Кримінальне право та кримінологія

УДК 343.9

Цюприк Ігор Володимирович
доктор юридичних наук,
професор кафедри кримінального процесу та криміналістики
Національна академія СБУ
Tsiupryk Igor
Doctor of Law, Professor of the Department of
Criminal Procedure and Forensics
National Academy of the Security Service of Ukraine
ORCID: 0009-0007-4460-9968

ПУБЛІЧНО-ПРИВАТНЕ ПАРТНЕРСТВО ЯК СТРАТЕГІЧНИЙ ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ В УКРАЇНІ

PUBLIC-PRIVATE PARTNERSHIP AS A STRATEGIC TOOL FOR ENSURING CYBERSECURITY UNDER THE LEGAL REGIME OF MARTIAL LAW IN UKRAINE

Анотація. *Вступ. Кібератаки проти державних інституцій, критичної інфраструктури, банківської системи, засобів масової інформації та телекомунікацій стали звичним інструментом впливу держави-агресора під час повномасштабного вторгнення на території України. Наша держава стала унікальним полігоном, де формуються нові стратегії кіберзахисту у реальному часі за участю як публічної влади, так і приватного сектору. У таких умовах постало складне завдання - ефективно забезпечити та організувати кіберзахист як складову національної безпеки України, що вимагає не лише технічних рішень і цифрових інструментів, а й створення надійного нормативно-правового*

забезпечення, що дозволить мобілізувати та координувати дії всіх учасників кіберпростору.

Таким чином, актуальність даного дослідження обумовлена безпрецедентним рівнем кіберзагроз, від ефективності боротьби з якими залежить стійкість національного суверенітету України.

Метою статті є комплексний аналіз ролі органів державної влади та приватного сектору у протидії кіберзагрозам в умовах правового режиму воєнного стану, а також виявлення основних проблем нормативного забезпечення кіберзахисту і визначення перспектив вдосконалення відповідного правового регулювання.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правові акти національного та міжнародного законодавства щодо забезпечення кібербезпеки; 2) доктринальні джерела; 3) аналітичні матеріали з відкритих джерел, що стосуються кіберзахисту в умовах правового режиму воєнного стану в Україні.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування; аналізу та синтезу; порівняльно-правовий метод; логічного узагальнення результатів.

Результати. У науковій статті наведено ефективні приклади співпраці органів державної влади з приватним сектором під час війни в Україні; визначено значення приватного сектору, як важливого ресурсу національного кіберфронту; окреслено головні нормативно – правові прогалини, що ускладнюють ефективне функціонування кіберзахисту в умовах правового режиму воєнного стану.

Перспективи. У подальших наукових дослідженнях варто зосередити увагу на розробках: моделі державно-приватного партнерства у сфері кібербезпеки, яка б враховувала специфіку інформаційних загроз, особливості правового режиму воєнного стану та принципи публічного адміністрування в умовах цифрової трансформації; механізмів

інформаційного обміну між публічною владою та приватним сектором; нормативно-правового забезпечення дорадчої участі приватного сектору у формуванні кіберполітики.

Ключові слова: *кібербезпека, воєнний стан, державна влада, приватний сектор, правове регулювання.*

Summary. *Introduction. Cyberattacks targeting government institutions, critical infrastructure, the banking system, media, and telecommunications have become a routine tool of influence used by the aggressor state during the full-scale invasion of Ukraine. Ukraine has become a unique testing ground where new cybersecurity strategies are being developed in real-time, involving both public authorities and the private sector. In such circumstances, a complex task has emerged—effectively ensuring and organizing cyber defense as a component of Ukraine's national security. This requires not only technical solutions and digital tools but also the establishment of a reliable legal and regulatory framework that enables the mobilization and coordination of all subjects in cyberspace.*

Accordingly, the relevance of this study is driven by the unprecedented scale of cyber threats, with the resilience of Ukraine's national sovereignty depending on the effectiveness of countering them.

