DOI: 10.51369/2707-7276-2025-1(38)-4
УДК 044.946.5.056

*ПАНАСЮК Тетяна Іванівна*
ORCID ID: 0009-0005-9416-5424

*ПЕТРЕНКО Світлана Володимирівна*
ORCID ID: 0000-0003-1219-2401

# СУЧАСНИЙ СТАН ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ: ДОСВІД УКРАЇНИ

У статті досліджено питання сучасного стану розвитку інституту державно-приватного партнерства (ДПП) та державно-приватної взаємодії (ДПВ) у сфері кібербезпеки в Україні. Проаналізовано нормативно-правові акти, які регулюють ці питання, зокрема закони України «Про державно-приватне партнерство» та «Про основні засади забезпечення кібербезпеки України». Вивчення норм зазначених законів і наукових публікацій за вказаною темою свідчить, що наразі поняття ДПП та ДПВ можна ототожнювати, оскільки як партнерство, так і взаємодія проявляються у спільній діяльності, спрямованій на досягнення визначеної мети. Крім того, чинні нормативні документи визначають однакові форми ДПП та ДПВ: обмін інформацією про інциденти кібербезпеки, реалізацію спільних наукових і дослідницьких проєктів, навчання та підвищення кваліфікації кадрів у цій сфері.

На підставі аналізу основних стратегічних документів України з питань забезпечення національної безпеки обґрунтовано, що одним із шляхів зміцнення системи кібербезпеки є застосування ДПП у цій сфері.

Особливу увагу зосереджено на дослідженні форм залучення фахівців приватного сектору з кібербезпеки до співпраці з державними органами. Ураховуючи сучасний досвід залучення фахівців приватного сектору шляхом прийняття на військову службу до відповідних інституцій безпеки й оборони або на посаду державної служби на підставі укладеного трудового договору, у статті пропонується розглянути альтернативні варіанти співпраці.

Проаналізовано досвід взаємодії державного та приватного секторів у сфері кібербезпеки протягом останніх років, зокрема щодо обміну інформацією про інциденти кібербезпеки через Національний кластер кібербезпеки, платформу MISP-UA, а також урядову команду України з реагування на комп'ютерні інциденти CERT-UA. З урахуванням активної діяльності державного та приватного секторів в аспекті навчання, підвищення кваліфікації фахівців визначено результативні кроки в напрямі виконання державного завдання та формування кіберрезерву. Зокрема досліджено досягнення завершеної реінтеграційної програми «Кіберзахисники», призначеної для підготовки фахівців у сфері кібербезпеки із ветеранів і ветеранок російсько-української війни.

***Ключові слова:*** *державно-приватна взаємодія, державно-приватне партнерство, кіберрезерв, національна безпека, приватний сектор, стратегія кібербезпеки.*

**Постановка проблеми.** Аналіз розвитку політичного, економічного й інших аспектів сучасного суспільного життя свідчить, що жодні державні інституції не здатні самостійно реагувати й ефективно протидіяти загрозам національній безпеці. Тому кожна країна намагається вести гнучку й багатовекторну політику з метою пошуку та набуття додаткових безпекових спроможностей.

Одним із напрямів, який дає змогу зміцнити можливості держави й ефективно протидіяти загрозам національній безпеці, є використання інституту державно-приватного партнерства (ДПП). Світова тенденція щодо делегування державним сектором частини повноважень недержавному сектору показує свою ефективність і дієвість. Незважаючи на те, що застосування інституту ДПП, здебільшого, у національному науковому, бізнесовому та законотворному середовищі асоціювалося зі сферами будівництва, охорони здоров'я, екології, науки, освіти, протягом останніх років виникла потреба його використання й у сфері кібербезпеки.

Слід зауважити, що активізація ДПП у сфері національної безпеки відбулася з початком гібридної війни рф проти України, коли населення країни об'єдналося з метою допомоги силам оборони протидіяти загрозі. Причому ініціатором партнерства виступив саме приватний сектор, продуктивна діяльність якого (благодійних організацій, волонтерських, громадських об'єднань, окремих юридичних осіб) сприяла підвищенню зацікавленості держави в партнерстві. Дослідники цієї проблематики О. Дідич, О. Наумко зазначають, що результатом об'єднаних зусиль приватного та державного секторів стала успішна діяльність щодо дієвого опору та захисту території України [6]. Разом із позитивним досвідом упровадження ДПП виникають і певні перешкоди, серед яких А. Марущак та В. Панченко визначають складність і бюрократизм налагодження співпраці і наявність особистих амбіційних бажань суб'єктів як приватного, так і державного секторів; відмінності технічного забезпечення приватного та державного секторів, загрозу розкриття комерційної таємниці суб'єктів взаємодії та можливість репутаційних ризиків [12].

Сьогодні потребує подальшого дослідження питання розвитку можливостей і визначення дієвих механізмів використання інституту державно-приватного партнерства у сфері кібербезпеки з урахуванням унікального досвіду постійної протидії України агресії з боку рф.

