УДК 342.95:004.056(477)

https://doi.org/10.52058/2786-6025-2025-11(52)-175-188

Костенко Інеса Володимирівна кандидат юридичних наук старший науковий співробітник Науково-дослідного інституту державного будівництва та місцевого самоврядування Національної академії правових наук України, https://orcid.org/0000-0002-8784-5422

Оксінь Віталій Юрійович доктор юридичних наук, професор, професор кафедри публічного управління, адміністрування та права Національного університету «Полтавська політехніка імені Юрія Кондратюка», https://orcid.org/0000-0001-6080-7752

Левченко Діана Сергіївна PhD в галузі право, старший викладач кафедри менеджменту та інноваційного розвитку Бізнес Школи КРОК, https://orcid.org/0000-0001-8343-2260

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ

Анотація. Статтю присвячено аналізу державно-приватного партнерства у сфері кібербезпеки як важливого інструмента зміцнення національної безпеки України в умовах зростання кіберзагроз і триваючої військової агресії. Підкреслено, що сучасний цифровий простір висуває нові вимоги до взаємодії держави й бізнесу, адже саме приватний сектор володіє значною частиною критичної цифрової інфраструктури, технологічними ресурсами та експертним потенціалом, необхідними для своєчасного реагування на кібератаки. Відзначено, що з 2022 року ефективність української моделі кіберзахисту значною мірою забезпечувалася завдяки узгодженим діям державних органів, ІТ-компаній, телекомунікаційних операторів, енергетичних і фінансових установ, що дозволило підтримати стабільність ключових цифрових сервісів попри масовані атаки.

У статті обґрунтовується, що розвиток державно-приватної взаємодії у кіберсфері потребує оновлення адміністративно-правових підходів, які регламентують обмін інформацією, порядок спільного реагування на інциденти, механізми відповідальності суб'єктів критичної інфраструктури та засади довгострокової координації між державою й бізнесом. Показано, що українська система дедалі активніше інтегрується у європейський та

євроатлантичний простір кібербезпеки, спираючись на вимоги Директиви Європейського Союзу NIS2 (Network and Information Security Directive 2), рекомендації Агентства Європейського Союзу з кібербезпеки (European Union Agency for Cybersecurity, ENISA), практики Агентства з кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency, CISA) та підходи Організації Північноатлантичного договору (North Atlantic Treaty Organization, НАТО), які акцентують необхідність ризик-орієнтованого управління та партнерської моделі захисту. Наголошено, що подальше зміцнення взаємодії потребує оновлення законодавства, посилення спроможності Національного координаційного центру кібербезпеки (НКЦК), розбудови галузевих платформ обміну інформацією ISAC (Information Sharing and Analysis Centers) та формування високого рівня довіри між сторонами.

Зроблено висновок, що державно-приватне партнерство у сфері кібербезпеки набуває статусу стратегічного ресурсу держави, який визначає її здатність забезпечувати кіберстійкість, протидіяти загрозам та гарантувати безперервність функціонування критичної інфраструктури. Воно стає фундаментальною опорою цифрового суверенітету України та важливою умовою її стійкості у складному безпековому середовищі.

Ключові слова: кібербезпека, національна безпека, державно-приватне партнерство, публічно-приватна взаємодія, критична інфраструктура, кіберстійкість, кібератаки.

Kostenko Inesa Ph.D. in Law, Researcher at the Research Institute of State Building and Local Self-Government of the National Academy of Legal Sciences of Ukraine, https://orcid.org/0000-0002-8784-5422

Oksin Vitaliy Doctor of Law,Professor, Professor of the Department of Public Management, Administration and Law of the National University "Poltava Polytechnic named after Yuriy Kondratyuk", https://orcid.org/0000-0001-6080-7752

Levchenko Diana Ph.D. in Law, Senior Lecturer, Department of Management and Innovative Development, Higher Educational Institution "University of Economics and Law "KROK",https://orcid.org/0000-0001-8343-2260

PUBLIC–PRIVATE PARTNERSHIP IN THE FIELD OF CYBERSECURITY AS A TOOL FOR ENSURING NATIONAL SECURITY: AN ADMINISTRATIVE AND LEGAL ASPECT

Abstract. The article examines public–private partnership in the field of cybersecurity as a significant mechanism for strengthening Ukraine’s national

security in the context of escalating cyber threats and the ongoing armed aggression. It is emphasised that the modern digital environment imposes new requirements on the interaction between the state and the private sector, as the latter owns a substantial share of critical digital infrastructure, technological resources and expert capabilities essential for timely response to cyberattacks. It is noted that since 2022 the effectiveness of Ukraine's cybersecurity model has largely depended on coordinated actions of public authorities, IT companies, telecommunications operators, and energy and financial institutions, which made it possible to maintain the resilience of key digital services despite large-scale attacks.

