УДК 343.9:342.72(477)
DOI https://doi.org/10.32782/2524-0374/2025-2/26

ВИДИ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У ДІЯЛЬНОСТІ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

TYPES OF INFORMATION WITH RESTRICTED ACCESS IN THE ACTIVITIES OF THE STATE BORDER GUARD SERVICE OF UKRAINE

Міняйлук В.В., ад'юнкт відділення ад'юнктури і докторантури
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

Кузьмич М.М., заступник начальника відділу повсякденної діяльності
Національна академія Державної прикордонної служби України імені Богдана Хмельницького

В умовах посилюваних загроз інформаційній безпеці державних органів, зокрема Державної прикордонної служби України (далі – Держприкордонслужба), актуальність дослідження нормативно-правового регулювання інформації з обмеженим доступом набуває особливого значення. Сучасні виклики, пов'язані з гібридними загрозами, кібератаками та витоками конфіденційної інформації, вимагають удосконалення механізмів правового захисту даних, що мають стратегічне значення для прикордонної безпеки та державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз.

Мета статті – дослідити нормативно-правову базу регулювання інформації з обмеженим доступом у Держприкордонслужбі, класифікувати основні види такої інформації та визначити основні загрози інформаційній безпеці в сучасних умовах.

У дослідженні застосовано методи аналізу нормативно-правових актів, порівняльно-правовий метод для характеристики вітчизняного досвіду регулювання інформації з обмеженим доступом, системний підхід для визначення класифікації відомостей та методи прогнозування для оцінювання потенційних загроз інформаційній безпеці Держприкордонслужби.

Аналіз чинного законодавства показав, що регулювання інформації з обмеженим доступом у Держприкордонслужбі базується на таких нормативних актах, як наказ Адміністрації Держприкордонслужби № 501 та наказ Служби безпеки України № 383, які визначають категорії інформації, порядок її обробки та захисту. Здійснена класифікація дозволила виокремити основні групи інформації за рівнем доступу, характером змісту та способом захисту. Дослідження виявило основні загрози інформаційній безпеці, серед яких навмисне та ненавмисне розголошення, кібератаки, дезінформація та технічні загрози, що можуть вплинути на функціонування Держприкордонслужби.

Забезпечення інформаційної безпеки в діяльності Держприкордонслужби є важливим елементом національної безпеки України. Ефективна нормативно-правова база, чітке розмежування рівнів доступу до інформації та впровадження сучасних механізмів захисту дозволяють мінімізувати ризики витоку даних та протидіяти інформаційним загрозам.

Ключові слова: правовий захист, гібридні загрози, кібератака, територіальна цілісність, інформація з обмеженим доступом, службова інформація, державна таємниця.

In the context of growing threats to the information security of state bodies, in particular, the State Border Guard Service of Ukraine (hereinafter – the State Border Guard Service), the relevance of studying the legal regulation of restricted information is of particular importance. Modern challenges related to hybrid threats, cyberattacks and confidential information leaks require improvement of the mechanisms of legal protection of data of strategic importance for border security and state sovereignty, territorial integrity, democratic constitutional order and other national interests of Ukraine from real and potential threats.

The purpose of the article is to study the legal framework for regulating restricted information in the State Border Guard Service, to classify the main types of such information and to identify the main threats to information security in the current environment.

The study uses the methods of analysis of regulatory legal acts, the comparative legal method to characterize the national experience of regulating restricted information, a systematic approach to determine the classification of information, and forecasting methods to assess potential threats to the information security of the State Border Guard Service.

The analysis of the current legislation showed that the regulation of restricted information in the State Border Guard Service is based on such regulations as Order of the Administration of the State Border Guard Service № 501 and Order of the Security Service of Ukraine № 383, which define the categories of information, the procedure for its processing and protection. The classification made it possible to distinguish the main groups of information by the level of access, nature of content, and method of protection. The study identified the main threats to information security, including intentional and unintentional disclosure, cyberattacks, disinformation and technical threats that could affect the functioning of the State Border Guard Service.

