ПРАВОВІ ЗАСАДИ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

УДК 351.746.1:004.056
DOI https://doi.org/10.32782/ehrlichsjournal-2026-18.10

ОЛЕКСАНДР МЕРЕНИЧ
доктор філософії у галузі права
ORCID: 0000-0002-3837-4724

МИХАЙЛО МЕРЕНИЧ
доктор філософії у галузі права
ORCID: 0009-0004-9377-0879

Анотація. Статтю присвячено дослідженню правових засад діяльності Служби безпеки України (далі – СБУ) у сфері захисту критичної інформаційної інфраструктури. Установлено, що відповідний напрям діяльності СБУ формується на перетині правового регулювання державної безпеки, контррозвідувальної діяльності, кібербезпеки та захисту критичної інфраструктури. Обґрунтовано, що повноваження СБУ у цій сфері мають спеціальний безпековий характер і не повинні ототожнюватися із загальним управлінням системою кіберзахисту. Їхнє основне призначення полягає у виявленні, попередженні та нейтралізації загроз державній безпеці, пов'язаних із кібершпигунством, кібертероризмом, кібердиверсіями та іншими протиправними посяганнями на об'єкти критичної інформаційної інфраструктури.

Проаналізовано положення законів України «Про Службу безпеки України», «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру» та підзаконних нормативно-правових актів. Особливу увагу приділено законодавчим змінам 2025 р., якими уточнено компетенцію СБУ у сфері кібербезпеки та її місце у національній системі реагування на кіберінциденти, кібератаки та кіберзагрози.

Запропоновано розглядати діяльність СБУ щодо захисту критичної інформаційної інфраструктури через сукупність контррозвідувального, превентивного, оперативно-реагувального та координаційного напрямів.

Визначено необхідність подальшого нормативного розмежування повноважень основних суб'єктів національної системи кібербезпеки та вдосконалення механізмів їхньої взаємодії в умовах збройної агресії проти України.

Ключові слова: Служба безпеки України; критична інформаційна інфраструктура; критична інфраструктура; кібербезпека; кіберзахист; державна безпека; кібершпигунство; кібертероризм; кібердиверсія; кіберінцидент.

LEGAL PRINCIPLES OF THE ACTIVITIES OF THE SECURITY SERVICE OF UKRAINE IN THE FIELD OF PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE

UDC 351.746.1:004.056
DOI https://doi.org/10.32782/ehrlichsjournal-2026-18.10

OLEXANDR MERENYCH
Doctor of Philosophy in Law
ORCID: 0000-0002-3837-4724

MYKHAILO MERENYCH
Doctor of Philosophy in Law
ORCID: 0009-0004-9377-0879

Abstract. This scientific article is devoted to the study of the legal principles of the activities of the Security Service of Ukraine (hereinafter referred to as the SBU) in the field of protection of critical information infrastructure. It is established that the relevant direction of the SBU's activities is formed at the intersection of legal regulation of state security, counterintelligence activities, cybersecurity and protection of critical infrastructure. It is substantiated that the powers of the SBU in this area are of a special security nature and should not be identified with the general management of the cyber defense system. Their main purpose is to identify, prevent and neutralize threats to state security related to cyber espionage, cyber terrorism, cyber sabotage and other unlawful encroachments on critical information infrastructure facilities.

The provisions of the laws of Ukraine «On the Security Service of Ukraine», «On National Security of Ukraine», «On the Basic Principles of Ensuring Cybersecurity of Ukraine», «On Critical Infrastructure» and subordinate regulatory legal acts were analyzed. Particular attention was paid to the legislative changes of 2025, which clarified the competence of the SBU in the field of cybersecurity and its place in the national system of response to cyber incidents, cyber attacks and cyber threats.

It is proposed to consider the activities of the SBU in protecting critical information infrastructure through a combination of counterintelligence, preventive, operational response and coordination areas.

The need for further regulatory delimitation of the powers of the main subjects of the national cybersecurity system and improvement of the mechanisms of their interaction in conditions of armed aggression against Ukraine was identified.

Key words: Security Service of Ukraine; critical information infrastructure; critical infrastructure; cybersecurity; cyber defense; state security; cyber espionage; cyber terrorism; cyber sabotage; cyber incident.