The article argues that the development of public–private cooperation in the cyber domain requires renewed administrative and legal approaches regulating the exchange of information on cyber incidents, procedures for coordinated response, liability mechanisms for operators of critical infrastructure, and sustainable channels of communication between the state and private actors. It is demonstrated that Ukraine's cybersecurity system is increasingly integrating into the European and Euro-Atlantic security space, relying on the requirements of the European Union's NIS2 Directive (Network and Information Security Directive 2), the recommendations of the European Union Agency for Cybersecurity (ENISA), the practices of the United States Cybersecurity and Infrastructure Security Agency (CISA), and the approaches of the North Atlantic Treaty Organization (NATO), all of which underline the importance of risk-based governance and a partnership-oriented security model. It is emphasised that further consolidation of this cooperation requires legislative modernisation, institutional strengthening of the National Cybersecurity Coordination Centre (NCCC), the development of sectoral Information Sharing and Analysis Centres (ISACs), and the cultivation of a high level of trust between the parties.

It is concluded that public–private partnership in the field of cybersecurity is becoming a strategic asset of the state, determining its ability to ensure cyber resilience, counter threats, and maintain the continuity of critical infrastructure operations. It constitutes a fundamental pillar of Ukraine's digital sovereignty and a key precondition for its stability in an increasingly challenging security environment.

Keywords: cybersecurity, national security, public–private partnership, public–private cooperation, critical infrastructure, cyber resilience, cyberattacks.

Постановка проблеми. Стрімке ускладнення кіберзагроз та їх інтеграція у воєнно-політичні стратегії держав актуалізували державно-приватне партнерство (ДПП) як ключовий інструмент забезпечення кіберстійкості й національної безпеки. Український та міжнародний досвід послідовно демонструє, що саме синергія державних інституцій і приватного сектора визначає здатність держави протидіяти багатовекторним кібератакам,

забезпечувати безперервність функціонування критичної інфраструктури та впроваджувати ризик-орієнтовані моделі управління у сфері кіберзахисту [1; 2; 6].

Аналітичні дослідження національних та зарубіжних авторів підтверджують: ефективна система ДПП у кібербезпеці не обмежується залученням технічних спроможностей бізнесу, а охоплює нормативно-правові механізми взаємодії, моделі обміну інформацією, інституційні формати спільного реагування на інциденти та стандарти організації кіберзахисту на рівні критичної інфраструктури [1; 3; 4; 7]. В умовах повномасштабної війни Україні особливо значущими є сталі канали обміну оперативною інформацією, участь приватних компаній у виявленні та нейтралізації загроз, а також розбудова партнерських механізмів, що довели свою ефективність у країнах ЄС, США та НАТО [5; 9; 11; 12].

Міжнародні структури виробили комплексні моделі участі приватного сектору у забезпеченні кібербезпеки: рекомендації OECD щодо належного врядування у сфері ДПП [10], програми стратегічної взаємодії з індустрією (NATO Industry Cyber Partnership) [11], багатосторонні платформи координації та обміну даними на кшталт Joint Cyber Defense Collaborative у США [12], а також законодавчі рамки кіберінформаційного обміну, визначені Cybersecurity Information Sharing Act of 2015 [13]. У свою чергу, ENISA напрацьовує нормативні та організаційні стандарти для формування дієвих національних ДПП-моделей, зокрема щодо їх інституційного дизайну, ролей учасників та механізмів реагування [9]. Практичні механізми залучення експертів приватного сектору, на кшталт британської програми NCSC “Industry 100” (i100), підтверджують ефективність інтеграції бізнес-компетенцій у державні процеси кіберзахисту [15].

Україна поступово кодифікує правові основи державно-приватної взаємодії у сфері кібербезпеки. Проєкт Закону «Про державно-приватну взаємодію у сфері кібербезпеки» формує нормативну рамку, що спрямована на інституціоналізацію партнерських механізмів, врегулювання обміну інформацією та узгодження процедур реагування з урахуванням міжнародних стандартів [8]. Наукові дослідження також наголошують на потребі модернізації адміністративно-правових процедур, підвищенні правової визначеності щодо ролі приватного сектору, спрощенні регуляторних бар’єрів та формалізації участі бізнесу в національній системі кіберзахисту [2; 6; 7].

Отже, сучасний стан безпекового середовища вимагає концептуального оновлення адміністративно-правових засад ДПП у сфері кібербезпеки — від правового статусу суб’єктів і процедур координації до режимів обміну інформацією та інституційної підзвітності. Аналіз міжнародних практик та українського досвіду дозволяє сформувати комплексне бачення того, як

державно-приватне партнерство може стати системним інструментом посилення кіберстійкості держави, зокрема в умовах воєнних загроз.