Ensuring information security in the activities of the SBGS is an important element of Ukraine's national security. An effective regulatory framework, clear delineation of the levels of access to information and implementation of modern protection mechanisms allow minimizing the risks of data leakage and countering information threats.

Key words: legal protection, hybrid threats, cyberattack, territorial integrity, restricted information, proprietary information, state secret.

Сучасні виклики у сфері національної безпеки та захисту державного кордону України зумовлюють необхідність удосконалення системи збереження та використання інформації з обмеженим доступом. Державна прикордонна служба України виконує важливу роль у забезпеченні територіальної цілісності держави, протидії незаконній міграції, контрабанді та іншим загрозам, що потребують ефективного управління інформаційними потоками.

Одним із важливих аспектів функціонування Держприкордонслужби є використання різних видів інформації з обмеженим доступом, зокрема службової, конфіденційної та державної таємниці. Однак у сучасних умовах спостерігаються виклики щодо захисту такої інформації, зокрема загрози кібербезпеці, витоки даних, а також нормативно-правові колізії у сфері інформаційного захисту.

Попри наявність законодавчого регулювання та впровадження сучасних технологій захисту інформації, існує необхідність у поглибленому дослідженні видів інформації з обмеженим доступом у діяльності Держприкордонслужби. Це дозволить визначити недоліки чинної системи інформаційної безпеки та сформулювати рекомендації щодо її вдосконалення.

Проблематика інформації з обмеженим доступом у сфері національної безпеки, зокрема в діяльності Держприкордонслужби, є предметом наукового та практичного інтересу серед дослідників у галузях права, інформаційної безпеки та державного управління.

У сучасних наукових розвідках значна увага приділяється правовому регулюванню використання інформації з обмеженим доступом. Зокрема, в роботах І. П. Кушнір [1; 2] аналізується законодавча база України щодо охорони державної таємниці, зокрема її відповідність міжнародним стандартам. Авторка наголошує, що, попри чітко визначені правові норми, на практиці існують труднощі з їх імплементацією в контексті сучасних кіберзагроз та можливих витоків інформації.

Науковці О. М. Сибіга [3] та С. Г. Зицик [4] фокусуються на питаннях ефективності заходів безпеки в Держприкордонслужбі щодо захисту службової інформації. Висновки авторів свідчать, що, хоча існують певні протоколи щодо захисту інформації, їх дотримання ускладнене через застарілі технічні засоби та недостатній рівень цифрової грамотності персоналу. Подібні висновки зроблено й у праці А. І. Марущака та Н. О. Кудрявцевої [5], які досліджують механізми протидії інформаційним загрозам в умовах гібридної війни. Автори зазначають, що державні органи потребують оновлення підходів до обробки й зберігання інформації, а також удосконалення механізмів контролю доступу.

Окремі автори зосереджуються на міжнародному досвіді у сфері захисту інформації. Так, О. Б. Фаріон [6] аналізує практики НАТО та ЄС щодо класифікації інформації з обмеженим доступом і вказує на можливість адаптації цих підходів в Україні. Автор наголошує на важливості інтеграції передових технологій шифрування та впровадження єдиної системи доступу для органів сектору безпеки.

У дослідженнях Д. А. Купрієнка [7] та І. В. Кукіна [8] розглядаються соціально-психологічні аспекти використання конфіденційної інформації в правоохоронних структурах. Автори наголошують, що ризики витоків інформації часто пов'язані не лише з технічними недоліками систем захисту, а й з людським фактором – неналежним дотриманням протоколів секретності та недостатнім рівнем мотивації персоналу щодо збереження державної таємниці.

