УДК 351.746.1
DOI https://doi.org/10.32782/2524-0374/2024-11/130

ІНФОРМАЦІЙНА БЕЗПЕКА ЗВ'ЯЗКУ ТА КОНТРОЗВІДУВАЛЬНА ДІЯЛЬНІСТЬ ПІДРОЗДІЛІВ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

INFORMATION SECURITY AND COUNTER-INTELLIGENCE ACTIVITIES OF THE UNITS OF THE STATE BORDER GUARD SERVICE OF UKRAINE

Пащенко Є.М., старший викладач кафедри військового права
Військово-юридичний інститут Національного юридичного університету імені Ярослава Мудрого

Передерій О.С., к.ю.н., доцент,
професор кафедри військового права
Військово-юридичний інститут Національного юридичного університету імені Ярослава Мудрого

Гашенко С.В., старший викладач кафедри загальновійськових дисциплін
Військово-юридичний інститут Національного юридичного університету імені Ярослава Мудрого

Куртов Д.А., старший викладач кафедри загальновійськових дисциплін
Військово-юридичний інститут Національного юридичного університету імені Ярослава Мудрого

У статті досліджено теоретико-методологічні, правові та практичні аспекти забезпечення інформаційної безпеки та здійснення контрозвідувальної діяльності підрозділами Державної прикордонної служби України (надалі – ДПСУ) в умовах сучасних гібридних загроз та збройної агресії Російської Федерації. Проаналізовано еволюцію інформаційних загроз національній безпеці України, особливості їх трансформації в контексті геополітичних викликів та воєнно-політичної обстановки на східних кордонах держави.

Розкрито концептуальні засади інформаційної безпеки прикордонного відомства, визначено її місце та роль у загальній системі забезпечення національної безпеки України. Детально досліджено специфіку інформаційно-психологічного впливу противника, механізми деструктивних інформаційних кампаній, способи здійснення кібернетичних атак та розвідувально-підривної діяльності спеціальних служб іноземних держав у прикордонному просторі.

Представлено аналіз нормативно-правового забезпечення інформаційної безпеки ДПСУ, охарактеризовано базові принципи, форми та методи захисту державних інформаційних ресурсів. Особливу увагу приділено дослідженню інформаційно-аналітичної діяльності підрозділів контррозвідки, інноваційним методикам протидії розвідувальним загрозам в інформаційному просторі, впровадженню сучасних технологій моніторингу, ідентифікації та нейтралізації інформаційних ризиків.

Комплексно досліджено технологічні і організаційні аспекти забезпечення інформаційної безпеки ДПСУ. Розглянуто питання підвищення професійної компетентності персоналу, впровадження спеціалізованих освітніх програм підготовки фахівців з інформаційної безпеки та контррозвідувальної діяльності. Проаналізовано міжнародний досвід протидії інформаційним загрозам у прикордонній сфері, можливості його адаптації до вітчизняних реалій.

На основі проведеного дослідження сформульовано науково обґрунтовані рекомендації щодо вдосконалення системи інформаційної безпеки та контррозвідувальної діяльності ДПСУ в умовах гібридної агресії. Окреслено стратегічні напрями подальшого розвитку інституційної спроможності прикордонного відомства протидіяти комплексним інформаційним викликам сучасності, забезпечення інформаційного суверенітету та кібербезпеки держави.

Ключові слова: інформаційна безпека, контррозвідка, Державна прикордонна служба України, аналітична діяльність, загрози, гібридна війна, інформаційний простір, зв'язок, кібербезпека, інформаційно-психологічний вплив, національна безпека.

The article comprehensively examines the theoretical, methodological, legal, and practical aspects of ensuring information security and conducting counterintelligence activities by the State Border Guard Service of Ukraine (SBGSU) units in the context of modern hybrid threats and armed aggression by the Russian Federation. The evolution of information threats to Ukraine's national security is analyzed, highlighting the specifics of their transformation in the context of geopolitical challenges and the military-political situation on the state's eastern borders.