Аналіз останніх досліджень і публікацій. Проблематика державно-приватного партнерства (ДПП) у сфері кібербезпеки поступово посідає помітне місце в сучасній українській науці, де вона розглядається у контексті публічного управління, національної безпеки та правового регулювання інформаційних відносин. Вагомий внесок у формування наукових підходів до ДПП у кіберпросторі зробили вітчизняні дослідники, які висвітлили як загально-теоретичні засади, так і практичні аспекти впровадження відповідних механізмів.

Одним із перших комплексних національних досліджень стала аналітична доповідь НІСД під загальною редакцією Д. Дубова, у якій узагальнено міжнародний досвід державно-приватної взаємодії у сфері кібербезпеки, окреслено ключові виклики для України та запропоновано можливі напрями розбудови партнерських моделей [1]. Подальший розвиток тематики відображено в працях С. Гнатюка, який аналізує актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки України та окреслює основні проблеми і напрями її вдосконалення [2]. Дослідження В. Григоренка зосереджене на найкращих зарубіжних практиках розбудови механізмів ДПП у сфері кібербезпеки й можливостях їх використання в українських умовах [3], тоді як Ю. Заскока розглядає сучасний стан ДПП у сфері кібербезпеки України та виокремлює характерні проблеми його забезпечення [4].

У контексті безпекових викликів, пов’язаних з повномасштабним вторгненням, важливими є висновки О. Дідича та О. Наумка, які аналізують роль державно-приватного партнерства в системі забезпечення національної безпеки держави в умовах воєнної агресії [5]. Б. Панасюк досліджує сучасний стан державно-приватного партнерства у сфері кібербезпеки, приділяючи увагу особливостям українського досвіду й наявним тенденціям розвитку цієї взаємодії [6]. Правові аспекти взаємодії державних органів та приватних суб’єктів із метою захисту електронних інформаційних ресурсів України, зокрема нормативні засади та форми такої співпраці, розкрито в роботах С. Петрова [7].

На нормативному рівні важливим орієнтиром для подальшого розвитку ДПП у сфері кібербезпеки є проєкт Закону України «Про державно-приватну взаємодію у сфері кібербезпеки», який спрямований на формування правових рамок інституціоналізації партнерства, визначення суб’єктного складу та загальних правил взаємодії між державними органами й приватним сектором [8]. Проте, попри значний масив теоретичних і прикладних напрацювань, а також активну розробку нормативної бази, низка концептуальних аспектів державно-приватного партнерства у сфері кібербезпеки й надалі потребує

поглибленого наукового аналізу. Ідеться, зокрема, про уточнення меж і змісту повноважень учасників взаємодії, визначення оптимальних правових режимів обміну інформацією, узгодження процедур спільного реагування на кібер-інциденти, а також про формалізацію участі приватного сектору у захисті критичної інфраструктури в умовах зростаючих кіберзагроз. Додаткового опрацювання потребують питання інтеграції національного законодавства з міжнародними підходами та рекомендаціями, що формуються в межах діяльності ENISA, OECD, НАТО та інших міжнародних акторів, а також практиками, які демонструють високу результативність у країнах-партнерах. Саме ці аспекти залишаються відкритими і визначають подальший напрям розвитку адміністративно-правового регулювання державно-приватного партнерства у сфері кібербезпеки.

Метою дослідження є комплексний аналіз адміністративно-правових засад державно-приватного партнерства у сфері кібербезпеки та визначення напрямів удосконалення національної моделі взаємодії держави й приватного сектору з урахуванням міжнародних стандартів і сучасних безпекових викликів.

Виклад основного матеріалу. Державно-приватне партнерство у сфері кібербезпеки посідає проміжне місце між традиційними механізмами публічного адміністрування та новітніми моделями взаємодії у цифровому середовищі. На відміну від класичних інфраструктурних проєктів, де домінує передання об'єктів чи фінансових ризиків, у кіберпросторі партнерство концентрується на спільному виконанні функцій, безпосередньо пов'язаних із забезпеченням національної безпеки та стійкості критичних процесів. У відповідних дослідженнях підкреслюється, що визначальними рисами такого ДПП є інституційно закріплений обмін інформацією про кіберзагрози, розмежування повноважень і відповідальності сторін, узгодженість процедур реагування на інциденти та наявність постійних каналів координації між державними органами й приватними суб'єктами [1; 2; 7].

У структурі національної системи кібербезпеки ДПП розглядається як механізм, що дозволяє залучити експертний, технологічний та організаційний потенціал приватного сектору до виконання завдань, які традиційно сприймалися як прерогатива публічної влади.