The purpose of the article is to provide a comprehensive analysis of the role of state authorities and the private sector in countering cyber threats under the legal regime of martial law, as well as to identify key regulatory gaps and propose directions for improving the relevant legal framework.

Materials and methods. The study is based on the following materials: national and international legal acts on cybersecurity; doctrinal legal sources; analytical reports and open-source materials concerning cyber defense under martial law in Ukraine.

The research methodology includes theoretical generalization and classification, analysis and synthesis, comparative legal method, and logical generalization of the findings.

Results. The article provides effective examples of cooperation between public authorities and the private sector during the war in Ukraine. It highlights the private sector's significance as a crucial resource on the national cyber front and outlines major regulatory gaps that hinder the effective functioning of cyber defense under martial law.

Discussion. Future research should focus on the development of: a public-private partnership model for cybersecurity that takes into account the specific nature of information threats, the peculiarities of the martial law regime, and the principles of public administration in the context of digital transformation; mechanisms of information exchange between public authorities and the private sector; and regulatory frameworks enabling the consultative involvement of the private sector in the formation of cyber policy.

Key words: *cybersecurity, martial law, public authorities, private sector, legal regulation.*

Постановка проблеми. З початком повномасштабного вторгнення на територію України кіберпростір став одним із головних фронів протистояння. Масовані кібератаки на об'єкти критичної інфраструктури, органи державної влади, фінансовий сектор та інформаційне середовище довели, що питання кібербезпеки набули першочергового значення для національної безпеки держави. У таких умовах особливої актуальності набуває дослідження ролі публічної влади у забезпеченні кіберзахисту, а також взаємодії з приватним сектором і громадянським суспільством.

Попри значні зусилля державних органів у розбудові національної системи кібербезпеки, чинне правове регулювання не забезпечує належної координації між публічними та приватними суб'єктами. Відсутність чітких

правових механізмів публічно-приватного партнерства знижує ефективність реагування на кіберзагрози, що зумовлює потребу в комплексному аналізі наявного стану правового забезпечення кібербезпеки, виявленні прогалин та формулюванні напрямів удосконалення нормативно - правової бази.

Аналіз останніх досліджень і публікацій. Проблематика кібербезпеки як складової національної безпеки та роль держави в цій сфері є предметом дослідження низки українських і зарубіжних науковців. Так, у працях А. Сороченка, Б. Шулюка, Б. Головкіна, Я. Ізмайлова, В. Цимбалюка, Н. Малиновської, О. Крутій, О. Радченка, В. Козлова, О. Федорчака та О. Кравченка здійснено ґрунтовний аналіз інституційно-правових засад функціонування національної системи кібербезпеки України. Дослідники розглядають повноваження ключових державних органів у цій сфері, зокрема Державної служби спеціального зв'язку та захисту інформації України, Ради національної безпеки і оборони, а також розкривають роль національних стратегій та програм у забезпеченні кіберзахисту [1–5].

Вагомий внесок у вивчення нормативно-правових аспектів забезпечення кібербезпеки зроблено в аналітичних записках Національного інституту стратегічних досліджень, де окреслено основні тенденції розвитку державно-приватної взаємодії, а також вказано на необхідність розробки правових механізмів взаємодії з IT-сектором [7]. Крім того, автор Ю. Шипілова учасник Міжнародної фундації виборчих систем (IFES) [8] надає всебічний огляд та аналіз існуючої правової системи кібербезпеки в Україні, дотримання країною міжнародних зобов'язань і найкращих практик, приділяючи значну увагу міжвідомчій координації.

Окремі наукові публікації акцентують увагу на викликах воєнного стану, що зумовлює трансформацію існуючих правових механізмів кіберзахисту. Зокрема, у дослідженні Інституту досліджень кібервійни завдяки підтримці, наданій Агентством США зміжнародного розвитку

(USAID) [9] наведено докладну картину кіберзагроз, з якими стикалась Україна протягом 2023 року, що дозволяє оцінити ступінь вразливості державного і приватного секторів.

