in the fight against terrorism and the urgent need for widespread informatization of law enforcement agencies.

Key words: *military organization of the state, subversive-terrorist activity, information system, automated system, digitalization, terrorist threats.*

Постановка проблеми. Війна Росії проти України породжує нову віху в розвитку оперативного, воєнного мистецтва і виникнення досі невідомих наукових поглядів, практичного досвіду у різних галузях знань. Обумовлені під впливом широкомасштабного російського вторгнення зміни в організаційно-технічних формах і методах роботи правоохоронних органів відбуваються і в системі антитерористичного захисту держави, її адаптації та трансформації до реалій об'єктивної дійсності.

Наряду з обстрілами з використанням артилерії, реактивних систем залпового вогню, балістичних ракет та авіації об'єктів військової інфраструктури, російські війська знищують церкви, школи, лікарні, житлові райони, міста… Відповідаючи на запитання про те, чи готова Європа визнати росію країною-терористом, Генеральний секретар Європейського Парламенту Клаус Велле зауважив: «Те, що відбувалося тут (Буча), і те, що відкривається нині в Ізюмі, – це, беззаперечно, тероризм у дії. Те, що робить російське військо в Україні, – це,

безперечно, злочини. Маємо визнати те, що здавалося неможливим в Європі впродовж багатьох десятків років. Треба зупинити це, щоб така само війна не поширилася на нашому континенті. Сама ця війна – це беззаперечний акт тероризму. Те, що під час неї відбувається, – це також тероризм. Ми не можемо не зважати на жертви, особливо серед цивільного населення. Тому нам залишається сподіватися, що це знайде належну оцінку і світова громада знайде якісь способи, щоб належно оцінити та покарати такі дії» [1].

Кваліфіковані як воєнні злочини за статтею 438 Кримінального кодексу України за фактами порушення законів та звичаїв війни різанина цивільного населення у містах Буча, Ізюм мала на меті тероризувати усе українське населення та унеможливити опір спротиву.

Захоплення і пошкодження Запорізької АЕС, Каховської ГЕС та спеціальні інформаційні акції щодо їх можливого підриву свідчать про застосування окупантами військової тактики нового покоління – сіяння паніки, ядерний шантаж, знищення енергетичної інфраструктури, яка спрямована не стільки на безпосереднє знищення противника, скільки на досягнення політичних цілей. Одна з форм війн такого роду – це диверсійно-терористична діяльність [2].

Зважаючи на суміжність злочинів як терористичний акт і диверсія, оцінка вищевикладених жахіть засвідчує, що стратегія і тактика російсько-української війни використовує диверсійно-терористичну діяльність як єдиний інструмент досягнення «усіх цілей спеціальної операції» в Україні: військових, політичних, моральних, історичних.

Ефективна протидія агресору у зазначеному секторі національної безпеки потребує консолідації усього арсеналу сил та засобів, в тому числі шляхом підвищення рівня координації і взаємодії за рахунок інформатизації усього кола суб'єктів боротьби з тероризмом.

Аналіз останніх досліджень і публікацій. Чимало акцентувань на інформатизації та автоматизації напрямку протидії загрозам терористичного характеру наявно в наукових доробках В. Рижова, М. Шиліна, В. Крутова та інших. Зокрема, у працях І. Рижова фундаментально описана спеціалізована інформаційна система у сфері боротьби з тероризмом, побудована на новітніх комп'ютерних та мережевих технологіях в інтересах оптимізації процесів збору, обробки, накопичення інформації. Таку технологію названо моніторингом.

На застосуванні інноваційних методів, інформаційних систем, інтелектуальних технологій в процесі побудови системи антитерористичного захисту України зазначав у своїх наукових роботах В. Крутов.

Науковий огляд інформаційних систем США, Великобританії, Канади, Франції та інших країн НАТО засвідчив, що підвищення інтенсивності інформаційного обміну шляхом впровадження в діяльність правоохоронних органів інформаційних систем набувають все більшої актуальності в іноземних країнах. Успішно реалізовані у світі проекти інформатизації – системи Echelon, Prism, Frenchelon, ISE, SIS являються міждержавними метасистемами забезпечення діяльності розвідки, контррозвідки, органів правопорядку.

Однак в Україні, навіть задекларовані на законодавчому рівні далекоглядні і короткострокові перспективи протягом тривалого часу залишаються не реалізованими.

Мета статті. Провести оцінку перебудови воєнної організації України та стану взаємодії її складових елементів. Акцентувати увагу на нагальній потребі в сучасних інформаційних системах секторів оборони і безпеки для підвищення ефективності протидії диверсійно-терористичним загрозам воєнного стану.