У роботах вітчизняних авторів увага акцентується на тому, що партнерство в кібербезпеці має будуватися не лише на договірних конструкціях, а й на поєднанні адміністративно-правового регулювання з процедурними й технічними стандартами, які забезпечують оперативність прийняття рішень в умовах динамічного загрозового середовища [1–4; 6]. З цієї точки зору ДПП виступає елементом системи публічного управління, що забезпечує інтеграцію приватних акторів у загальну архітектоніку національної безпеки, зокрема у воєнний період [5].

Міжнародний досвід демонструє, що результативні моделі державно-приватної взаємодії в кібербезпеці формуються за наявності чітко визначених правових рамок і стабільних організаційних форматів співпраці. У документах ENISA публічно-приватні партнерства характеризуються як необхідна умова безпеки та стійкості критичної інформаційної інфраструктури, з урахуванням того, що значна частина відповідних ресурсів перебуває у власності приватних суб'єктів; при цьому особливий акцент робиться на тривалому характері співпраці та інституційній формалізації обміну інформацією [9]. Рекомендації OECD щодо публічного врядування ДПП підкреслюють важливість прозорості, підзвітності та збалансованого розподілу ризиків між учасниками, що створює методологічну основу для належного правового оформлення партнерських моделей у різних сферах, включно з кібербезпекою [10]. У межах євро-атлантичного простору ініціатива NATO Industry Cyber Partnership покликана забезпечити більш тісну взаємодію Альянсу з індустрією в питаннях кібероборони та обміну інформацією, тоді як у США створення Joint Cyber Defense Collaborative при CISA відображає перехід до більш операційно-орієнтованих форматів спільного планування та реагування за участю державних органів і технологічних компаній [11–13].

З огляду на ці тенденції державно-приватне партнерство у сфері кібербезпеки доцільно розглядати як невід'ємний структурний компонент системи національної кібербезпеки України, потенціал якого виходить за межі суто договірних відносин. Його зміст охоплює спільне управління ризиками, інституційно оформлений обмін інформацією, участь приватного сектору у процесах виявлення, попередження та локалізації кіберінцидентів, а також залучення бізнесу до розбудови стійкості критичної інфраструктури. Водночас наявні дослідження й нормативні ініціативи свідчать, що українська модель ДПП у кібербезпеці перебуває на стадії становлення: окремі елементи взаємодії вже функціонують, однак комплексна адміністративно-правова конструкція, яка б забезпечувала системність та передбачуваність цієї взаємодії, ще потребує подальшого доктринального опрацювання і законодавчого закріплення [4–8].

Проєкт Закону України «Про державно-приватну взаємодію у сфері кібербезпеки» є спробою кодифікувати спеціальний режим співпраці державних і приватних суб'єктів саме у сфері кібербезпеки та чітко відмежувати його від класичних інфраструктурних моделей державно-приватного партнерства. У статті 2 законопроєкту визначено, що його метою є впорядкування та розвиток такої взаємодії, зміцнення довіри, побудова сталих комунікацій і координації дій, консолідація зусиль у забезпеченні кібербезпеки, посилення спроможностей національної системи кібербезпеки, функціонування організаційно-технічної моделі кіберзахисту та стимулювання інновацій і розвитку національного ринку кіберпродуктів і послуг [8]. Водночас прямо встановлено,

що цей спеціальний режим не застосовується до відносин, пов'язаних із фінансуванням, створенням, будівництвом та технічним обслуговуванням майна з передачею відповідних ризиків приватному партнеру, для яких передбачені інші правові інструменти [8]. Такий підхід загалом узгоджується з позицією, висловленою в аналітичній доповіді НІСД, де підкреслюється відмінність між інвестиційно-інфраструктурними ДПП і функціональною взаємодією у сфері кібербезпеки [1].

Важливою новелою законопроєкту є розбудований категоріальний апарат, орієнтований саме на кіберсферу. У статті 1 дано визначення «державного учасника» як широкого кола органів публічної влади, державних підприємств, установ, господарських товариств із державною участю, наукових установ та органів місцевого самоврядування, які реалізують завдання у сфері державно-приватної взаємодії в кібербезпеці [8]. «Приватний учасник» трактується як будь-яка юридична або фізична особа — резидент чи нерезидент України, що має намір співпрацювати або співпрацює з державним учасником у межах цього закону [8]. Окремо інституціоналізовано поняття «проекту» та «проекту за нагальною потребою (ad hoc)», а також «третьої особи», яка залучається для допоміжних функцій [8]. Така конструкція фактично закріплює багаторівневу конфігурацію суб'єктів державно-приватної взаємодії, про необхідність якої раніше говорилося у наукових працях, присвячених залученню бізнесу, наукової спільноти та міжнародних партнерів до забезпечення кібербезпеки України [2; 3; 5; 6].