Попри значний науковий інтерес до проблематики інформації з обмеженим доступом, залишається низка нерозв'язаних питань. Зокрема, недостатньо висвітлено особливості класифікації інформації у Держприкордонслужбі залежно від специфіки оперативної діяльності, рівня загроз та сучасних технологічних викликів. Також потребує додаткової уваги комплексний аналіз правових та технічних механізмів захисту інформації в умовах реформування сектору безпеки і оборони України.

Ця стаття спрямована на заповнення цих наукових прогалин шляхом детального аналізу видів інформації з обмеженим доступом у діяльності Держприкордонслужби, ідентифікації основних загроз інформаційній безпеці та розробки рекомендацій щодо вдосконалення механізмів її захисту.

Мета статті – здійснити комплексний аналіз видів інформації з обмеженим доступом у діяльності Державної прикордонної служби України, визначити основні загрози інформаційній безпеці.

Для досягнення поставленої мети необхідно виконати такі завдання:

1) проаналізувати нормативно-правову базу, що регулює використання інформації з обмеженим доступом у Держприкордонслужбі;

2) класифікувати види інформації з обмеженим доступом у діяльності Держприкордонслужбі та визначити їхні особливості;

3) дослідити основні загрози інформаційній безпеці в умовах сучасних викликів.

Наукова думка, враховуючи наявне правове регулювання суспільних правовідносин у певній сфері, постійно розвивається, виявляючи нові прогалини в чинних нормах права. Одним із питань, що становить предмет дискусій у науковому середовищі вже тривалий час, є визначення поняття «інформація з обмеженим доступом». Попри важливість цього поняття для правозастосовної практики та його широке використання в законодавстві, чітке та універсальне доктринальне визначення цієї категорії досі відсутнє. Як зазначають В. Ліпкан та Л. Капінус, навіть у спеціалізованих працях, що присвячені інформаційному праву, аналіз цього поняття є недостатнім [9, с. 46].

Порівняння основних визначень поняття «інформація з обмеженим доступом» представлено в таблиці 1.

Усі автори розглядають інформацію з обмеженим доступом як категорію, доступ до якої обмежується відповідно до законодавчих норм або волі власника. Однак Д. В. Коц зосереджується на фізичних носіях інформації, В. Ліпкан і Л. Капінус – на персональних даних, А. І. Марущак – на розмежуванні конфіденційної та таємної інформації, тоді як В. Ю. Баскаков пропонує структурований підхід із чітким розподілом за видами. Дослідження А. І. Марущака найбільше фокусується на нормативно-правових обмеженнях доступу до інформації, що наближає його підхід до положень чинного законодавства. Водночас В. Ю. Баскаков робить спробу розробки комплексної моделі правового регулювання, що передбачає врахування не лише законодавчих норм, але й механізмів їх реалізації.

Аналіз наведених наукових підходів свідчить про наявність диспропорції у визначеннях поняття «інформація з обмеженим доступом» на теоретичному рівні, що вказує на необхідність уніфікації та систематизації цього поняття. У зв'язку з цим постає важливе питання щодо відповідності чинного законодавства національним та міжнародним стандартам правового регулювання доступу до інформації.

Правове регулювання інформації з обмеженим доступом в Україні базується на конституційних та законодавчих нормах, які визначають загальні принципи доступу до інформації, її класифікацію та обмеження. Конституція України, зокрема статті 17, 31, 32, 34, 50, 92, встановлює основи інформаційної політики держави, визначаючи, які відомості можуть бути обмежені в доступі, які є відкри-

Таблиця 1

Дефініції поняття «інформація з обмеженим доступом» (складено за даними [9, с. 46; 10, с. 109; 11, с. 48; 12])

Автор	Визначення інформації з обмеженим доступом	Важливі аспекти
Д. В. Коц	Відомості або дані, які можуть зберігатися на матеріальних носіях або в електронному вигляді, доступ до яких обмежений власником або державою на законних підставах	Враховує різні носії інформації
В. Ліпкан, Л. Капінус	Інформація про фізичну особу, яка не підлягає розголошенню та доступ до якої обмежено самою особою чи юридичною особою	Основний акцент на персональних даних
А. І. Марущак	Відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України	Охоплює конфіденційну та таємну інформацію
В. Ю. Баскаков	Інформація, що підлягає правовому регулюванню з урахуванням її видів, доступу до неї та режимів використання	Пропонує консолідований підхід до регулювання

тими, а також які сфери потребують додаткового правового врегулювання на рівні законів [13].