У публікаціях на професійних платформах, таких як DOU.ua, GigaCloud, а також в офіційних релізах Державної служби спеціального зв'язку та захисту інформації України [10; 13–14], окреслено приклади практичної взаємодії між державою та ІТ-спільнотою, в тому числі у форматі кіберволонтерства, цифрових альянсів та обміну інформацією про загрози.

Проте, попри значну кількість напрацювань, в українській науковій літературі все ще недостатньо висвітлено питання публічно-приватного партнерства саме в контексті сучасних викликів воєнного стану. Більшість наявних досліджень зосереджені переважно на теоретичному обґрунтуванні поняття кібербезпеки або на загальній характеристиці інституційних структур, не приділяючи достатньої уваги механізмам координації, розподілу відповідальності та правового регулювання взаємодії між державою, бізнесом і громадянськими ініціативами. Залишається не до кінця дослідженим потенціал публічно-приватного партнерства як інструмента зміцнення кіберзахисту в умовах воєнного стану, коли традиційні моделі реагування потребують оперативної адаптації та інноваційних підходів.

Отже, дана стаття спрямована на заповнення окресленої прогалини шляхом комплексного аналізу правового статусу та ролі публічної влади у забезпеченні кібербезпеки, а також формування практичних рекомендацій щодо розвитку ефективних моделей взаємодії між державними органами, приватним сектором і громадянським суспільством. У цьому контексті особливу увагу буде приділено аналізу чинного законодавства, зокрема Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки України, а також досвіду участі ІТ-компаній у

проектах кібероборони (наприклад, проект «Кіберполк») та актуальним практикам цифрового суверенітету [2; 4; 11; 14].

Метою статті є комплексний аналіз ролі органів державної влади та приватного сектору у протидії кіберзагрозам в умовах правового режиму воєнного стану, а також виявлення основних проблем нормативного забезпечення кіберзахисту і визначення перспектив вдосконалення відповідного правового регулювання.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правові акти національного та міжнародного законодавства щодо забезпечення кібербезпеки; 2) доктринальні джерела; 3) аналітичні матеріали з відкритих джерел, що стосуються кіберзахисту в умовах правового режиму воєнного стану в Україні.

В процесі здійснення дослідження було використано наступні наукові методи: теоретичного узагальнення та групування; аналізу та синтезу; порівняльно-правовий метод; логічного узагальнення результатів.

Виклад основного матеріалу. У системі національної безпеки України публічна влада відіграє ключову роль у формуванні, реалізації та координації політики кібербезпеки. У контексті повномасштабного вторгнення в Україну, завдання публічної влади не лише значно ускладнились, а й набули критичного значення для збереження стабільності національної безпеки держави.

Центральними суб'єктами, що забезпечують організацію кіберзахисту на державному рівні, є Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, Державна служба спеціального зв'язку та захисту інформації України, а також Рада національної безпеки і оборони України. Крім того, як передбачено ст. 8 Закону до основних суб'єктів національної системи кібербезпеки також відноситься Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи України,

Національний банк України, Міністерство закордонних справ України [2]. Їхня роль є не лише інституційною, а й стратегічною: від оперативного реагування до розроблення нормативно-правових засад кіберзахисту.

Державна служба спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку) є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону [1].

Під час правового режиму воєнного стану функції Держспецзв'язку було істотно розширено. Вона виступає головним координатором міждержавного реагування на кіберзагрози, адмініструє Національну телекомунікаційну мережу, здійснює криптографічний захист урядової інформації, розробляє нормативно-технічну документацію з питань безпеки інформації. Окрім того, Держспецзв'язок здійснює сертифікацію комплексних систем захисту інформації, що є особливо важливим для безпеки баз даних, інформаційних систем органів державної влади та оборонно-промислового комплексу. Служба також активно координує співпрацю з союзниками у сфері кібербезпеки. Результатом такої співпраці стало не лише постачання технічного обладнання та спеціального програмного забезпечення, а й створення міжвідомчих команд швидкого реагування на масштабні кібератаки, а також підвищення рівня підготовки українських фахівців.