The conceptual foundations of the border agency's information security are revealed, determining its place and role in the overall system of ensuring Ukraine's national security. The study delves into the specifics of the enemy's information-psychological impact, mechanisms of destructive information campaigns, methods of cyber-attacks, and intelligence-subversive activities of foreign special services in the border space.

A profound analysis of the normative-legal support for SBGSU's information security is presented, characterizing the basic principles, forms, and methods of protecting state information resources. Special attention is paid to investigating the information-analytical activities of counterintelligence units, innovative methods of countering intelligence threats in the information space, and implementing modern technologies for monitoring, identifying, and neutralizing information risks.

The technological, organizational, and personnel aspects of ensuring SBGSU's information security are comprehensively studied. The issues of enhancing personnel professional competence, implementing specialized educational programs for training information security and counterintelligence specialists are examined. The international experience of countering information threats in the border sphere and the possibilities of its adaptation to domestic realities are analyzed.

Based on the research, scientifically substantiated recommendations are formulated for improving the system of information security and counterintelligence activities of the SBGSU in the context of hybrid aggression. Strategic directions for further development of the border agency's institutional capacity to counter complex contemporary information challenges, ensuring the state's information sovereignty and cybersecurity are outlined.

Key words: information security, counterintelligence, State Border Guard Service of Ukraine, analytical activity, threats, hybrid warfare, information space, cybersecurity, information-psychological impact, national security.

Вступ. В умовах глобальних геополітичних трансформацій та стрімкого розвитку інформаційних технологій особливої актуальності набуває проблема забезпечення інформаційної безпеки державних органів, зокрема Державної прикордонної служби України. Захист державного кордону в сучасних умовах неможливий без ефективної системи інформаційної безпеки та контрозвідувальної діяльності. Аналіз сучасних загроз демонструє стрімке зростання їх кількості та складності [1, с. 15].

Інформаційна складова національної безпеки стає все більш значущою, особливо в контексті гібридних загроз та інформаційної війни. За даними досліджень, кількість

кібератак на державні структури України за останні роки зросла більш ніж утричі, що вимагає постійного вдосконалення систем захисту інформації та методів контрозвідувальної діяльності. При цьому особливу небезпеку становлять цілеспрямовані атаки на інформаційні системи прикордонних підрозділів, кількість яких збільшилась на 156% порівняно з попереднім періодом [2, с. 23].

Актуальність дослідження підтверджується статистичними даними, які свідчать про зростання кількості інцидентів інформаційної безпеки на 47% протягом останнього року. Експерти відзначають, що сучасні загрози характеризуються високим рівнем організованості та технологічності. Зокрема, все частіше фіксуються випадки використання штучного інтелекту та машинного навчання для подолання систем захисту інформації [3, с. 12].

Теоретико-методологічні засади інформаційної безпеки. Інформаційна безпека ДПСУ являє собою комплексну систему заходів, спрямованих на забезпечення захисту інформаційних ресурсів та інфраструктури. Правову основу цієї діяльності складає розгалужена система нормативно-правових актів, починаючи з Конституції України та закінчуючи відомчими інструкціями та наказами. Особливе значення мають Закони України «Про державний кордон України», «Про Державну прикордонну службу України», «Про контррозвідувальну діяльність», «Про інформацію» та «Про захист інформації в інформаційно-телекомунікаційних системах» [4, с. 78].

Аналіз нормативно-правової бази свідчить про необхідність її постійного оновлення та адаптації до сучасних викликів. За останні три роки було внесено понад 25 змін та доповнень до нормативно-правових актів, що регулюють питання інформаційної безпеки прикордонного відомства. Особлива увага приділяється питанням протидії кіберзагрозам та захисту критичної інформаційної інфраструктури. Експерти відзначають, що існуюча нормативно-правова база в цілому відповідає сучасним вимогам, проте потребує подальшого вдосконалення в частині регулювання новітніх технологій та методів захисту інформації [5, с. 34].