Одним з основних законодавчих актів, що регламентує інформаційні відносини, є Закон України «Про інформацію» (від 02.10.1992 № 2657-XII). Його положення формують підхід до класифікації інформації залежно від доступу. Відповідно до статті 20 зазначеного Закону України, інформація поділяється на відкриту та інформацію з обмеженим доступом [14]. Остання, відповідно до ст. 21 Закону України «Про інформацію», поділяється на конфіденційну, таємну та службову інформацію.

Важливо зазначити, що законодавство не пропонує єдиного загальноприйнятого визначення поняття «інформація з обмеженим доступом», а лише класифікує її підвиди. З огляду на це, для всебічного аналізу цього поняття доцільно розглянути визначення термінів «інформація», «конфіденційна інформація», «таємна інформація» та «службова інформація».

У статті 1 Закону України «Про інформацію» поняття «інформація» визначено як будь-які відомості або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [14].

Конфіденційна інформація охоплює дані про фізичну особу, а також інші відомості, доступ до яких обмежується власником – фізичною або юридичною особою, за винятком суб'єктів владних повноважень. Окрім цього, у спеціальному законодавстві містяться додаткові визначення конфіденційної інформації, зокрема в контексті статистичних даних.

Таємна інформація регулюється Законом України «Про доступ до публічної інформації» (від 13.01.2011 № 2939-VI), відповідно до якого це відомості, розголошення яких може завдати шкоди особі, суспільству або державі [15]. До таких відомостей належать державна, професійна, банківська таємниці, а також таємниця досудового розслідування та інші категорії, визначені законодавством.

Поняття «службова інформація» також не має конкретного визначення в законодавчих актах, проте її зміст можна встановити з аналізу нормативних положень. До неї належать документи органів влади, що містять внутрішньовідомчу кореспонденцію, доповідні записки, аналітичні матеріали, які стосуються формування політики установи, здійснення наглядових та контрольних функцій, ухвалення рішень. Окрім того, службовою інформацією можуть бути відомості, отримані під час оперативно-розшукової діяльності, у сфері оборони, які не віднесені до державної таємниці.

Правове регулювання інформації з обмеженим доступом в Україні ґрунтується на системному підході, що поєднує конституційні норми, спеціальні закони та підзаконні акти. Визначення та регулювання кожної категорії інформації мають свої особливості, що свідчить про необхідність детального аналізу нормативно-правової бази та її подальшого вдосконалення відповідно до сучасних викликів інформаційної безпеки.

Правове регулювання інформації з обмеженим доступом у Держприкордонслужбі потребує окремого розгляду. Здійснюється воно на основі сукупності нормативно-правових актів, що визначають порядок поводження з такою інформацією, її захист, обмеження доступу до неї та механізми контролю за її обігом.

Одним з основних нормативних актів є наказ Адміністрації Держприкордонслужби від 07.07.2011 № 501, який визначає категорії службової інформації, що підлягають обмеженню доступу у сфері охорони державного кордону України [16]. Цей документ містить чіткий перелік даних, які можуть мати обмежений доступ із метою забезпечення прикордонної безпеки. Така інформація охоплює не лише технічні, але й організаційні та стратегічні відомості, що можуть стати підставою для порушення національної безпеки в разі неналежного доступу.

Додатково, важливим є наказ Служби безпеки України від 23.12.2020 № 383, який регулює відомості, що становлять державну таємницю, зокрема питання, пов'язані з прикордонною безпекою та захистом інформації, що здійснюється в межах діяльності Держприкордонслужби [17]. Цей наказ забезпечує захист чутливої інформації, яка може мати стратегічне значення для державної безпеки України, що, відповідно, підтверджує важливість створення правового режиму для її охорони.