До прикладу, лише за період травня 2025 року Держспецзв'язку: підписала Меморандум щодо співпраці та взаємодії в галузі кібербезпеки з Генеральним директором Управління національної безпеки Норвегії; підписала Меморандум про взаєморозуміння у сфері захисту критичної

інфраструктури з Міністерством юстиції та безпеки Королівства Нідерланди; спільно з аналітичним центром ICE Task Force підготувала звіт «Війна та кібер: три роки боротьби та уроки для глобальної безпеки», що охоплює ключові тенденції кібервійни проти України з початку повномасштабного вторгнення у 2022 році до сьогодні [10].

Рада національної безпеки і оборони України (далі – РНБО) відповідно до Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України [3]. В умовах воєнного стану саме РНБО виступає ініціатором стратегічних рішень, які закладають основи для формування стійкої архітектури кіберзахисту держави.

У межах РНБО функціонує Національний координаційний центр кібербезпеки (далі - НКЦК) - постійно діючий робочий орган, створений відповідно до указу Президента України у 2016 році. НКЦК виконує важливу функцію міжвідомчого узгодження дій між державними структурами, зокрема Службою безпеки України, Держспецзв'язку, Міністерством оборони, Міністерством цифрової трансформації, а також з представниками приватного сектору та міжнародними партнерами.

Одним із ключових досягнень НКЦК стало розроблення Стратегії кібербезпеки України на період з 2021 року до 2025 року, затвердженої Указом Президента № 447/2021 [4]. Крім того, РНБО координує систему впровадження індикаторів кіберзагроз, адмініструє впровадження національного сегменту кіберпростору, організовує масштабні навчання з кібероборони та аналізує звіти про кіберінциденти, надаючи стратегічні рекомендації Уряду.

В той же час, Computer Emergency Response Team of Ukraine (далі - CERT-UA) - національна урядова команда реагування на кіберінциденти, кібератаки, кіберзагрози, що є структурним підрозділом Держспецзв'язку і виконує роль першої лінії оборони в системі кібербезпеки державного

сектору. Основним завданням CERT-UA є моніторинг кібератак, їх документування, аналіз, нейтралізація наслідків та надання методичної допомоги суб'єктам, які забезпечують кібербезпеку, у тому числі і об'єктам критичної інфрастуктури.

З початком повномасштабної війни CERT-UA зазнала значного інституційного посилення - як у технічному, так і в кадровому сенсі. Було запроваджено нові алгоритми швидкого реагування, сформовано базу кіберзагроз, посилено співпрацю з приватним сектором і міжнародними організаціями. CERT-UA щомісяця фіксує сотні інцидентів, пов'язаних із розповсюдженням шкідливого програмного забезпечення, DDoS-атаками, фішингом та цілеспрямованим кібершпіонажем, який, як правило, має проросійське походження. На своєму офіційному веб-сайті команда демонструє виявлені та зафіксовані ними кіберзагрози, висвітлює механізм їх дії, індикатори та приклади ланцюжків ураження, що стає своєрідним запобіжником та сприяє кіберобізнаності як громадян України, так і її державних органів.

Не менш важливим є у те, що у період 2024–2025 років Україна активізувала співпрацю між державною владою та приватним сектором з метою посилення кібербезпеки, розвитку цифрової інфраструктури та впровадження інноваційних технологій.