Нормативний зміст державно-приватної взаємодії конкретизується через систему принципів, напрямів, форм, методів та умов її здійснення. У статті 3 законопроєкту закріплено принципи рівності можливостей і недискримінації приватних учасників, юридичної рівності державного і приватного учасника, орієнтації на досягнення конкретних завдань у сфері кібербезпеки, добровільності участі приватних суб'єктів та стимулювання розвитку конкурентоспроможного національного ринку кіберпослуг [8]. Стаття 4 подає розгорнутий перелік напрямів взаємодії: обмін інформацією про кіберінциденти, кібератаки, кіберзагрози та заходи кіберзахисту; моніторинг систем і об'єктів критичної інформаційної інфраструктури, атрибуція, реагування та відновлення; виявлення вразливостей (включно з можливістю винагороди за їх виявлення); розроблення методичних матеріалів, протоколів та шаблонів; участь у формуванні політики, підготовці нормативних актів, стандартів та рекомендацій; консультативна допомога; дослідження й експериментальні розробки; тренінги, освіта, підвищення кваліфікації та атестація; створення й розвиток центрів реагування, аналітичних та інноваційних центрів; розбудова інфраструктури кіберзахисту; виконання завдань кібероборони, кіберрозвідки й активної протидії агресії у кіберпросторі; програми

стимулювання розвитку національного ринку продуктів і послуг у сфері кібербезпеки [8]. Така багатовекторність загалом співзвучна тим функціональним блокам, які ENISA виділяє як ключові при описі публічно-приватних партнерств у кібербезпеці [9].

Стаття 5 законопроєкту деталізує завдання та повноваження державних учасників. Для органів державної влади, інших державних органів та органів місцевого самоврядування передбачено обов'язок планувати діяльність у сфері державно-приватної взаємодії шляхом прийняття документів програмно-цільового характеру, забезпечувати комунікацію з потенційними приватними учасниками на всіх етапах проектів, створювати нормативні, організаційні та технологічні умови реалізації взаємодії, здійснювати оцінку ефективності проектів та узагальнювати практику [8]. Аналогічні завдання, з урахуванням їх статусу, покладаються на інші державні учасники (державні підприємства, установи, господарські товариства тощо) [8]. Законопроєкт також фіксує повноваження щодо розроблення програмно-цільових документів із визначенням напрямів, очікуваних результатів, критеріїв відбору приватних учасників, форм та методів взаємодії, а також щодо укладення договорів, меморандумів, протоколів та прийняття актів про умови приєднання до проектів [8]. У наукових працях підкреслюється, що саме недостатня визначеність таких процедур у попередній практиці була одним із чинників фрагментарності співпраці держави та бізнесу в кіберсфері [2; 4; 7], тож відповідні положення законопроєкту можна оцінювати як крок до їх інституціоналізації.

Форми, методи та умови державно-приватної взаємодії визначені у статтях 7–8 законопроєкту. Передбачено три основні форми реалізації проектів: договори й інші правочини; протоколи, меморандуми та подібні документи, що не спрямовані на встановлення або зміну цивільних прав та обов'язків; умови приєднання, які є однаковими для всіх приватних учасників і затверджуються актом державного учасника [8]. Методи взаємодії розуміються як конкретні інструменти та механізми в межах обраної форми, що не заборонені законодавством [8]. Умови проекту повинні охоплювати, зокрема, предмет і очікувані результати, розподіл функцій і обов'язків між державним, приватним учасником і, за потреби, третіми особами, порядок обробки інформації, строки, режим користування результатами, у тому числі майнові права інтелектуальної власності [8]. Особливої уваги заслуговує вимога, за якої у разі створення в межах проекту продукту у сфері кібербезпеки, призначеного для застосування державними учасниками, умови проекту мають забезпечувати державному учаснику право використання відповідних об'єктів та право дозволяти їх використання іншим особам у необхідному обсязі [8]. Така деталізація прав інтелектуальної власності кореспондує з рекомендаціями OECD щодо прозорого розподілу ризиків і вигод у ДПП [10] та з висновками К. Айхенсер

щодо важливості чіткої регламентації ролей і прав сторін у публічно-приватних моделях кібербезпеки [14].

Стаття 6 законопроєкту встановлює загальне правило конкурентного відбору приватних учасників, якщо проект передбачає залучення обмеженої кількості таких осіб, із віднесенням деталізації процедури та підстав неконкурентного відбору до компетенції Кабінету Міністрів України [8]. Водночас прямо передбачено, що конкурентна процедура не застосовується для проектів за нагальною потребою та в інших випадках, визначених законодавством [8]. Також окреслено коло осіб, які не допускаються до участі: суб'єкти, щодо яких відкрито процедури банкрутства чи ліквідації, які не мають необхідних реєстраційних відомостей, пов'язані з державами-агресорами, а також особи, щодо яких застосовані санкції [8]. Ці обмеження відображають прагнення поєднати відкритість доступу до участі в проектах із базовими безпековими запобіжниками, на що звертають увагу й українські дослідники, аналізуючи ризики участі у критичних процесах суб'єктів із сумнівною юрисдикційною прив'язкою [3; 6]. Разом з тим передача ключових елементів конкурсної процедури на рівень підзаконного регулювання залишає відкритими питання прозорості та уніфікованості практики відбору.