Постановка проблеми. Функціонування сучасної держави безпосередньо залежить від стійкості інформаційних, електронних комунікаційних та технологічних систем, які забезпечують роботу енергетики, транспорту, фінансової системи, зв'язку, охорони здоров'я, державного управління та інших життєво важливих сфер. Порушення роботи таких систем здатне спричинити наслідки, що виходять далеко за межі інформаційної безпеки окремого суб'єкта та створюють загрозу державній і національній безпеці.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає критичну інформаційну інфраструктуру як сукупність об'єктів критичної інформаційної інфраструктури, функціонування яких має істотне значення для стійкості відповідних об'єктів критичної інфраструктури [1]. Їхня особливість полягає у тому, що кібератака може не лише призвести до втрати або пошкодження інформації, а й порушити безперервність надання життєво важливих функцій і послуг.

В умовах збройної агресії проти України захист таких об'єктів набуває особливого безпекового значення. Кібератаки дедалі частіше поєднуються з розвідувальною, диверсійною та іншою діяльністю, спрямованою на послаблення спроможності держави. За таких умов одним із ключових суб'єктів протидії відповідним загрозам є Служба безпеки України.

Водночас діяльність СБУ у цій сфері здійснюється поряд із повноваженнями Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України та інших суб'єктів

національної системи кібербезпеки, що зумовлює необхідність чіткого визначення правової природи та меж компетенції СБУ саме у сфері захисту критичної інформаційної інфраструктури.

Окремі аспекти правового регулювання захисту критичної та критичної інформаційної інфраструктури, забезпечення її кібербезпеки та протидії загрозам на відповідних об'єктах досліджували такі вітчизняні науковці, як: М. Ковалів, Р. Скриньковський, Ю. Назар, С. Єсімов, І. Красницький, Х. Кайдрович, С. Князь, Ю. Кемська, О. Герасименко, А. Ковальчук та ін. Наявний науковий доробок сформував належне підґрунтя для аналізу системи захисту критичної інфраструктури та її правового забезпечення. Водночас недостатньо дослідженим залишається саме місце Служби безпеки України у механізмі захисту критичної інформаційної інфраструктури з урахуванням сучасного розмежування повноважень суб'єктів національної системи кібербезпеки та законодавчих змін останніх років.

Метою статті є визначення правових засад та основних напрямів діяльності Служби безпеки України у сфері захисту критичної інформаційної інфраструктури, з'ясування особливостей її компетенції та співвідношення з повноваженнями інших суб'єктів забезпечення кібербезпеки.

Методологічну основу дослідження становлять системний, формально-юридичний, структурно-функціональний та порівняльно-правовий методи, застосовані для аналізу законодавства, визначення змісту повноважень СБУ та їхнього місця у загальній системі захисту критичної інформаційної інфраструктури.

Виклад основного матеріалу. Правове підґрунтя діяльності Служби безпеки України у досліджуваній сфері має комплексний характер. Вихідні положення визначаються Конституцією України та Законом України «Про Службу безпеки України». Відповідно до останнього, СБУ є державним органом спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України. До її завдань належать захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного та оборонного потенціалу, законних інтересів держави від розвідувально-підривної діяльності, а також протидія іншим посяганням, що безпосередньо створюють загрозу життєво важливим інтересам України [2].

Більш предметно місце СБУ у відповідній сфері визначене Законом України «Про національну безпеку України». Так, ст. 19 Закону безпосередньо відносить до діяльності СБУ контррозвідувальний захист кібербезпеки, інформаційної безпеки держави та об'єктів критичної інфраструктури [3]. Таким чином, діяльність СБУ щодо критичної інформаційної інфраструктури має розглядатися передусім у контексті виконання її основної функції – забезпечення державної безпеки.

Велике значення для визначення спеціальних повноважень СБУ має також Закон України «Про основні засади забезпечення кібербезпеки України». Службу безпеки України віднесено до основних суб'єктів національної системи кібербезпеки поряд із Держспецзв'язку, Національною поліцією, Міністерством оборони України, Генеральним штабом Збройних сил України, розвідувальними органами та іншими визначеними законом суб'єктами. При цьому законодавство не встановлює однакової компетенції для всіх зазначених органів. Держспецзв'язку забезпечує формування та реалізацію державної політики у сфері кіберзахисту, здійснює державний контроль, забезпечує функціонування відповідної організаційно-технічної інфраструктури та координує діяльність суб'єктів забезпечення кібербезпеки саме щодо кіберзахисту [1]. Натомість функціональне призначення СБУ зосереджується на загрозах, які мають безпосередній зв'язок із державною безпекою.