Важливим аспектом є регулювання інформаційної діяльності в Держприкордонслужби. Законодавство встановлює порядок створення, збору, зберігання, використання, поширення, охорони та захисту інформації з обмеженим доступом, що дозволяє чітко організувати роботу служби. Компетенція посадових осіб у роботі з такою інформацією також чітко визначена, що сприяє ефективному виконанню обов'язків, зокрема в питаннях захисту державної таємниці та інформації, що підлягає обмеженому доступу.

Процедура отримання допуску до інформації з обмеженим доступом у Держприкордонслужби є важливою складовою правового режиму. Вона забезпечує контроль за доступом до критично важливих даних, а також визначає порядок надання доступу до таких відомостей. Окрім того, за порушення встановлених вимог щодо доступу та використання цієї інформації передбачена відповідальність, що передбачає як дисциплінарні, так і адміністративні санкції. Це сприяє дотриманню встановлених норм та гарантує безпеку інформації.

Оскільки інформація з обмеженим доступом може бути різного виду та мати різний рівень важливості, необхідно здійснювати її детальну класифікацію з метою адекватного управління та захисту. Класифікація дозволяє не тільки визначити рівень конфіденційності кожної категорії даних, а й розробити відповідні заходи для захисту цієї інформації в межах діяльності Держприкордонслужби (табл. 2).

Насамперед інформація поділяється на два основних види залежно від рівня доступу: службова інформація та державна таємниця. Службова інформація охоплює дані, які є важливими для щоденної діяльності Держприкордонслужби, зокрема щодо організації прикордонної охорони, оперативної ситуації на кордоні, планів патрулювання та забезпечення правопорядку. Державна таємниця охоплює відомості, які мають надзвичайно важливе значення для національної безпеки, такі як стратегічні плани оборони, розвідка, інформація про терористичні загрози, операції щодо захисту кордону, а також інші дані, що можуть суттєво вплинути на суверенітет держави.

Згідно з критерієм важливості, інформація, що забезпечує прикордонну безпеку, є найбільш чутливою та потребує суворого контролю доступу. Це можуть бути дані про порушення кордону, незаконну міграцію, контрабанду, а також інші дії, що загрожують національній безпеці. Такі дані можуть містити маршрути контрабанди, переміщення нелегальних мігрантів, а також специфічну інформацію, пов'язану з діяльністю організованих злочинних груп чи терористичних осередків. Водночас внутрішньоорганізаційна інформація не має прямого впливу на безпеку країни, але є необхідною для ефективної роботи Держприкордонслужби, зокрема в плануванні та організації робочих процесів, кадрових змін, документообігу тощо.

Особливу роль у класифікації інформації з обмеженим доступом відіграє характер її змісту. Інформація, що стосується загроз національній безпеці, є надзвичайно чутливою та може містити дані про тероризм, шпигунство, диверсії, порушення територіальної цілісності країни, а також про специфічні заходи, що можуть бути вжиті у випадку цих загроз. Важливим аспектом є також інформація про діяльність контрабандистів та нелегальних мігрантів, яка безпосередньо стосується правопорушень на кордоні та вимагає швидкого реагування.