Важливе місце в законопроєкті посідають гарантії прав приватних учасників та режим обробки інформації (статті 9–11). Приватний суб'єкт може ініціювати проект шляхом подання пропозиції державному учаснику, який зобов'язаний розглянути її в установлені строки та надати мотивовану відповідь щодо доцільності реалізації [8]. Гарантії включають, зокрема, заборону використання інформації, отриманої від приватного учасника в межах проекту, для ініціювання заходів державного нагляду (контролю), встановлення порушень або застосування санкцій, за винятком випадків вчинення кримінальних правопорушень чи виконання прямого обов'язку надання інформації за законом [8]. Інформація, одержана від приватного учасника, визнається конфіденційною; порядок і цілі її обробки мають визначатися умовами проекту, а сторони зобов'язані забезпечити захист інформації та несуть відповідальність за порушення встановленого режиму [8]. Така конструкція загалом відповідає тенденції, яку демонструє Cybersecurity Information Sharing Act of 2015, спрямований на створення стимулів до обміну інформацією про кіберзагрози без ризику її використання проти самого надавача [13], і корелює з підходами ENISA та CISA до формування довірчого правового середовища для публічно-приватного інформаційного обміну [9; 12].

У сукупності положення законопроєкту [8] свідчать про спробу наблизити національний режим державно-приватної взаємодії у сфері кібербезпеки до структурно оформлених моделей, описаних у європейських та євроатлантичних документах і практиках [1; 3; 9–12; 15].

Водночас у науковій площині залишаються відкритими питання мінімального обсягу імперативних обов'язків приватних учасників щодо повідомлення про інциденти, транскордонних аспектів співпраці, критеріїв оцінювання ефективності проектів, процедурної деталізації конкурсного відбору та інтеграції державно-приватної взаємодії у загальну систему публічного управління кібербезпекою [2; 4–7; 14].

Практична реалізація державно-приватного партнерства у сфері кібербезпеки в Україні формується під впливом як внутрішніх безпекових викликів, так і зовнішніх зобов'язань держави. У працях вітчизняних авторів наголошується, що співпраця державних органів з IT-компаніями, операторами зв'язку, фінансовими установами та іншими суб'єктами бізнесу істотно посилилася після 2014 року і набула особливого значення в період повномасштабного вторгнення, коли від швидкості спільних дій залежала стійкість критичної інфраструктури та безперервність надання послуг [1; 2; 5; 6].

Водночас підкреслюється, що значна частина таких форм взаємодії має характер тимчасових домовленостей, меморандумів про співпрацю чи галузевих ініціатив, які не завжди спираються на уніфіковані адміністративно-правові процедури та чітко визначений статус учасників [3; 4; 7]. Це обмежує можливість перетворення окремих успішних практик на стійку національну модель державно-приватної взаємодії у кіберсфері.

Проєкт Закону України «Про державно-приватну взаємодію у сфері кібербезпеки» покликаний інституціоналізувати вже наявні форми співпраці, надаючи їм чітко окреслені правові рамки. Його положення про напрями взаємодії, форми реалізації проектів, права приватних учасників та гарантії захисту інформації, отриманої в межах співпраці, фактично відображають спробу закріпити на законодавчому рівні ті механізми, які, за спостереженнями дослідників, уже функціонують у практиці взаємодії держави й бізнесу, але не мають належної правової визначеності [2; 5–8]. Одночасно дослідження вказують на те, що без належних процедур оцінювання ефективності проектів, прозорих критеріїв відбору приватних учасників та узгоджених стандартів обміну інформацією ризик фрагментарності й надалі зберігатиметься [4; 6; 7].

Міжнародні моделі публічно-приватної взаємодії у кібербезпеці демонструють більш високий рівень інституційної оформленості. ENISA узагальнює практику створення національних платформ партнерства, орієнтованих на постійний обмін інформацією, спільну оцінку ризиків та участь приватного сектору у формуванні політики [9]. Рекомендації OECD щодо врядування публічно-приватними партнерствами акцентують на прозорості, підзвітності та збалансованому розподілі ризиків, що важливо для ефективної організації довгострокової взаємодії [10]. У межах НАТО ініціатива NATO Industry Cyber Partnership спрямована на системну взаємодію з промисловими партнерами в