Одним із ключових напрямів співпраці стало залучення міжнародних технологічних гігантів до підтримки українських державних установ. Зокрема, компанія Microsoft продовжила надавати безкоштовні хмарні послуги українським державним органам до кінця 2025 року, що сприяє зміцненню цифрової стійкості держави та посиленню захисту державних установ у кіберпросторі. Як повідомляє міністр цифрової трансформації України Михайло Федоров: «У 2023 році компанія надала Україні технологічну допомогу на суму $500+ мільйонів, у 2024-му ще на $100 мільйонів, у 2025-му допомога надходитиме в такому ж обсязі». Компанія

також допомогла перенести цифрову інфраструктуру в безпечні дата-центри по всій Європі та активно підтримує проекти з кібербезпеки, розслідування воєнних злочинів та фінансування гуманітарних організацій в Україні.

Активно співпрацюють з державними органами й українські мобільні оператори та телекомунікаційні компанії. Наприклад, у грудні 2024 року компанії Київстар, VEON і Starlink підписали угоду про запуск революційної технології супутникового зв'язку Direct to Cell, що забезпечить зв'язком навіть найвіддаленіші куточки країни. Крім того, у 2024 році телекомунікаційні оператори України, зокрема Київстар, Vodafone Україна та lifecell, активізували взаємодію з державними органами для забезпечення безперебійного зв'язку та захисту мереж від кібератак, зокрема, було впроваджено спільні ініціативи з CERT-UA щодо обміну інформацією про кіберінциденти та впровадження механізмів швидкого реагування на загрози. У рамках Kyiv International Cyber Resilience Forum 2025 було проведено спільні навчання з виявлення та нейтралізації кібератак на інфраструктуру телекомунікаційних компаній, що дозволило підвищити рівень готовності до потенційних загроз [12].

У 2025 році державні органи України посилили співпрацю з провідними дата-центрами та хмарними провайдерами, такими як GigaCloud і De Novo та дата-центр «ПАРКОВИЙ»: «…Компанії підписали спільний Меморандум «Про заснування Громадської спілки «Український альянс цифрового суверенітету». У документі визначено ключові принципи співпраці та завдання, які має виконувати кожен учасник ініціативи. Одним із таких завдань є повернення критично важливих державних даних під українську юрисдикцію, зокрема через такі інструменти як політика Data Embassy та багатодоменна безпека» [14].

Українські технологічні компанії, зокрема FAVBET Tech, також активно долучилися до ініціатив з кібербезпеки: «…FAVBET Tech підтримала захід та стала партнером KICRF, що є продовженням зусиль з

розвитку кібербезпеки в Україні та розширення співпраці для боротьби з цифровими загрозами. З 2022 року компанія є частиною української цифрової армії, бере участь у розробці ПЗ для потреб війська…» [15].

«FAVBET Tech став новим партнером ГО «КіберПолк» та співпрацюватиме з організацією у напрямах кіберзахисту, військово-інформаційних операцій та підготовки фахівців з цифрової безпеки. Команда технологічної компанії буде залучена в тому числі до розробки програмного забезпечення для потреб ЗСУ, а також обмінюватиметься з фахівцями організації досвідом для пошуку вразливостей у ворожих ІТ системах» [11]. У 2025 році компанія стала партнером конференції InfoSec Ukraine 2025, де представила власні рішення у сфері штучного інтелекту для виявлення та запобігання кібератакам.

Не варто забувати й про важливий внесок громадян України, що об'єдналися на волонтерських засадах задля допомоги у боротьбі з кіберзагрозами. Наприклад, «ІТ-Армія України» - це спільнота ІТ-фахівців з усього світу, що була створена в лютому 2022 року за ініціативи Міністерства цифрової трансформації України, що допомагає виконувати широкий спектр завдань, зокрема здійснювати: DDOS - атаки на кіберінфраструктуру противника, захист критичної інфраструктури України, аналітичну та розвідувальну роботу (моніторинг ворожих телеграм-каналів, виявлення військових перевезень, геолокація фото/відео), інформаційну боротьбу (протидію дезінформації, злам пропагандистських ресурсів, виведення з ладу платформ дезінформації).