Виклад основного матеріалу. В сучасних умовах воєнна організація нашої держави зазнає перебудови і розвитку. Відображенням трансформаційних процесів на напрямі боротьби з тероризмом є зміни в «Положенні про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України» в редакції від 11 червня 2022 року (398/2022) [3]. Відтепер, АТЦ відповідно до покладених на нього завдань, бере в установленому порядку участь у протидії диверсійним проявам (п. 14 ст. 4 Положення), а також сприяє розвідувальним органам України у виконанні покладених на них завдань та здійсненні функцій, взаємодіє із суб'єктами розвідувального співтовариства.

Аналіз оперативної обстановки на Півдні України свідчить про стрімку адаптацію органів військового управління, правоохоронних органів, інших військових формувань та виокремленні при цьому контрдиверсійної діяльності на фоні інших напрямів протидії загрозам у безпекових сферах, в тому числі терористичного характеру.

Реальним прикладом еволюції форм і методів боротьби з диверсійно-терористичними загрозами є створення у квітні 2022 року Сил спеціальних операцій з контрдиверсійної боротьби (ССО

КДБ) при основному командному пункті оперативно-стратегічного угруповання військ «Олександрія». До завдань, що покладені на вказану структуру, серед інших, віднесено проведення спеціальних розвідувальних, контрдиверсійних заходів і спеціальних операцій, спрямованих на припинення та попередження диверсійної діяльності незаконних воєнізованих або збройних формувань (груп), терористичних організацій, організованих груп та злочинних організацій та їх посібників, викриття можливих маршрутів їх пересування; виявлення місць зберігання зброї та засобів здійснення диверсій; виявлення, або отримання інформації щодо діяльності диверсійних розвідувальних груп, терористів.

Для забезпечення роботи ССО КДБ в операційній зоні вказаного ОСУВ та підпорядкованих оперативних угруповань військ включені посадові особи з числа органів СБУ, Збройних Сил України, Національної гвардії України, Державної прикордонної служби України, Національної поліції України, Головного управління розвідки Міністерства оборони України та Служби зовнішньої розвідки України, а також розроблені структура, положення, тимчасовий штат.

Подальший розвиток ССО КДБ знаходить своє відображення в утворенні нових тимчасових структур та виданні відповідних бойових документів. Зокрема, з метою виконання завдань із забезпечення заходів правового режиму воєнного стану, здійснення цілодобового контролю по забезпеченню фільтраційних, контрдиверсійних та інших заходів, передбачених правовим режимом воєнного стану, під час несення служби на блокпостах і контрольно-пропускних пунктах, подальшого збору та узагальнення отриманої інформації та прийняття управлінських рішень в інтересах ОСУВ «Олександрія», при Ситуаційному центрі Головного управління Національної поліції в Одеській області створено Координаційну групу (КГ).

До складу цієї КГ включено представників територіальних (регіональних) підрозділів ГУНП в Одеській області, Управління СБУ в Одеській області, Департаменту військової контррозвідки СБУ, Національної гвардії України, Державної прикордонної служби України, Військової служби правопорядку в ЗС України. Ідентичні КГ створені також при Ситуаційних центрах Головних управлінь Національної поліції в Миколаївській, Херсонській, Кіровоградській, Запорізькій та Дніпропетровській областях.

Військова наука визначає, що загальна організаційна побудова пункту управління (командного пункту) включає командний склад з відповідними робочими місцями та засоби зв'язку. При цьому, зв'язок з підлеглими забезпечує штаб вищого рівня.

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 9С162 «Ореанда-ПС».

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 органів, що протидіють диверсійно-терористичній діяльності. 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 (ОСУВ, ОУВ) та з'єднань (ССО КДБ, КГ при СЦ), які наразі приймають безпосередню участь у контрдиверсійній роботі, 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 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 IT-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.

Література

1. Газета Верховної Ради України «*Голос України*». «Буча, Ірпінь і те, що відбувається в Ізюмі, – це тероризм у дії», веб-ресурс URL: http://www.golos.com.ua/article/364495.

2. Чуваков О.А. «Диверсія і тероризм як суміжні злочини», веб-ресурс URL: http://dspace.onu.edu.ua:8080/handle/123456789/7975.

3. 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).

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 C2 до C4ISR: що ховається за цими абревіатурами», веб-ресурс 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. 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).

8. 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, веб-ресурс URL: https://mvs.gov.ua/uk/press-center/news/rozvitok-cifrovoyi-infrastrukturi-ta-stvorennya-cifrovix-servisiv-dlya-gromadyan-prioritet-programi-informatizaciyi-sistemi-mvs.

9. 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).

10. 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).

Горб В. В.,
співробітник Служби безпеки України (м. Одеса),
полковник