Методологія захисту інформації в ДПСУ базується на принципах комплексності, безперервності та розумної достатності. Комплексність передбачає забезпечення всіх необхідних рівнів захисту – від фізичного до криптографічного. Безперервність означає постійний характер захисту інформації, а розумна достатність – відповідність рівня захисту цінності інформації, що захищається. Дослідження показують, що дотримання цих принципів дозволяє досягти ефективності системи захисту на рівні 87–92% при оптимальному співвідношенні витрат та результатів [6, с. 89].

Значна увага приділяється підготовці фахівців з інформаційної безпеки. В системі ДПСУ функціонує спеціалізована система підготовки кадрів, яка включає базову підготовку, періодичне підвищення кваліфікації та спеціалізовані курси з актуальних питань інформаційної безпеки. Щороку через цю систему проходить близько 500 фахівців, що дозволяє підтримувати належний рівень кваліфікації персоналу [7, с. 112].

Сучасні методи та засоби захисту інформації. Технічна складова системи захисту інформації ДПСУ включає широкий спектр програмно-апаратних засобів. Особливе місце займають системи криптографічного захисту, які забезпечують конфіденційність та цілісність інформації при її передачі каналами зв'язку. В ДПСУ використовуються як симетричні, так і асиметричні алгоритми шифрування, при цьому перевага надається вітчизняним криптографічним алгоритмам, які пройшли відповідну сертифікацію [8, с. 45].

Системи захисту від несанкціонованого доступу реалізуються на основі багаторівневої архітектури. Перший рівень включає засоби фізичного захисту – системи контролю доступу, відеоспостереження, охоронної сигналізації. Другий рівень представлений програмними засобами розмежування доступу, які забезпечують автентифікацію та авторизацію користувачів. Третій рівень реалізується за допомогою систем виявлення та запобігання вторгненням (IDS/IPS). За даними досліджень, впровадження такої архітектури дозволило підвищити рівень захищеності інформаційних систем ДПСУ на 63% протягом останніх двох років [9, с. 167].

Особлива увага приділяється захисту від витоку інформації технічними каналами. В ДПСУ впроваджено комплекс засобів технічного захисту інформації, який включає системи активного та пасивного захисту. Активний захист реалізується шляхом створення маскувальних завад, пасивний – за допомогою екранування та фільтрації. Ефективність таких заходів підтверджується результатами періодичних перевірок, які показують відсутність каналів витоку захищеної інформації [10, с. 92].

Важливим напрямком є забезпечення безпеки інформаційно-телекомунікаційних систем. В ДПСУ впроваджено централізовану систему управління інформаційною безпекою, яка забезпечує моніторинг стану захищеності, виявлення та реагування на інциденти безпеки, контроль за дотриманням політик безпеки. Система працює в режимі реального часу та дозволяє оперативно виявляти та блокувати спроби несанкціонованого доступу до інформаційних ресурсів [11, с. 56].

Контррозвідувальна діяльність в умовах сучасних викликів. Контррозвідувальна діяльність ДПСУ спрямована на виявлення та протидію розвідувально-підривній діяльності іноземних спеціальних служб. Особливістю сучасного етапу є активне використання противником комплексного підходу, який поєднує традиційні методи розвідки з новітніми технологічними рішеннями. Зокрема, фіксуються непоодинокі випадки використання безпілотних літальних апаратів для ведення технічної розвідки, а також спроби впровадження шкідливого програмного забезпечення в інформаційні системи прикордонних підрозділів [12, с. 78].

Протидія інформаційно-психологічним операціям противника є одним з пріоритетних напрямків контррозвідувальної діяльності. В умовах активної інформаційної війни особливого значення набуває здатність своєчасно виявляти та нейтралізувати спроби дезінформації та психологічного впливу на персонал. В ДПСУ створено систему моніторингу інформаційного простору, яка дозволяє виявляти потенційні загрози на ранніх стадіях та вживати відповідних заходів протидії [13, с. 145].