Чинна редакція Закону України «Про основні засади забезпечення кібербезпеки України» покладає на СБУ запобігання, виявлення, припинення та розкриття визначених законом кримінальних правопорушень, що вчиняються у кіберпросторі або з його використанням; проведення контррозвідувальних та оперативно-розшукових заходів щодо боротьби з кібертероризмом, кібердиверсіями та кібершпигунством; координацію діяльності суб'єктів забезпечення кібербезпеки у протидії таким загрозам; перевірку готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; розслідування кібератак щодо критичної інформаційної інфраструктури та реагування на кіберзагрози у сфері державної безпеки [1].

Особливого значення набули зміни, внесені Законом України від 27 березня 2025 р. № 4336-IX, якими було оновлено механізм функціонування національної системи кібербезпеки та конкретизовано завдання її основних суб'єктів [4]. Останні зміни є важливими для визначення сучасної моделі

діяльності СБУ, оскільки ще чіткіше розмежовують загальний кіберзахист та безпекову протидію спеціальним видам кіберзагроз.

З огляду на нормативно визначені повноваження, діяльність СБУ у сфері захисту критичної інформаційної інфраструктури доцільно систематизувати за кількома основними напрямами.

Першим є *контррозвідувальний напрям.* Його зміст полягає у виявленні та нейтралізації діяльності іноземних спеціальних служб, пов'язаних із ними структур та інших суб'єктів, які використовують кіберпростір для одержання інформації, порушення роботи критично важливих систем або створення передумов для інших форм підривної діяльності. Саме цей напрям найбільш чітко відмежовує компетенцію СБУ від функцій органів, відповідальних переважно за технічний кіберзахист.

Другим є *превентивний напрям*. Захист критичної інформаційної інфраструктури не може обмежуватися реагуванням на вже реалізовану кібератаку. Законодавство надає СБУ можливість здійснювати заходи, спрямовані на завчасне виявлення загроз, а також негласно перевіряти готовність об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів [1]. Наукове значення превентивного підходу полягає у тому, що об'єктом правового реагування стає не лише завершене протиправне посягання, а й ризик реалізації загрози державній безпеці. У цій частині діяльність СБУ набуває виразно запобіжного характеру і відповідає сучасній ризик-орієнтованій моделі забезпечення безпеки критичної інфраструктури.

Третім є *оперативно-реагувальний напрям*, що охоплює діяльність під час виникнення кіберінцидентів, кібератак та кіберзагроз. Важливими інституційними елементами цього механізму є Ситуаційний центр забезпечення кібербезпеки СБУ та регіональні центри забезпечення кібербезпеки [5]. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури передбачають інформування відповідних структур СБУ про кіберінциденти та кібератаки, що стосуються об'єктів критичної інформаційної інфраструктури [6]. Функціонування такого механізму дає змогу не лише реагувати на конкретний інцидент, а й отримувати інформацію, необхідну для встановлення джерела кібератаки, її можливого зв'язку з діяльністю іноземних спеціальних служб, терористичних або диверсійних структур та оцінювання ширших наслідків для державної безпеки.

Четвертим є *координаційний напрям*. Закон наділяє СБУ спеціальними координаційними повноваженнями щодо протидії кібершпигунству, кібертероризму та кібердиверсіям [1]. При цьому необхідно чітко відрізняти зазначені повноваження від загальної координації діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту, яка належить до компетенції Держспецзв'язку.

Таке розмежування має принципове значення. Використання в законодавстві близьких за змістом категорій «кібербезпека», «кіберзахист», «захист критичної інфраструктури», «протидія кіберзлочинності» не повинно створювати уявлення про взаємозамінність компетенції відповідних державних органів. СБУ не є органом загального технічного адміністрування кіберзахисту критичної інформаційної інфраструктури. Її компетенція повинна визначатися через критерій загрози державній безпеці та спеціальні правові засоби, властиві діяльності органу безпеки. Саме такий підхід дає змогу сформулювати функціональне місце СБУ у досліджуваній системі. Держспецзв'язку забезпечує нормативне, організаційне та технічне функціонування системи кіберзахисту; Національна поліція протидіє кримінально протиправним посяганням у кіберпросторі відповідно до своєї компетенції; СБУ зосереджується на тих кіберзагрозах, які пов'язані з розвідувально-підривною діяльністю, тероризмом, диверсіями, шпигунством та іншими загрозами державній безпеці [1].