**Аналіз останніх досліджень і публікацій.** Науковий інтерес щодо дослідження проблематики ДПП значно збільшився протягом останнього десятиліття. Зокрема М. Гребенюк, В. Григоренко, Т. Ісакова, Б. Леонов, В. Шпачук досліджували досвід інших країн щодо використання ДПП у сфері кібербезпеки [3; 4]. Ґрунтовні дослідження у сфері кібербезпеки, визначення проблемних питань стратегування такої діяльності та використання ДПП у цій сфері провели Д. Дубов і С. Гнатюк [2; 5; 7]. Адміністративно-правові й теоретико-правові аспекти забезпечення кібербезпеки України вивчали В. Бухарєв, А. Тарасюк [1; 22] й інші науковці.

Водночас потребує дослідження й аналізу іноземний досвід нормативно-правового регулювання суспільних відносин у контексті розвитку інституту державно-приватного партнерства.

**Метою** статті є аналіз досвіду України щодо формування інститутів державно-приватного партнерства та державно-приватної взаємодії у сфері кібербезпеки в умовах дії правового режиму воєнного стану, зокрема залучення фахівців приватного сектору з кібербезпеки до протидії російській агресії.

**Виклад основного матеріалу.** Необхідність використання інституту державно-приватної взаємодії в будь-якій сфері суспільних відносин зумовлюється передусім наявністю дефіциту державних ресурсів та одночасним збільшенням суспільних потреб у цій сфері.

Сьогодні можемо констатувати, що наразі використання інституту ДПП має певне законодавче підґрунтя. Так, основні положення, принципи й організаційно-правові засади ДПП визначає Закон України «Про державно-приватне партнерство» від 01.07.2010 № 2404-VI [13]. У цьому законі ДПП визначається як співробітництво між державою Україна (державними партнерами) та юридичними особами (приватними партнерами) відповідно до визначених ознак ДПП, що здійснюється на основі договору у визначеному нормативно-правовими актами порядку. Аналіз положень указаного закону дає можливість виділити такі ознаки ДПП:

1) створення об'єкта ДПП або управління ним;

2) тривалий період такого партнерства – від 5 до 50 років;

3) передача у процесі здійснення ДПП частини ризиків приватному партнеру;

4) здійснення приватним партнером інвестиції в об'єкт ДПП.

У статті 4 Закону України «Про державно-приватне партнерство» вказані сфери застосування ДПП, однак серед них немає сфери кібербезпеки. Але ж в останнє десятиріччя суттєво змінилися пріоритети та напрями державної політики, зокрема кібербезпека законодавчо визначена як одна з основних складових національної безпеки держави. Велика увага приділяється і протидії деструктивній діяльності в кіберпросторі.

Основи національного галузевого законодавства у сфері кібербезпеки й основні напрями його подальшого розвитку відповідно до європейських демократичних засад, як зазначає С. Гнатюк [2], визначені в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [16]. Забезпечення кібербезпеки визначено складовою національної безпеки держави у статті 5 цього закону. Крім того, забезпечення безпеки в кіберпросторі є одним із пріоритетів державної політики, що відображено в основних стратегічних документах країни.

Так, Стратегія національної безпеки України, затверджена Указом Президента України від 14.09.2020 № 392/2020 [19], серед напрямів забезпечення національної безпеки та реалізації пріоритетів національних інтересів України визначає розвиток ДПП та посилення спроможностей

національної системи кібербезпеки з метою ефективної протидії кіберзагрозам у сучасному безпековому середовищі. На основі Стратегії національної безпеки України розроблена Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021 [18].

Протидія в кіберпросторі у Стратегії воєнної безпеки України, затвердженій Указом Президента України від 25.03.2021 № 121/2021 [17], визначена як один із напрямів всеосяжної оборони України. Розвиток спроможностей держави у сфері забезпечення кібероборони, кіберзахисту та кібербезпеки згідно з цією Стратегія визначає одним з основних завдань держави.

Функціонування національної системи кібербезпеки відповідно до положень частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України [16] можливе зокрема шляхом забезпечення державно-приватної взаємодії у запобіганні кіберзагрозам. Належить зауважити, що норми Закону України «Про основні засади забезпечення кібербезпеки України» містять поняття ДПВ у забезпеченні кібербезпеки. Виходячи з цього, потребує вирішення питання, чи розглядає законодавець таку взаємодію як різновид ДПП згідно з визначеннями та нормами чинного законодавства щодо ДПП і чи потрапляє вона під дію Закону України «Про державно-приватне партнерство» [13] або навпаки ДПВ є ширшим поняттям, що включає в себе ДПП й інші форми співпраці: створення сприятливих обставин для інвестицій, розвиток підприємницької діяльності та регулювання політики в певній сфері тощо. Крім того, ДПВ можна визначати як одну із форм ДПП або розглядати ДПП як інституалізовану взаємодію. Більшість науковців (С. Гнатюк, В. Григоренко [2; 4] та ін.) ототожнює зазначені поняття. На нашу думку, виходячи з положень чинних нормативно-правових актів, поняття ДПП та ДПВ можна вважати тотожними, ґрунтуючись на тому, що за своєю природою і партнерство, і взаємодія полягають у спільній діяльності, яка спрямована на досягнення загальної та єдиної мети. Незважаючи на те, що чинні нормативні документи використовують як поняття ДПП (Стратегія кібербезпеки України), так і ДПВ (Закон України «Про основні засади забезпечення кібербезпеки»), вони визначають однакові форми ДПП та ДПВ: обмін інформацією про інциденти кібербезпеки, реалізацію спільних наукових і дослідницьких проєктів, навчання та підвищення кваліфікації кадрів у цій сфері.

