№ 8(49) 2025
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК : 351.74:004.056.5

https://doi.org/10.52058/2786-6025-2025-8(49)-149-157

Насонов Максим Ігорович кандидат економічних наук, докторант кафедри конституційного, адміністративного та фінансового права Академії праці, соціальних відносин і туризму, м. Київ, https://orcid.org/0009-0009-7044-837

СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ: ПОВНОВАЖЕННЯ, ВЗАЄМОДІЯ, ВІДПОВІДАЛЬНІСТЬ

Анотація. В умовах глобальної цифровізації та перманентної гібридної агресії проти України, питання забезпечення інформаційної безпеки перетворилося на один із ключових пріоритетів національної безпеки. Інформаційний простір став полем протиборства, де ворожі актори застосовують широкий спектр інструментів: від кібератак на об'єкти критичної інфраструктури до проведення масштабних дезінформаційних кампаній. Ефективна протидія цим загрозам неможлива без злагодженої та чітко організованої системи державних органів, відповідальних за різні аспекти інформаційної безпеки. Зазначено, що актуальність даного дослідження зумовлена необхідністю наукового осмислення інституційної архітектури сектору безпеки в інформаційній сфері, виявлення її сильних та слабких сторін, а також розробки науково обґрунтованих рекомендацій щодо її вдосконалення.

У статті також проведено комплексний аналіз системи суб'єктів забезпечення інформаційної безпеки України. Досліджено нормативно-правові засади їх функціонування, розмежовано повноваження ключових суб'єктів, таких як Рада національної безпеки і оборони України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Кіберполіція та інші. Особливу увагу приділено аналізу механізмів їхньої взаємодії та координації, зокрема через діяльність Національного координаційного центру кібербезпеки.

Виявлено основні проблеми у функціонуванні системи, серед яких: часткове дублювання функцій, недостатній рівень міжвідомчої координації на практичному рівні та складнощі у притягненні до відповідальності за неналежне виконання обов'язків у сфері кіберзахисту.

На основі проведеного аналізу сформульовано пропозиції щодо вдосконалення законодавства та оптимізації інституційних механізмів з метою підвищення ефективності національної системи інформаційної безпеки в умовах гібридної війни.

Ключові слова: інформаційна безпека, кібербезпека, суб'єкти забезпечення інформаційної безпеки, повноваження, взаємодія, відповідальність, Національний координаційний центр кібербезпеки, гібридна війна.

Nasonov Maksim Igorovich Candidate of Economic Sciences, Doctoral student at the Department of Constitutional, Administrative and Financial Law of the Academy of Labor, Social Relations and Tourism, Kyiv, https://orcid.org/0009-0009-7044-837

INFORMATION SECURITY ENTITIES IN UKRAINE: AUTHORITY, INTERACTION, RESPONSIBILITY

Abstract. In the context of global digitalization and permanent hybrid aggression against Ukraine, the issue of ensuring information security has become one of the key priorities of national security. The information space has become a field of confrontation, where hostile actors use a wide range of tools: from cyberattacks on critical infrastructure facilities to conducting large-scale disinformation campaigns. Effective counteraction to these threats is impossible without a coordinated and clearly organized system of state bodies responsible for various aspects of information security.

It is noted that the relevance of this study is due to the need for a scientific understanding of the institutional architecture of the security sector in the information sphere, identifying its strengths and weaknesses, and developing scientifically based recommendations for its improvement.

The article also conducts a comprehensive analysis of the system of entities ensuring information security in Ukraine.

The regulatory and legal frameworks of their functioning are studied, the powers of key entities are delimited, such as the National Security and Defense Council of Ukraine, the Security Service of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Cyber Police, and others. Particular attention is paid to the analysis of the mechanisms of their interaction and coordination, in particular through the activities of the National Cybersecurity Coordination Center.

The main problems in the functioning of the system were identified, including: partial duplication of functions, insufficient level of interdepartmental coordination at the practical level and difficulties in holding accountable for improper performance of duties in the field of cyber defense.

Based on the analysis, proposals were formulated to improve legislation and optimize institutional mechanisms in order to increase the effectiveness of the national information security system in the context of hybrid warfare.

Keywords: information security, cybersecurity, information security entities, authority, interaction, responsibility, National Cybersecurity Coordination Center, hybrid warfare.