З вищевикладеного чітко простежується, що завдяки спільним зусиллям держави, приватного сектору та громадянського суспільства було впроваджено ефективні механізми захисту критичної інфраструктури, підвищено рівень обізнаності бізнесу щодо кіберзагроз та забезпечено інтеграцію інноваційних технологій у систему національного кіберзахисту,

що вкотре підкреслює важливість подальшого розвитку публічно-приватного партнерства для забезпечення кіберзахисту України.

Проте, в українських реаліях співпраця держави з приватним сектором у сфері кіберзахисту значно випереджає законодавство. Наприклад: компанії-оператори зв'язку співпрацюють із CERT-UA (командою реагування на комп'ютерні інциденти) без формалізованих угод, керуючись швидше принципами національної безпеки; приватні хостинг-провайдери та дата-центри регулярно надають тимчасовий простір для переносу державних ресурсів у разі атак; IT-компанії (зокрема, аутсорсинг та security-as-a-service фірми) фактично виконують роль резервних підрозділів для державних органів, передаючи трафік на резервні маршрути, допомагаючи з шифруванням даних, впровадженням VPN тощо.

Попри значні досягнення на практичному рівні, нормативно-правове врегулювання публічно-приватного партнерства у сфері кібербезпеки залишається фрагментарним і несистемним. Наявні законодавчі конструкції, хоча й частково визнають можливість такої співпраці, однак не забезпечують належного правового механізму її реалізації.

Ще у 2022 році Єгор Аушев – співзасновник і генеральний директор компанії Cyber Unit Technologies зазначав, що на його погляд: «…все, крім секретної інформації в державі, має обслуговувати приватний сектор, а держава має бути великим замовником у нього, спонукаючи його до розвитку й створення внутрішнього ринку, бо зараз, немає якісного внутрішнього ринку з кібербезпеки» [13].

Фактично, поняття «публічно-приватного партнерства» в контексті кібербезпеки не закріплено в національному законодавстві, що підлягає подальшому правовому врегулюванню. Більш того, Закон України «Про основні засади забезпечення кібербезпеки України» не відносить приватний сектор, в особі фізичних та юридичних осіб, до суб'єктів національної системи кібербезпеки, що значно обмежує можливість залучення

представників бізнесу до процесів формування державної політики у цій сфері, а також позбавляє їх доступу до інституційних інструментів державного реагування на кіберзагрози.

Хоча у вказаному Законі йдеться про доцільність залучення приватних команд реагування, про необхідність обміну інформацією між державою, бізнесом та громадянами, однак механізм такої взаємодії не отримав нормативного наповнення. Внаслідок цього у правозастосовній практиці виникає колізійність: з одного боку, декларується важливість участі приватного сектору, з іншого — законодавство не визначає форм, процедур чи засобів такої участі. Сама термінологія закону сформульована занадто широко, а відсутність підзаконних актів, що деталізують відповідні положення, лише поглиблює правову невизначеність.

Слід також зазначити, що норми чинного законодавства, на жаль, не відповідають викликам, пов'язаним із кількістю кіберзагроз в умовах правового режиму воєнного стану. Чинні положення законодавства, які стосуються державно-приватної співпраці в сфері кібербезпеки, залишаються декларативними та такими, що не передбачають ефективного інструментарію взаємодії.

Наприклад, ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» передбачає напрями взаємодії з приватним сектором, зокрема створення системи виявлення загроз, обмін інформацією, підвищення обізнаності та цифрової грамотності, обмін інформацією тощо. Проте жоден із запропонованих механізмів не деталізовано на рівні конкретних процедур, суб'єктів виконання чи фінансування, що робить їх непридатними для практичного застосування [2].

Окремо варто звернути увагу на положення Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 07.03.2025 № 204-р. Документ чітко визначає потребу створення кіберрезерву та відпрацювання механізму його

мобілізації. Проте навіть така прогресивна ініціатива станом на травень 2025 року досі не знайшла свого нормативного закріплення та реалізації [5].