Таблиця 2

Класифікація інформації з обмеженим доступом у діяльності Держприкордонслужби (складено за даними [18, с. 149; 19])

Види інформації	Особливості
За рівнем доступу	
Службова інформація	Інформація, що необхідна для виконання службових обов'язків в межах діяльності Держприкордонслужби. Охоплює оперативні дані та інформацію, що стосується виконання функцій прикордонної служби.
Державна таємниця	Інформація, що має критичне значення для національної безпеки та охорони державного кордону, що підлягає спеціальному захисту, зокрема військові плани, стратегії охорони кордону.
За категорією важливості	
Інформація, що забезпечує прикордонну безпеку	Дані, що стосуються стану охорони державного кордону, ситуації на прикордонних територіях, результатів антитерористичних операцій.
Інформація для внутрішнього користування	Дані, які використовуються виключно в межах Держприкордонслужби для забезпечення внутрішніх процесів, таких як інструкції, звіти та плани.
За характером змісту	
Інформація про загрози національній безпеці	Повідомлення про потенційні чи фактичні загрози на кордоні, включаючи розвіддані, інформацію про диверсійні групи, шляхи незаконного перетину кордону.
Інформація про діяльність контрабандистів та нелегальних мігрантів	Дані про рух контрабанди, маршрути нелегальних мігрантів, прикордонні порушення, що впливають на охорону кордону.
За способом захисту	
Інформація, що підлягає криптографічному захисту	Інформація, що передається через зашифровані канали зв'язку або зберігається в захищених базах даних, наприклад, дані про об'єкти критичної інфраструктури на кордоні.
Інформація з обмеженим доступом на рівні доступу конкретних осіб	Інформація, доступ до якої обмежений для певних осіб або категорій осіб усередині Держприкордонслужби, наприклад, особисті дані працівників, звіти за результатами перевірок, інформація про розміщення та пересування прикордонних сил.
За рівнем конфіденційності	
Конфіденційна інформація	Інформація, що не підлягає розголошенню без відповідних дозволів, зокрема щодо внутрішніх операцій, планів патрулювання чи оперативних даних.
Особливо конфіденційна інформація	Інформація, що може суттєво зашкодити державним інтересам у випадку розголошення, наприклад, дані про стан сил і засобів охорони кордону, військові таємниці.
За територіальним розподілом	
Інформація на рівні прикордонних підрозділів	Дані, що стосуються окремих підрозділів Держприкордонслужби, їхнього розташування, пересування та операцій на прикордонних ділянках.
Інформація на рівні центрального апарату	Загальна інформація, що має стратегічне значення для всіх підрозділів Держприкордонслужби та координації їхньої діяльності загалом.

Інформація з обмеженим доступом вимагає відповідного захисту, що забезпечується різними технічними та організаційними заходами. Для збереження цілісності та конфіденційності даних використовуються засоби криптографічного захисту, які гарантують безпеку передачі та зберігання відомостей через зашифровані канали зв'язку або в захищених інформаційних системах. Крім того, доступ до такої інформації регулюється через систему допуску, що надається лише уповноваженим посадовим особам, що визначаються згідно з їхніми посадовими обов'язками та рівнем допуску.

Інформація з обмеженим доступом також класифікується за рівнем конфіденційності. Конфіденційна інформація охоплює дані, що необхідні для нормального функціонування Держприкордонслужби, але не є критичними для безпеки держави. Водночас особливо конфіденційна інформація має критично високий рівень важливості та містить дані, розголошення яких може значно вплинути на національну безпеку, зокрема інформацію про стратегічні плани оборони, тактику дій прикордонних нарядів або інші відомості, що забезпечують безпеку країни.

Крім того, інформація з обмеженим доступом класифікується за територіальним розподілом. Інформація на рівні прикордонних підрозділів стосується даних, що використовуються безпосередньо на місцях для забезпечення безпеки на окремих ділянках кордону, зокрема щодо розташування прикордонних нарядів, тактики та стратегії їхньої роботи, переміщення підрозділів. Натомість інформація на рівні центрального апарату є більш загальною та містить стратегічні плани, звіти, інформацію для координації дій між різними підрозділами та органами державної влади.

Таким чином, класифікація інформації з обмеженим доступом є важливим інструментом для забезпечення належної охорони державного кордону та ефективного виконання функцій Держприкордонслужби. Вона дозволяє не лише оптимізувати доступ до критично важливих відомостей, але й гарантувати їх належний захист від несанкціонованого доступу чи витоків, що можуть загрожувати безпеці держави. Усі ці категорії й заходи є невід'ємною частиною забезпечення національної безпеки та безперебійного функціонування системи охорони кордону України.