Постановка проблеми. Національна система забезпечення інформаційної безпеки України є багатокомпонентною структурою, до якої входять органи державної влади, військові формування, правоохоронні та розвідувальні органи. Її правову основу становлять: Закон України «Про національну безпеку України», Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки України та інші нормативно-правові акти. Незважаючи на наявність розгалуженої нормативної бази, на практиці виникає низка проблем, які потребують наукового аналізу, а саме:

1) розмитість та часткове дублювання повноважень. У деяких сферах компетенції ключових суб'єктів забезпечення інформаційної безпеки, зокрема Служби безпеки України та Держспецзв'язку, перетинаються, що призводить до інституційних конфліктів та неефективного використання ресурсів;

2) недостатня ефективність координації. Попри існування Національного координаційного центру кібербезпеки (НКЦК), міжвідомча взаємодія, особливо на тактичному рівні під час реагування на інциденти, часто залишається ускладненою через бюрократичні перепони та різну відомчу культуру;

3) прогалини у правовому регулюванні відповідальності. Механізми притягнення до відповідальності посадових осіб за бездіяльність або неналежне виконання обов'язків щодо захисту інформаційних ресурсів є недостатньо чіткими та рідко застосовуються на практиці.

Тож, як бачимо, існує нагальна потреба в системному дослідженні функціонального розподілу, механізмів взаємодії та юридичної відповідальності суб'єктів інформаційної безпеки для підвищення загальної стійкості держави до сучасних інформаційних загроз.

Аналіз останніх досліджень і публікацій. У науковій літературі останніх років активно досліджується правова та інституційна система забезпечення інформаційної безпеки в Україні. Так, Веселова О.Ю. акцентує увагу на нормативному оформленні повноважень головних суб'єктів кібербезпеки, зокрема СБУ, Держспецзв'язку, ЗСУ та розвідувальних органів, визначених у Стратегії кібербезпеки України. Малашко В.М. та Єсімов С.Б. аналізують чинне законодавство в цій сфері, підкреслюючи вплив Угоди про асоціацію з ЄС і необхідність гармонізації з європейськими стандартами [1, с. 30]. Науковці підкреслюють складність взаємодії між ключовими суб'єктами: РНБО, СБУ, Міністерством цифрової трансформації, CERT-UA, Центром протидії дезінформації, а також неурядовими ініціативами.

Зокрема, Шевчук О.І. вказує на важливість координаційної ролі Держспецзв'язку в системі управління інформаційною безпекою [2, с. 89]. Мельник В.І. розглядає адміністративно-правові аспекти цієї взаємодії в умовах воєнного стану, наголошуючи на потребі оперативного реагування та підвищення ролі суспільства [3, с. 43].

Попри значну кількість публікацій, присвячених суб'єктам забезпечення інформаційної безпеки держави та окремим аспектам кібербезпеки зокрема, бракує комплексних досліджень, які б системно аналізували повноваження, механізми взаємодію та питання відповідальності всієї сукупності таких суб'єктів.

Мета статті – комплексний аналіз системи суб'єктів забезпечення інформаційної безпеки України, визначення їхніх повноважень, оцінка ефективності механізмів взаємодії та розробка пропозицій щодо посилення їхньої відповідальності.

Виклад основного матеріалу. Національна система кібербезпеки складається з основних суб'єктів, кожен з яких виконує специфічні функції. Діяльність суб'єктів забезпечення інформаційної безпеки України, регулюється профільним законодавством, яке визначає межі їхньої компетенції.

Отже, розглянемо кожен з таких суб'єктів та окреслимо ряд повноважень якими вони наділені у сфері кібербезпеки нашої держави.

1. Рада національної безпеки і оборони України (РНБО) є координаційним органом з питань національної безпеки і оборони при Президентові України. Ключова роль РНБО в інформаційній сфері реалізується через Національний координаційний центр кібербезпеки (НКЦК), який є робочим органом РНБО.

Національний координаційний центр кібербезпеки (НКЦК) [4]:

- забезпечує координацію та контроль за діяльністю всіх суб'єктів сектору безпеки;
- аналізує стан кіберзахисту;
- прогнозує загрози;
- розробляє пропозиції щодо стратегічного розвитку системи. Діяльність центру спрямована на синхронізацію зусиль різних відомств на стратегічному рівні.

2. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) є основним технічним регулятором у сфері кіберзахисту. До її ключових повноважень належать [5]:

а) формування та реалізація державної політики у сферах кіберзахисту, криптографічного та технічного захисту інформації; б) забезпечення функціонування Державного центру кіберзахисту та урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

в) проведення державних експертиз та аудитів інформаційної безпеки на об'єктах критичної інфраструктури.