З огляду на зазначене, комплексне вирішення проблеми нормативної фрагментарності участі приватного сектору в забезпеченні кібербезпеки України потребує не лише внесення точкових змін до чинного законодавства, а й розроблення нового, спеціалізованого законодавчого акта – Закону України «Про публічно-приватне партнерство у сфері кібербезпеки», що встановить чіткі правові дефініції, інституційні форми співпраці, відповідальність, механізми фінансування та стимули для залучення бізнесу до виконання функцій із захисту кіберпростору.

Важливим кроком є також розроблення типових договорів публічно-приватного партнерства у сфері кібербезпеки, які могли б регламентувати розподіл зобов'язань, доступ до інфраструктури, обробку конфіденційної інформації, а також визначати механізми врегулювання конфліктів між сторонами.

Окремої уваги потребує питання спеціального статусу приватних фахівців у разі їх мобілізації до кіберрезерву України. На законодавчому рівні слід закріпити правовий статус учасників кіберрезерву, визначити порядок їх залучення, відповідальність, гарантії соціального захисту, обсяг доступу до конфіденційної інформації, а також передбачити механізми державного замовлення на послуги у сфері кібербезпеки. Для цього може бути внесено відповідні зміни до Закону «Про основні засади забезпечення кібербезпеки України».

Крім того, доцільним є створення спеціалізованої публічно – приватної координаційної платформи, наділеної консультативно-дорадчими функціями, яка б включала в себе представників публічної влади, приватного сектору та наукових установ, задля: спільного розроблення нормативно-правових актів, стандартів та регламентів у сфері кібербезпеки, наданні аналітичної підтримки органам державної влади та

сприяння в формуванні державної політики у сфері кібербезпеки; встановлення єдиних стандартів та уніфікованого механізму інформаційного обміну між державою та приватним сектором.

Не менш важливим є розширення участі представників приватного сектору в експертних дорадчих органах публічної влади, що сприятиме формуванню прозорої та інклюзивної політики у сфері національної кібербезпеки, що дозволить не лише залучити фаховий потенціал, а й формалізувати комунікацію між сектором безпеки й бізнесом.

На завершення варто зазначити, що в умовах триваючої агресії проти України, сучасний кіберзахист не може бути ефективним без повноцінного та законодавчо врегульованого партнерства між публічною владою та приватним сектором. Формування інтегрованої правової системи, що передбачатиме прозорі правила взаємодії, захист інтересів сторін і спільну відповідальність за безпеку в кіберпросторі, є ключовою умовою для забезпечення кіберстійкості України.

Майбутнє кібербезпеки України - це інтегрована система, де держава й бізнес не просто співпрацюють, а функціонують як єдиний цифровий організм у захисті національного інформаційного суверенітету.

Література

1. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 01.06.2025).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 27.05.2025).

3. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text (дата звернення: 29.05.2025).

4. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 02.06.2025).

5. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 7 березня 2025 р. № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (дата звернення: 03.06.2025).

6. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 27.05.2025).

7. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні: Аналітична записка Національного інституту стратегічних досліджень. URL: https://niss.gov.ua/sites/default/files/2017-12/kiberbezpek-d3e61.pdf (дата звернення: 01.06.2025).

8. Брошура Міжнародної фундації виборчих систем «Правова база української кібербезпеки: загальний огляд і аналіз». URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf (дата звернення: 02.06.2025).

9. Ландшафт кіберзагроз України у 2023 році: Дослідження Інституту дослідженнь кібервійни. URL:

https://ua.understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_3_ua.pdf (дата звернення: 04.06.2025).

10. *Державна служба спеціального зв'язку та захисту інформації України: державний сайт України*. URL: https://cip.gov.ua/ua/news (дата звернення: 28.05.2025).