Отже, аналіз нормативно-правової бази продемонстрував, що діяльність Держприкордонслужби у сфері використання інформації з обмеженим доступом регулюється низкою законодавчих та підзаконних актів. Основними серед них є наказ Адміністрації Держприкордонслужби від 07.07.2011 № 501 «Про затвердження Переліку відомостей, що становлять службову інформацію у Державній прикордонній службі України» та наказ Служби безпеки України від 23.12.2020 № 383 «Про затвердження Зводу відомостей, що становлять державну таємницю». Ці документи визначають категорії інформації, порядок

її обробки, збереження, а також відповідальність за порушення режиму секретності.

Класифікація видів інформації з обмеженим доступом у діяльності Держприкордонслужби дозволила виокремити основні категорії відомостей залежно від рівня доступу, важливості, характеру змісту, способу захисту, рівня конфіденційності та територіального розподілу. Інформація поділяється на службову та таку, що становить державну таємницю, з диференціацією за важливістю для прикордонної безпеки. Вона може мати стратегічне (загрозливе для державної безпеки), оперативне (пов'язане з функціонуванням підрозділів) або внутрішньоорганізаційне значення. Кожна категорія інформації має свої особливості захисту, що передбачає використання криптографічних засобів, регламентованого доступу, технічних і організаційних заходів безпеки.

Дослідження основних загроз інформаційній безпеці в умовах сучасних викликів засвідчило, що Держприкордонслужба стикається з широким спектром небезпек, які можуть мати як внутрішнє, так і зовнішнє походження. Основними загрозами є витік інформації через неналежне збереження або навмисне розголошення, кібератаки, дезінформація, спроби незаконного отримання відомостей про прикордонну діяльність, а також технічні ризики, зокрема втручання в електронні системи управління. Важливим чинником залишається ведення інформаційної війни, спрямованої на дискредитацію Держприкордонслужби, викривлення реального стану безпекової ситуації та маніпуляцію громадською думкою.

Подальші дослідження мають бути спрямовані на удосконалення нормативно-правових механізмів захисту інформації з обмеженим доступом у Держприкордонслужбі, зокрема шляхом розробки детальніших регламентів доступу, зберігання та поширення таких відомостей. Важливим напрямом є впровадження сучасних технологій кіберзахисту, зокрема засобів криптографічного шифрування, систем багаторівневої аутентифікації та штучного інтелекту для моніторингу можливих загроз.