Акцентуємо увагу на тому, що Державна служба спеціального зв'язку та захисту інформації України фокусується на превентивних заходах, встановленні стандартів та технічному реагуванні на інциденти в державному секторі та на об'єктах критичної інфраструктури.

3. Служба безпеки України (СБУ) є головним органом у системі контррозвідувальної діяльності та протидії загрозам державній безпеці в інформаційній сфері. Повноваження Служби безпеки України включають [6]:

- виявлення, попередження та припинення розвідувально-підривної діяльності іноземних спецслужб в інформаційному просторі;
- боротьбу з такими протиправними діяннями, як: кібертероризм та кібершпигунство;
- розслідування кримінальних правопорушень проти основ національної безпеки, вчинених з використанням комп'ютерних систем.

Як бачимо, Служба безпеки України концентрується на виявленні та нейтралізації найбільш небезпечних загроз, які походять від іноземних спецслужб, терористичних організацій, кіберзлочинних угрупувань та інших суб'єктів, які здійснюють діяльність, спрямовану на підрив суверенітету, конституційного ладу, обороноздатності та безпосередньо інформаційної безпеки нашої держави.

4. Департамент кіберполіції Національної поліції України, правоохоронний орган, який спеціалізується на боротьбі із загально кримінальною кіберзлочинністю. Перед кіберполіцією у першу чергу стоять наступні завдання [7]:

а) протидія шахрайству з використанням електронно-обчислювальної техніки, несанкціонованому втручанню в роботу комп'ютерних мереж;

б) боротьба з розповсюдженням шкідливого програмного забезпечення, дитячої порнографії в мережі Інтернет та іншими кіберзлочинами.

Зазначимо, що зазвичай, кіберполіція працює переважно із кримінальними правопорушеннями, що мають кримінальний, інформаційний, а не політичний чи військовий характер.

До інших не менш важливих суб'єктів забезпечення інформаційної безпеки України належать:

- Міністерство оборони України та Збройні Сили України, які безпосередньо відповідальні за кібероборону нашої держави у військовій сфері;
- розвідувальні органи, які займаються кіберрозвідкою;
- Національний банк України – забезпечує кібербезпеку в банківській системі.

Важливо розуміти, що ефективність усієї системи забезпечення інформаційної безпеки буде залежить від якості взаємодії між її елементами. Основним майданчиком для координації, як ми вже зазначали вище, є Національний координаційний центр кібербезпеки (НКЦК), який проводить регулярні засідання та організовує обмін інформацією між ключовими суб'єктами. Важливу роль відіграє платформа обміну даними про кіберінциденти MISP-UA, яку адмініструє CERT-UA.

Однак, попри існуючі механізми взаємодії, вони є доволі формальними, що призводить до суттєвих проблем та викликів.

Науковці зазначають, що взаємодія доволі часто має ситуативний характер і залежить від особистих контактів між керівниками середньої ланки, а не від сталих інституційних процедур [8, с 48]. Проблемою у даному аспекті залишається відомча конкуренція, особливо між силовими структурами, які ускладнює не своєчасний та не повний обмін критично важливою інформацією.

Проведення спільних навчань, таких як національні кіберзмагання, позитивно впливає на злагодженість дій, але їхня періодичність та масштаб є недостатніми для вироблення стійких навичок міжвідомчої співпраці.

Отже, хочемо дещо зупинитись на системних проблемах системи кібербезпеки України та шляхах їх вирішення. Так, аналіз поточної системи забезпечення інформаційної безпеки в Україні показує, що, попри наявність розгалуженої інституційної структури з формально визначеними повноваженнями, її ефективність знижується через низку системних проблем. Розуміння цих викликів є ключовим для розробки дієвих заходів, які дозволять посилити стійкість нашої держави до сучасних кіберзагроз.

Однією з головних проблем, на наш погляд, є нечітке розмежування повноважень у суміжних сферах, що часто призводить до конкуренції замість необхідної співпраці.

Наприклад, у ситуаціях, які стосуються кіберінцидентів на об'єктах критичної інфраструктури, виникає плутанина між повноваженнями Держспецзв'язку, СБУ та Кіберполіції. Кожне відомство може мати власні протоколи та підходи до розслідування таких протиправних діянь, що уповільнює процес розкриття і призводить до дублювання функцій. Така невизначеність не лише гальмує швидке реагування, а й розмиває відповідальність, що є неприпустимим в умовах постійних загроз.