11. Об'єднання IT-компаній IT Ukraine Association. URL: https://itukraine.org.ua/favbet-tech-priyednuyetsya-do-tsifrovoyi-armiyi-kiberpolk/ (дата звернення: 01.06.2025).

12. *Офіційний вебсайт Київського Міжнародного Форуму з Кібербезпеки 2025*. URL: https://cyberforumkyiv.org/ (дата звернення: 27.05.2025).

13. Українська спільнота розробників DOU.ua. URL: https://dou.ua/lenta/articles/aushev-about-cyber-unit/ (дата звернення: 31.06.2025).

14. Хмарний сервіс GigaCloud. URL: https://gigacloud.ua/news/ukrayinski-provajdery-predstavyly-alyans-czyfrovogo-suverenitetu/ (дата звернення: 31.06.2025).

15. Щоденна газета «Факти та коментарі». URL: https://fakty.ua/451563-tehnologii-protiv-kiberatak-glavnye-vyzovy-i-strategii-zacshity-na-kievskom-mezhdunarodnom-forume-po-kiberbezopasnosti (дата звернення: 29.05.2025).

References

1. Law of Ukraine "On the State Service for Special Communications and Information Protection of Ukraine" of February 23, 2006, No. 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (date of access: 01.06.2025).

2. Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" of October 5, 2017, No. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (date of access: 27.05.2025).

3. Law of Ukraine "On the National Security and Defense Council of Ukraine" of March 5, 1998, No. 183/98-VR. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text (date of access: 29.05.2025).

4. Presidential Decree of Ukraine "On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 'On the Cybersecurity Strategy of Ukraine'" of August 26, 2021, No. 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (date of access: 02.06.2025).

5. Order of the Cabinet of Ministers of Ukraine No. 204-p "On the Approval of the Action Plan for 2025 for the Implementation of the Cybersecurity Strategy of Ukraine" of March 7, 2025. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (date of access: 03.06.2025).

6. Convention on Cybercrime of November 23, 2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (date of access: 27.05.2025).

7. Analytical Note of the National Institute for Strategic Studies "Current Issues of Public-Private Cooperation Development in the Field of Cybersecurity in Ukraine". URL: https://niss.gov.ua/sites/default/files/2017-12/kiberbezpek-d3e61.pdf (date of access: 01.06.2025).

8. Brochure by the International Foundation for Electoral Systems "Legal Framework of Ukrainian Cybersecurity: General Overview and Analysis". URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf (date of access: 02.06.2025).

9. Research of the Institute for Cyber Warfare Studies "Ukraine's Cyber Threat Landscape in 2023". URL: https://ua.understandingcyberwar.org/wp-content/uploads/2024/09/Proekt_3_ua.pdf (date of access: 04.06.2025).

10. Official Website of Ukraine: State Service for Special Communications and Information Protection of Ukraine. URL: https://cip.gov.ua/ua/news (date of access: 28.05.2025).

11. IT Ukraine Association – Union of IT Companies. URL: https://itukraine.org.ua/favbet-tech-priyednuyetsya-do-tsifrovoyi-armiyi-kiberpolk/ (date of access: 01.06.2025).

12. Official Website of the Kyiv International Cybersecurity Forum 2025. URL: https://cyberforumkyiv.org/ (date of access: 27.05.2025).

13. Ukrainian Developer Community DOU.ua. URL: https://dou.ua/lenta/articles/aushev-about-cyber-unit/ (date of access: 31.06.2025).

14. GigaCloud Cloud Service. URL: https://gigacloud.ua/news/ukrayinski-provajdery-predstavyly-alyans-czyfrovogo-suverenitetu/ (date of access: 31.06.2025).

15. Daily Newspaper "Fakty ta Komentari". URL: https://fakty.ua/451563-tehnologii-protiv-kiberatak-glavnye-vyzovy-i-strategii-zacshity-na-kievskom-mezhdunarodnom-forume-po-kiberbezopasnosti (date of access: 29.05.2025).