Наведене також узгоджується із сучасними напрямами інституційного розвитку СБУ. Так, Стратегією розвитку Служби безпеки України на 2025–2030 рр. серед пріоритетних напрямів визначено контррозвідувальне забезпечення інформаційної безпеки та кібербезпеки держави, а також контррозвідувальне забезпечення критичної інфраструктури [7].

У науковій літературі слушно наголошується, що правове забезпечення кібербезпеки критичної інформаційної інфраструктури потребує системного поєднання правових, організаційних і технічних механізмів [8]. Своєю чергою, О. Герасименко, аналізуючи роль СБУ у протидії загрозам на об'єктах критичної інфраструктури, окремо звертає увагу на терористичні, диверсійні та кібернетичні загрози й необхідність ризик-орієнтованого підходу до їх нейтралізації [9]. Водночас сучасний стан правового регулювання критичної інфраструктури все ще характеризується значною кількістю взаємопов'язаних нормативно-правових актів, що потребують системного узгодження [10].

У зв'язку із цим подальше вдосконалення правових засад діяльності СБУ має здійснюватися не шляхом механічного розширення її компетенції, а через точніше визначення функціональних меж відповідальності. Доцільним є нормативне забезпечення чіткого порядку взаємодії СБУ, Держспецзв'язку, Національної поліції, секторальних органів та операторів критичної інфраструктури залежно від характеру й рівня конкретної кіберзагрози.

Не менш важливим є подальший розвиток системи оперативного обміну інформацією. Своєчасне отримання від оператора критичної інфраструктури відомостей про ознаки кібератаки може мати значення не лише для відновлення роботи системи, а й для виявлення координованої розвідувальної або диверсійної операції. Саме тому інформаційна взаємодія має розглядатися як один із ключових елементів правового механізму превентивного захисту.

Висновки. Проведене дослідження дає підстави визначити діяльність Служби безпеки України у сфері захисту критичної інформаційної інфраструктури як спеціальний напрям забезпечення державної безпеки, що реалізується у межах національних систем кібербезпеки та захисту критичної інфраструктури.

Установлено, що компетенція СБУ у цій сфері охоплює передусім контррозвідувальний, превентивний, оперативно-реагувальний та координаційний напрями. Її визначальною ознакою є спрямованість на протидію кібершпигунству, кібертероризму, кібердиверсіям та іншим посяганням, здатним створити загрозу державній безпеці.

Обґрунтовано необхідність чіткого розмежування діяльності СБУ та інших суб'єктів національної системи кібербезпеки. СБУ не повинна підміняти органи, відповідальні за формування політики, державний контроль і технічне забезпечення кіберзахисту; її спеціальна роль полягає у застосуванні контррозвідувальних та інших передбачених законом засобів реагування на загрози безпекового характеру.

Подальше вдосконалення правового регулювання має бути спрямоване на конкретизацію механізмів міжвідомчої взаємодії, оперативного обміну інформацією та розподілу відповідальності під час виявлення і нейтралізації кібератак на об'єкти критичної інформаційної інфраструктури.

ВИКОРИСТАНІ МАТЕРІАЛИ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

3. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

4. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. *Відомості Верховної Ради України.* 2025. № 35. Ст. 134. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text

5. Ситуаційний центр забезпечення кібербезпеки СБУ. *Служба безпеки України*. URL: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky

6. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518. *Офіційний вісник України*. 2019. № 50. Ст. 1697. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

7. Стратегія розвитку Служби безпеки України на 2025–2030 роки. *Служба безпеки України.* URL: https://ssu.gov.ua/stratehiia-rozvytku-sluzhby-bezpeky-ukrainy-na-20252030-roky

8. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України / М. Ковалів та ін. *Traektoriâ Nauki = Path of Science.* 2021. Vol. 7, № 4. С. 2011–2018. DOI: https://doi.org/10.22178/pos.69-12

9. Герасименко О. М. Ґенеза поняття «критична інфраструктура» у контексті протидії Службою безпеки України загрозам на її об'єктах. *Аналітично-порівняльне правознавство.* 2025. Т. 3, № 4. С. 146–154. DOI: https://doi.org/10.24144/2788-6018.2025.04.3.22