На додаток до цього, існує недосконаліть практичних механізмів взаємодії між суб'єктами кібербезпеки. Відсутність єдиних, обов'язкових протоколів реагування та оперативної координації призводить до того, що інформація про загрози передається повільно, а реакція на них є фрагментарною. В умовах кібератак, де кожна секунда на вагу золота, така затримка може мати катастрофічні наслідки. Вирішення цієї проблеми вимагає

не просто формальної співпраці, а й створення дієвих, спільних платформ для обміну даними та координації дій у режимі реального часу [8, с 49].

Ще одним критичним недоліком є слабкість інституту відповідальності. Питання відповідальності у досліджуваній сфері є одним із найменш врегульованих. Законодавство передбачає кримінальну та адміністративну відповідальність для посадових (службових) осіб за порушення у сфері захисту інформації. Наприклад, стаття 363 Кримінального кодексу України встановлює відповідальність за порушення правил експлуатації автоматизованих систем. Проте довести причинно-наслідковий зв'язок між бездіяльністю конкретної посадової (службової) особи та настанням шкідливих наслідків внаслідок кібератаки вкрай складно, тому керівники, відповідальні за кібербезпеку в державних установах та на об'єктах критичної інфраструктури, часто не відчувають особистої відповідальності за недостатній рівень захисту.

Більшість випадків неналежного забезпечення кіберзахисту на державних підприємствах чи в органах влади завершуються лише заходами дисциплінарного впливу, що не створює достатнього превентивного ефекту.

Відсутній також дієвий механізм парламентського та громадського контролю за діяльністю суб'єктів інформаційної безпеки, що знижує рівень їхньої підзвітності. Необхідно розробити чіткі критерії оцінки ефективності (KPIs) для керівників, відповідальних за кібербезпеку, та посилити механізми аудиту та контролю [9, с. 191], тому як ефективний парламентський та громадський контроль за діяльністю суб'єктів інформаційної безпеки часто є номінальним, що знижує їхню підзвітність.

Для подолання окреслених проблем необхідно застосовувати комплексний підхід, який буде включати заходи на трьох рівнях: законодавчому, інституційному та практичному.

Вважаємо, що на законодавчому рівні потрібно деталізувати та уточнити повноваження всіх суб'єктів у суміжних сферах, особливо в контексті розслідування кіберінцидентів на критичній інфраструктурі. Це дозволить уникнути дублювання повноважень та конфліктних ситуацій. Також, слід внести зміни, які посилять відповідальність керівників за недбалість у сфері кіберзахисту.

На інституційному рівні, на наш погляд, необхідно надати НКЦК при РНБО реальні повноваження та достатнє ресурсне забезпечення, що надасть змогу НКЦК ефективно виконувати роль головного координатора. Впровадження обов'язкових спільних протоколів реагування та регулярних спільних навчань допоможе відпрацювати взаємодію в кризових ситуаціях.

На практичному рівні потрібно розвивати культуру співпраці та довіри між різними відомствами. Створення спільних аналітичних та оперативно-технічних груп, що працюють на постійній основі, дозволить об'єднувати

зусилля та ділитися досвідом. Це сприятиме ефективній роботі та забезпечить більш стійкий та скоординований захист.

Реалізація зазначених пропозицій дозволить значно підвищити результативність в роботі суб'єктів забезпечення інформаційної безпеки та посилити стійкість України до загроз у кіберпросторі. Це є ключовим завданням для забезпечення національної безпеки в сучасних умовах.

Висновки. Проведений аналіз показав, що в Україні створено розгалужену інституційну систему забезпечення інформаційної безпеки з формально визначеними повноваженнями ключових суб'єктів. Стратегічну координацію покликаний здійснювати НКЦК при РНБО, технічний захист покладено на Держспецзв'язку, контррозвідувальний – на СБУ, а боротьбу з загально кримінальною кіберзлочинністю – на Кіберполіцію.

Разом з тим, ефективність цієї системи знижується через низку системних проблем, таких як:

- нечітке розмежування повноважень у суміжних сферах, що провокує конкуренцію замість співпраці;
- недосконаліть практичних механізмів взаємодії, що уповільнює реакцію на загрози;
- слабкість інституту відповідальності, що не стимулює посадових (службових) осіб до проактивних дій у сфері кіберзахисту.