питаннях кібероборони [11], тоді як створення Joint Cyber Defense Collaborative при CISA і правове регулювання обміну інформацією у Cybersecurity Information Sharing Act of 2015 ілюструють можливість поєднання багатосторонньої платформи співпраці з чіткими гарантіями для приватних учасників [12; 13]. Концептуальний аналіз К. Айхенсер показує, що в таких моделях приватні компанії дедалі активніше виконують функції з виявлення, стримування й атрибуції кібератак, що потребує додаткових механізмів легітимації та публічної підзвітності спільних рішень [14]. Показовою у цьому контексті є також британська програма NCSC “Industry 100”, яка забезпечує структуроване залучення експертів приватного сектору до діяльності державних органів кіберзахисту [15]. З урахуванням воєнного досвіду України та зазначених міжнародних напрацювань напрями вдосконалення практико-інституційної моделі державно-приватного партнерства у сфері кібербезпеки можуть бути сформульовані у кількох вимірах. По-перше, доцільним є подальше розгортання механізмів, закладених у проєкті закону, з перетворенням їх на дієві процедури відбору приватних учасників, укладення проектів, обробки інформації й оцінювання результативності співпраці [6–8]. По-друге, потребує розвитку інфраструктура сталого інформаційного обміну, включно з галузевими та міжгалузевими платформами, здатними працювати в режимі підвищеної загрозової напруги. По-третє, важливою є адаптація елементів європейських та євроатлантичних моделей — зокрема принципів ризик-орієнтованого управління, практики спільного планування оборонних заходів та залучення приватних експертів до роботи профільних органів кібербезпеки — до українських реалій [1; 3; 9–12; 15]. Саме в цьому площині державно-приватне партнерство у кіберсфері поступово набуває рис не лише інструмента реагування на окремі інциденти, а й стратегічного ресурсу, що визначає рівень кіберстійкості та національної безпеки держави.

Висновки. Проведене дослідження підтверджує, що державно-приватне партнерство є невід’ємним елементом сучасної системи забезпечення кібербезпеки України. Аналіз наукових джерел, нормативних актів і міжнародних практик засвідчує, що ефективність такої взаємодії визначається не лише технологічними спроможностями приватного сектору, а й чіткими адміністративно-правовими механізмами, які регламентують обмін інформацією, розподіл повноважень і спільне реагування на інциденти. Українська модель ДПП перебуває у фазі активного розвитку, однак потребує подальшої інституціоналізації, узгодження процедур із міжнародними стандартами та формалізації участі бізнесу у захисті критичної інфраструктури. Удосконалення правових та організаційних підходів до державно-приватного партнерства стане важливим чинником зміцнення кіберстійкості держави й підвищення результативності національної системи кібербезпеки в умовах воєнних і поствоєнних викликів.

Література:

1. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналітична доповідь [Електронний ресурс] / за заг. ред. Д. Дубова. – Київ: НІСД, 2018. – 84 с. – Режим доступу: https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf

2. Гнатюк С. Л. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні : аналітична записка [Електронний ресурс]. – Київ: Національний інститут стратегічних досліджень, 2017. – Режим доступу: https://niss.gov.ua/sites/default/files/2017-12/kiberbezpek-d3e61.pdf.

3. Григоренко В. А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки [Електронний ресурс] // Державне управління: удосконалення та розвиток. – 2021. – № 2 (37). – С. 155–161. – Режим доступу: https://doi.org/10.37750/2616-6798.2021.2(37).238405

4. Заскока Ю. В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення [Електронний ресурс] // Наукові перспективи. – 2021. – № 9 (21). – С. 85–98. – Режим доступу: http://perspectives.pp.ua/index.php/np/article/view/467/470

5. Дідич О. Р., Наумко О. М. Державно-приватне партнерство у забезпеченні національної безпеки в умовах повномасштабного вторгнення [Електронний ресурс] // Публічне адміністрування та національна безпека. – 2023. – № 2. – С. 118–123. – Режим доступу: https://www.pubadm.vernadskyjournals.in.ua/journals/2023/2_2023/20.pdf

6. Панасюк Б. М. Сучасний стан державно-приватного партнерства у сфері кібербезпеки: досвід України [Електронний ресурс] // Інформаційна безпека людини, суспільства, держави. – 2025. – № 1 (38). – С. 42–51. – Режим доступу: https://journals.uran.ua/ispss/article/view/340013/328076

7. Петров С. Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України / С. Г. Петров // Інформація і право. – 2019. – № 4 (31). – С. 107–113.