ЛІТЕРАТУРА

1. Кушнір І. П. Інформаційні загрози в діяльності державної прикордонної служби України. 2019. *Підприємництво, господарство і право.* Вип. 7. С. 147–150. DOI: https://doi.org/10.32849/2663-5313.2019.7.26
2. Кушнір І., Степанова Ю. Інформаційна безпека держави у прикордонній сфері як об'єкт державної зради. *Національний юридичний журнал: теорія і практика.* 2018. Вип. 4. С. 118–121. URL: http://www.jurnaluljuridic.in.ua/archive/2018/4/part_1/27.pdf (дата звернення: 05.02.2025).
1. Сибіга О. М. Поняття «доступ до інформації» і «право на інформацію» у національному законодавстві та науковій літературі. *Юридичний бюлетень.* 2018. Вип. 8. С. 234–240. URL: http://www.lawbulletin.oduvs.od.ua/archive/2018/8_2018/35.pdf (дата звернення: 05.02.2025).
2. 4. Зицик С. Г. Правове регулювання інформації з обмеженим доступом. *Юридичний науковий електронний журнал.* 2023. Вип. 5. С. 220–223. DOI: https://doi.org/10.32782/2524-0374/2023-5/54
3. 5. Марущак А. І., Кудрявцева Н. О. Доступ до інформації про діяльність Служби безпеки України в контексті протидії дезінформації. *Вісник Харківського національного університету внутрішніх справ.* 2022. Вип. 2. С. 281–291. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2022_2_28 (дата звернення: 05.02.2025).
4. 6. Фаріон О. Б. Інформаційна модель оперативно-розшукової діяльності оперативних підрозділів Державної прикордонної служби України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2020. Вип. 1(68). С. 81–85. DOI: https://doi.org/10.33099/2304-2745/2020-0/81-85
5. 7. Купрієнко Д. А. Окремі прийоми і способи збору конфіденційної та іншої інформації про об'єкти зацікавленості в умовах загострення воєнно-політичної обстановки. *Актуальні питання протидії кіберзлочинності та торгівлі людьми: збірник матеріалів Всеукр. наук.-практ. конф.* (м. Харків, 23 листопада 2018 р.). Харків: ХНУВС, 2018. С. 286–289.
6. 8. Кукін І. В. Методи та інструменти забезпечення інформаційної безпеки особистості у сфері національної безпеки та її прикордонному секторі. *Право та державне управління.* 2020. № 4. С. 233–240. DOI: https://doi.org/10.32840/pdu.2020.4.33
7. 9. Ліпкан В. А., Капінус Л. І. Доступ до інформації з обмеженим доступом: проблеми вироблення уніфікованих дефініцій. *Публічне право*. 2013. Вип. 4. С. 45–53. URL: http://nbuv.gov.ua/UJRN/pp_2013_4_8 (дата звернення: 05.02.2025).
8. 10. Коц Д. В. Теоретико-правові засади інформації з обмеженим доступом. *Вісник НТУУ «КПІ» Політологія. Соціологія. Право.* 2019. Вип. 2(42). С. 107–111. DOI: https://doi.org/10.20535/2308-5053.2019.2(42).194955
9. 11. Баскаков В. Ю. Інформація з обмеженим доступом: аналіз понятійно-термінологічного апарату. *Актуальні проблеми державотворення (Імперативи розвитку юридичної та безпекової науки; №9): матеріали наук.-практ. конф.* (м. Київ, 28 черв. 2011 р.). Київ, 2011. С. 47–49. URL: https://goal-int.org/informaciya-z-obmezhenim-dostupom-analiz-terminologichno-ponyatijnogo-aparatu/ (дата звернення: 05.02.2025).
10. 12. Марущак А. І. Свобода слова та інформація з обмеженим доступом: співвідношення понять. *Бюлетень Мін'юсту України.* 2005. № 6 (44). С. 44–49.
11. 13. Конституція України, прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 05.02.2025).
12. 14. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 05.02.2025).
13. 15. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 05.02.2025).
14. 16. Перелік відомостей, що становлять службову інформацію у Державній прикордонній службі України : наказ Адміністрації Державної прикордонної служби України від 07.07.2011 № 501. URL: https://dpsu.gov.ua/ua/vidi-informaciyi (дата звернення: 05.02.2025).
15. 17. Про затвердження Зводу відомостей, що становлять державну таємницю : наказ СБУ від 23.12.2020 № 383. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#Text (дата звернення: 05.02.2025).
16. 18. Кушнір І. П., Царенко О. М. Правовий режим інформації з обмеженим доступом у діяльності державної прикордонної служби. *Право та державне управління.* 2019. Вип. 3(1). С. 180–185. DOI: https://doi.org/10.32840/pdu.3-1.27
17. 19. Фаріон О., Купрієнко Д., Малюга В. Методичний підхід щодо забезпечення інформаційної безпеки органів Державної прикордонної служби України на каналах інтернет-комунікацій. *Збірник наукових праць національної академії державної прикордонної служби України. Серія: військові та технічні науки.* 2022. Т. 87. № 1–2. С. 169–187. DOI: https://doi.org/10.32453/3.v87i1-2.1088