10. Ковальчук А. Т. Система правового регулювання захисту об'єктів критичної інфраструктури в Україні: сучасний стан та напрями вдосконалення. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2025. Т. 5, № 90. С. 172–184. DOI: https://doi.org/10.24144/2307-3322.2025.90.5.21

REFERENCES

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII [On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine dated October 5, 2017, No. 2163-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy*, 2017, No. 45, Art. 403. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

2. Pro Sluzhbu bezpeky Ukrainy: Zakon Ukrainy vid 25.03.1992 r. № 2229-XII [On the Security Service of Ukraine: Law of Ukraine dated March 25, 1992, No. 2229-XII]. *Vidomosti Verkhovnoi Rady Ukrainy*, 1992, No. 27, Art. 382. Retrieved from: https://zakon.rada.gov.ua/laws/show/2229-12#Text [in Ukrainian].

3. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 r. № 2469-VIII [On National Security of Ukraine: Law of Ukraine dated June 21, 2018, No. 2469-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy*, 2018, No. 31, Art. 241. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].

4. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi infrastruktury: Zakon Ukrainy vid 27.03.2025 r. № 4336-IX [On Amendments to Certain Laws of Ukraine Concerning the Protection of Information and Cybersecurity of State Information Resources and Critical Information Infrastructure Facilities: Law of Ukraine dated March 27, 2025, No. 4336-IX]. *Vidomosti Verkhovnoi Rady Ukrainy*, 2025, No. 35, Art. 134. Retrieved from: https://zakon.rada.gov.ua/laws/show/4336-20#Text [in Ukrainian].

5. Sytuatsiinyi tsentr zabezpechennia kiberbezpeky SBU [Situational Center for Ensuring Cybersecurity of the Security Service of Ukraine]. *Sluzhba bezpeky Ukrainy*. Retrieved from: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky [in Ukrainian].

6. Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury: Postanova Kabinetu Ministriv Ukrainy vid 19.06.2019 r. № 518 [On Approval of the General Requirements for Cybersecurity of Critical Infrastructure Facilities: Resolution of the Cabinet of Ministers of Ukraine dated June 19, 2019, No. 518]. *Ofitsiinyi visnyk Ukrainy*, 2019, No. 50, Art. 1697. Retrieved from: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text [in Ukrainian].

7. Stratehiia rozvytku Sluzhby bezpeky Ukrainy na 2025–2030 roky [Strategy for the Development of the Security Service of Ukraine for 2025–2030]. *Sluzhba bezpeky Ukrainy*. Retrieved from: https://ssu.gov.ua/stratehiia-rozvytku-sluzhby-bezpeky-ukrainy-na-20252030-roky [in Ukrainian].

8. Kovaliv, M., Skrynkovskyi, R., Nazar, Yu., Yesimov, S., Krasnytskyi, I., Kaidrovych, Kh., Kniaz, S., & Kemska, Yu. (2021). Pravove zabezpechennia kiberbezpeky krytychnoi informatsiinoi infrastruktury Ukrainy [Legal support for cybersecurity of critical information infrastructure of Ukraine]. *Traektoriâ Nauki = Path of Science*, 7(4), 2011–2018. https://doi.org/10.22178/pos.69-12 [in Ukrainian].

9. Herasymenko, O. M. (2025). Heneza poniattia «krytychna infrastruktura» u konteksti protydii Sluzhboiu bezpeky Ukrainy zahrozam na yii obiektakh [Genesis of the concept of «critical infrastructure» in the context of countering threats to its facilities by the Security Service of Ukraine]. *Analitychno-porivnialne pravoznavstvo*, 3(4), 146–154. https://doi.org/10.24144/2788-6018.2025.04.3.22 [in Ukrainian].

10. Kovalchuk, A. T. (2025). Systema pravovoho rehuliuvannia zakhystu obiektiv krytychnoi infrastruktury v Ukraini: suchasnyi stan ta napriamy udoskonalennia [The system of legal regulation of the protection of critical infrastructure facilities in Ukraine: Current state and directions for improvement]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo*, 5(90), 172–184. https://doi.org/10.24144/2307-3322.2025.90.5.21 [in Ukrainian].

Дата першого надходження статті до видання: 10.09.2026
Дата прийняття статті до друку після рецензування: 28.09.2026
Дата публікації (оприлюднення) статті: 16.11.2026