8. Проєкт Закону України «Про державно-приватну взаємодію у сфері кібербезпеки» [Електронний ресурс] // Верховна Рада України. – 2025. – Режим доступу: https://itd.rada.gov.ua/billinfo/Bills/Card/58279

9. ENISA. Public-Private Partnerships in Cyber Security: Recommendations and Best Practices [Електронний ресурс]. – 2024. – Режим доступу:https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/public-private

10. OECD. Recommendation of the Council on Principles for Public Governance of Public-Private Partnerships [Електронний ресурс]. – 2025. – Режим доступу:https://ppp.worldbank.org/library/oecd-public-governance-public-private-partnerships

11. NATO. NATO Industry Cyber Partnership Launched at the NATO Cyber Defence Conference [Електронний ресурс]. – 2014. – Режим доступу:https://www.nato.int/cps/en/natohq/news_113121.htm

12. Cybersecurity and Infrastructure Security Agency (CISA). Joint Cyber Defense Collaborative: Unifying Cyber Defense Planning and Operations [Електронний ресурс]. – 2021. – Режим доступу:https://nsarchive.gwu.edu/sites/default/files/documents/qytieo-agiyf/04.pdf

13. United States Congress. Cybersecurity Information Sharing Act of 2015 (CISA), Public Law 114–113, Division N, §104, 129 Stat. 2242. – Режим доступу: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

14. Eichensehr K. E. Public-Private Cybersecurity [Електронний ресурс] // Texas Law Review. – 2017. – Т. 95, № 2. – С. 467–522. – Режим доступу: https://texaslawreview.org/public-private-cybersecurity

15. National Cyber Security Centre (NCSC). Industry 100 Programme (i100). – [Електронний ресурс]. – 2023. – https://www.ncsc.gov.uk/section/industry-100/about

References:

1. Dubov, D. (Ed.). (2018). *Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy: analytychna dopovid* [Public-private partnership in cybersecurity: International experience and opportunities for Ukraine: Analytical report]. Kyiv: NISD. Retrieved from https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf [in Ukrainian].

2. Hnatiuk, S. L. (2017). Aktualni pytannia rozvytku derzhavno-pryvatnoi vzaiemodii u sferi zabezpechennia kiberbezpeky v Ukraini: Analytychna zapyska

[Current issues in the development of public-private cooperation in ensuring cybersecurity in Ukraine: Analytical note]. *Kyiv: Natsionalnyi instytut stratehichnykh doslidzhen.* Retrieved from https://niss.gov.ua/sites/default/files/2017-12/kiberbezpek-d3e61.pdf [in Ukrainian].

3. Hryhorenko, V. A. (2021). Naikrashchi zarubizhni praktyky rozbudovy mekhanizmiv derzhavno-pryvatnoho partnerstva u sferi kiberbezpeky [Best foreign practices for building mechanisms of public-private partnership in cybersecurity]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok – Public Administration: Improvement and Development, 2*(37), 155–161. Retrieved from https://doi.org/10.37750/2616-6798.2021.2(37).238405 [in Ukrainian].

4. Zaskoka, Yu. V. (2021). Derzhavno-pryvatne partnerstvo v sferi kiberbezpeky Ukrainy: stan ta problemy zabezpechennia [Public-private partnership in Ukraine's cybersecurity: State and challenges]. *Naukovi perspektyvy – Scientific Perspectives, 9*(21), 85–98. Retrieved from http://perspectives.pp.ua/index.php/np/article/view/467/470 [in Ukrainian].

5. Didych, O. R., & Naumko, O. M. (2023). Derzhavno-pryvatne partnerstvo u zabezpechenni natsionalnoi bezpeky v umovakh povnomasshtabnoho vtorhnennia [Public-private partnership in ensuring national security under full-scale invasion]. *Publichne administruvannia ta natsionalna bezpeka – Public Administration and National Security, 2*, 118–123. Retrieved from https://www.pubadm.vernadskyjournals.in.ua/journals/2023/2_2023/20.pdf [in Ukrainian].

6. Panasiuk, B. M. (2025). Suchasnyi stan derzhavno-pryvatnoho partnerstva u sferi kiberbezpeky: dosvid Ukrainy [Current state of public-private partnership in the field of cybersecurity: Experience of Ukraine]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy – Information Security of the Person, Society and the State, 1*(38), 42–51. Retrieved from https://journals.uran.ua/ispss/article/view/340013/328076 [in Ukrainian].

7. Petrov, S. H. (2019). Pravovi osnovy vzaiemodii derzhavnykh orhaniv ta pryvatnykh subiektiv iz metoiu zakhystu elektronnykh informatsiinykh resursiv Ukrainy [Legal foundations of interaction between state bodies and private entities for protecting electronic information resources of Ukraine]. *Informatsiia i pravo – Information and Law, 4*(31), 107–113 [in Ukrainian].

8. Proekt Zakonu Ukrainy «Pro derzhavno-pryvatnu vzaiemodiiu u sferi kiberbezpeky» [Draft Law of Ukraine "On public-private cooperation in the field of cybersecurity"]. (2025). *Verkhovna Rada Ukrainy – Verkhovna Rada of Ukraine.* Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/58279 [in Ukrainian].