Для подолання цих викликів доцільно вжити таких заходів, як:

- на законодавчому рівні – деталізувати повноваження суб'єктів у суміжних сферах, зокрема у питаннях розслідування кіберінцидентів на об'єктах критичної інфраструктури. Внести зміни до законодавства з метою посилення відповідальності керівників за неналежний рівень кіберзахисту;
- на інституційному рівні – посилити реальні повноваження та ресурсну спроможність НКЦК як головного координатора. Впровадити обов'язкові спільні протоколи реагування на різні типи кіберзагроз. Розширити практику регулярних спільних навчань;
- на практичному рівні – розвивати культуру співпраці та довіри між різними відомствами, зокрема шляхом створення спільних аналітичних та оперативно-технічних груп.

Реалізація цих пропозицій дозволить підвищити взаємодію в роботі суб'єктів забезпечення інформаційної безпеки та посилити стійкість України до загроз у кіберпросторі.

Література:

1. Малашко В.М., Єсімов С.Б. Правові засади інформаційної безпеки в Україні. *Право і безпека.* 2020. №2. С. 27–34.

2. Шевчук О.І. Система управління інформаційною безпекою в контексті сучасних викликів. *Вісник ХНУВС*. 2024. №1. С. 88–93.

3. Мельник В.І. Інформаційна безпека в умовах воєнного стану: адміністративно-правові механізми. *Держава і право.* 2025. №2. С. 41–47.

4. Про Національний координаційний центр кібербезпеки: Указ Президента України від 7 червня 2016 року № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

5. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

6. Про Службу безпеки України: Закон України від 25.03.1992 р. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

7. URL: https://cyberpolice.gov.ua/normatyvno-pravovi-akty-yaki-rehlamentuiut-diialnist-politseiskoi-komisii/

8. Дубов Д. В. Інституційні механізми забезпечення кібербезпеки: міжнародний досвід та уроки для України. *Стратегічні пріоритети.* 2019. № 4 (52). С. 45–53.

9. Ткачук П. П. Проблеми правового регулювання відповідальності у сфері кібербезпеки. *Право і суспільство.* 2020. № 2. Ч. 2. С. 189–194.

References:

1. Malashko V.M., Yesimov S.B. (2020). Pravovi zasady informatsiynoyi bezpeky v Ukrayini [Legal principles of information security in Ukraine]. *Pravo i bezpeka.* №2, 27–34. [in Ukrainian].

2. Shevchuk O.I. (2024). Systema upravlinnya informatsiynoyu bezpekoyu v konteksti suchasnykh vyklykiv [Information security management system in the context of modern challenges]. *Visnyk KHNUVS,* №1, 88–93. [in Ukrainian].

3. Mel′nyk V.I. (2025). Informatsiyna bezpeka v umovakh voyennoho stanu: administratyvno-pravovi mekhanizmy [Information security in martial law conditions: administrative and legal mechanisms]. *Derzhava i pravo,* №2, 41–47. [in Ukrainian].

4. Pro Natsional′nyy koordynatsiynyy tsentr kiberbezpeky [About the National Cybersecurity Coordination Center]: Ukaz Prezydenta Ukrayiny (2016). URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

5. Pro Derzhavnu sluzhbu spetsial′noho zv'yazku ta zakhystu informatsiyi Ukrayiny [About the State Service for Special Communications and Information Protection of Ukraine]: Zakon Ukrayiny (2006). URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

6. Pro Sluzhbu bezpeky Ukrayiny [About the Security Service of Ukraine]: Zakon Ukrayiny. (1992). URL : https://zakon.rada.gov.ua/laws/show/2229-12#Text

7. URL: https://cyberpolice.gov.ua/normatyvno-pravovi-akty-yaki-rehlamentuiut-diialnist-politseiskoi-komisii/

8. Dubov D. V. (2019). Instytutsiyni mekhanizmy zabezpechennya kiberbezpeky: mizhnarodnyy dosvid ta uroky dlya Ukrayiny [Institutional mechanisms for ensuring cybersecurity: international experience and lessons for Ukraine]. *Stratehichni priorytety*, № 4 (52), 45–53. [in Ukrainian].

9. Tkachuk P. P. (2020). Problemy pravovoho rehulyuvannya vidpovidal′nosti u sferi kiberbezpeky [Problems of legal regulation of liability in the sphere of cybersecurity]. *Pravo i suspil'stvo*, № 2, 189–194. [in Ukrainian].