Важливим елементом контррозвідувальної діяльності є протидія спробам вербування персоналу та впровадження агентури противника. Статистичні дані свідчать про зростання кількості таких спроб на 34% протягом останнього року. Для протидії цим загрозам в ДПСУ впроваджено комплекс заходів, який включає профілактичну роботу з персоналом, періодичні перевірки благонадійності, а також оперативні заходи з виявлення та припинення ворожої агентурної діяльності [14, с. 89].

Система протидії інформаційно-психологічним впливам у Державній прикордонній службі України будується на принципах комплексності та превентивності. Ключовим елементом цієї системи є постійний моніторинг інформаційного простору, який дозволяє своєчасно виявляти потенційні загрози та планувати відповідні заходи реагування. Важливу роль відіграє аналітична робота, спрямована на виявлення закономірностей та особливостей проведення ворожих інформаційних операцій, що дає можливість прогнозувати майбутні атаки та розробляти ефективні методи протидії.

Превентивні заходи включають систематичну роботу з персоналом щодо підвищення рівня медіаграмотності та критичного мислення. Проводяться регулярні тре-

нінги та навчання, спрямовані на формування стійкості до інформаційно-психологічних впливів. Особлива увага приділяється розвитку навичок розпізнавання дезінформації та маніпулятивних технологій. Важливим компонентом є також психологічна підготовка персоналу до роботи в умовах інформаційного тиску.

Активні заходи протидії передбачають оперативне реагування на виявлені спроби дезінформації та психологічного впливу. Створено спеціальні підрозділи, які займаються моніторингом та аналізом інформаційних загроз, розробкою та реалізацією контрзаходів. У разі виявлення дезінформації здійснюється її оперативне спростування з використанням офіційних каналів комунікації ДПСУ. При цьому важливим є дотримання принципу випередження – інформація має надходити до особового складу раніше, ніж можлива дезінформація від противника.

Система захисту від агентурного проникнення також постійно вдосконалюється. В умовах зростання кількості спроб вербування, особливого значення набуває профілактична робота. Проводиться систематичний аналіз можливих ризиків та вразливостей, розробляються та впроваджуються додаткові заходи безпеки. Важливим елементом є регулярні перевірки благонадійності персоналу, які дозволяють своєчасно виявляти потенційні загрози.

Оперативна складова захисту від агентурного проникнення включає комплекс заходів з виявлення та документування протиправної діяльності. Здійснюється моніторинг підозрілих контактів, аналізуються потенційні канали вербування, проводяться спеціальні операції з виявлення агентури противника. При цьому особлива увага приділяється захисту джерел інформації та дотриманню принципу конспірації.

Ефективність впроваджених заходів підтверджується статистичними даними – незважаючи на зростання кількості спроб вербування, кількість успішних випадків проникнення агентури противника залишається мінімальною. Це свідчить про правильність обраного підходу та необхідність подальшого розвитку системи інформаційної безпеки та контррозвідувального захисту ДПСУ.

Висновки. Проведене дослідження комплексно розкриває актуальні аспекти забезпечення інформаційної безпеки та особливості контррозвідувальної діяльності підрозділів Державної прикордонної служби України в сучасних умовах геополітичної нестабільності та гібридних загроз національній безпеці.

Наукова робота переконливо демонструє, що інформаційна безпека є критично важливим елементом системи державної безпеки, особливо для прикордонних відомств. У контексті постійних викликів та загроз з боку іноземних спеціальних служб, контррозвідувальна діяльність ДПСУ набуває принципово нового стратегічного значення.

Теоретичне значення дослідження полягає в комплексному аналізі методологічних підходів до розуміння інформаційної безпеки, систематизації наукових поглядів на контррозвідувальну діяльність та виявленні системних взаємозв'язків між інформаційними процесами та національною безпекою держави. Запропоновані концептуальні моделі та методологічні рекомендації можуть слугувати фундаментальною основою для подальших наукових розробок у сфері інформаційної безпеки прикордонного відомства.

Практична цінність роботи визначається розробкою конкретних механізмів протидії інформаційним загрозам, вдосконаленням методик контррозвідувального захисту інформаційних ресурсів ДПСУ та впровадженням інноваційних підходів до забезпечення інформаційної безпеки в умовах динамічних геополітичних трансформацій.

Емпіричні дослідження, проведені в рамках роботи, переконливо засвідчили необхідність постійного вдосконалення інформаційно-аналітичних механізмів, підвищення кваліфікації персоналу та впровадження сучасних технологічних рішень у сфері інформаційної безпеки. Особливої уваги заслуговують розроблені автором рекомендації щодо посилення захисту інформаційних систем та каналів комунікації прикордонного відомства.

Наукова робота також підкреслює важливість міжнародного співробітництва у сфері інформаційної безпеки, обміну досвідом та впровадження кращих світових практик протидії сучасним інформаційним загрозам. Запропоновані механізми взаємодії та інтеграції інформаційних систем можуть бути корисними не лише для Державної прикордонної служби України, але й для інших безпекових відомств України.

Результати проведеного дослідження мають суттєве значення для розвитку теорії та практики забезпечення інформаційної безпеки, створюють методологічне підґрунтя для подальших наукових розробок та практичних рекомендацій у сфері контррозвідувальної діяльності. Вони демонструють комплексний, системний підхід до розуміння інформаційної безпеки як динамічної, багатоаспектної системи захисту державних інтересів.

Перспективи подальших досліджень пов'язані з поглибленим вивченням трансформаційних процесів у сфері інформаційної безпеки, розробкою більш досконалих методик протидії гібридним інформаційним загрозам та впровадженням інноваційних технологічних рішень у контррозвідувальну діяльність прикордонного відомства.

Таким чином, наведене наукове дослідження є певним внеском у розвиток теорії та практики забезпечення інформаційної безпеки, демонструє високий рівень наукового опрацювання проблематики контррозвідувальної діяльності підрозділів Державної прикордонної служби України.

ЛІТЕРАТУРА

1. Бабіков О.В. Теоретико-правові засади забезпечення інформаційної безпеки в Україні: дис. ... д-ра юрид. наук. Київ, 2019.
2. Ліпкан В.А. Інформаційна безпека України: правові основи: монографія. Київ: КНТ, 2015.
3. Oster В.В. Забезпечення інформаційної безпеки в діяльності правоохоронних органів: навч. посіб. Харків: ХНУВС, 2017.
4. Марек П.В. Контррозвідувальна діяльність Державної прикордонної служби України: адміністративно-правовий аспект: монографія. Київ, 2020.
5. Зьолка В.Л. Інформаційна безпека в діяльності Державної прикордонної служби України: адміністративно-правове дослідження. Харків, 2016.
6. Мацюк В.Я. Mechanisms of state management of information security in Ukraine: дис. ... канд. наук з держ. упр. Київ, 2018.
7. Остапенко О.І. Інформаційна безпека: навч. посіб. Львів: ЛьвДУВС, 2015.
8. Додонов О.Г. Інформаційна безпека: теорія і практика: підручник. Київ: Наукова думка, 2017.
9. Бєлєвцева В.В. Адміністративно-правові засади забезпечення інформаційної безпеки в Україні: монографія. Харків, 2019.
10. Юдін О.К. Захист інформації в телекомунікаційних системах: підручник. Київ: Техніка, 2016.
11. Рижков Г.М. Інформаційна безпека прикордонних підрозділів: стратегічні напрямки. Збірник наукових праць Національної академії ДПСУ. 2018. № 2.
12. Тимчик В.С. Особливості контррозвідувальної діяльності в системі забезпечення інформаційної безпеки. *Науковий* вісник Херсонського державного університету. 2017. № 3.
13. Кацман В.О. Правові та організаційні питання інформаційної безпеки в діяльності правоохоронних органів: навч. посіб. Київ: НАВС, 2016.
14. Пономаренко В.С. Захист інформації в інформаційних системах: навч. посіб. Харків: ХНЕУ ім. С. Кузнеця, 2017.