Отже, ДПВ та ДПП у сфері кібербезпеки не мають чітко визначеної нормативно-правової основи та потребують нормативного врегулювання, водночас є як суспільний, так і державний запит щодо такого врегулювання.

Урегулювання питань ДПП у сфері кібербезпеки, визначення форм і методів партнерства – одне із завдань (пункт 57) Плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки, затвердженого розпорядженням Кабінету Міністрів України від 19.12.2023 № 1163-р (далі – План заходів) [14].

Необхідно зазначити, що одним із напрямів ДПП у сфері кібербезпеки,

який наразі належним чином не досліджений і потребує подальшого опрацювання та нормативного закріплення, є залучення державою фахівців приватного сектору до співпраці, зокрема з урахуванням дії правового режиму воєнного стану. Таке залучення може реалізовуватися в різних формах, відповідно й нормативне врегулювання його буде різнитися. Актуальність цього питання підтверджується визначенням його одним із завдань (пункт 30) у Плані заходів [14].

Кабінет Міністрів України результатом вирішення зазначених вище завдань убачає розроблення та подання відповідних законопроєктів, термін виконання яких – IV квартал 2024 року.

Станом ще на 2017 рік серед фундаментальних проблем розвитку ДПВ у сфері кібербезпеки після недосконалості нормативно-правової бази С. Гнатюк визначав дефіцит ефективної державної політики, передусім – регуляторної та комунікативної. З метою вирішення цієї проблеми він пропонував проводити діяльність щодо налагодження належної комунікації держави з недержавним сектором (експертами з кібербезпеки, представниками бізнесу, громадськими організаціями тощо) та створення дієвих інституційно-правових інструментів такої взаємодії [2]. На думку Ю. Заскоки, сфера кібербезпеки в цілому є пріоритетним напрямом розвитку бізнесу та стала привабливою для його представників [9], відповідно в налагодженні діалогу зацікавлені як представники приватної сфери, так і державної. Зауважимо, що станом на 2024 рік комунікація вже налагоджувалася та здійснювалася доволі активно. Практична діяльність фахівців із кібербезпеки характеризується значною кількістю ініціатив, учиненням активних дій, спрямованих, насамперед, на налагодження на регулярній основі діалогу між приватними компаніями, спеціалістами у сфері кібербезпеки та державою (тренінги, форуми, панельні дискусії, семінари, воркшопи). Запит щодо створення платформи ДПВ реалізується шляхом широкого експертного та громадського обговорення цієї проблематики.

З 2014 року Україна стала полігоном для рф з питань тестування російськими спецслужбами й підконтрольними їм групами хакерів нових практик кібератак та випробування нових засобів і способів ведення кібервійни [21]. Разом із тим із цього часу в Україні вже напрацювали значний позитивний досвід участі громадських організацій, волонтерів бізнес-структур у здійсненні діяльності в кіберпросторі, спрямованої на протидію цій агресії, наданні допомоги у виявленні й ідентифікації кібертерористів, їхніх кураторів із рф та прихильників.

Водночас як державний, так і приватний сектори проводять активні дії щодо реалізації ДПП та ДПВ у всіх визначених чинним законодавством напрямах (пункт 4 частини 1 статті 7 та статті 10 Закону України «Про основні засади забезпечення кібербезпеки України») і мають напрацювання в:

– обміні інформацією про інциденти кібербезпеки;

– реалізації спільних наукових і дослідницьких проєктів;

– навчанні та підвищенні кваліфікації кадрів у цій сфері.

Аналіз численних проведених заходів свідчить, що здійснення діяльності у вказаних напрямах не відбувається ізольовано, а реалізується паралельно або спільно.

Так, із метою обміну інформацією приватний і державний сектори використовують можливості:

– координаційного органу – Національного кластеру кібербезпеки. Зазначена платформа об'єднує можливості, компетенції та ресурси Ради національної безпеки і оборони України та Фонду цивільних досліджень та розвитку США (CRDF Global), міжнародних партнерів, урядових організацій і приватного сектору. Станом на 1 серпня 2024 року Кластер провів 28 засідань, залучив 927 організацій і 2 515 учасників програм [10];

– платформи MISP-UA, яка використовується в усьому світі та відповідає міжнародним стандартам ЄС і НАТО. Платформа є системою збирання, обробки, обміну інформацією про кібератаки, кіберінциденти, кіберзагрози та технічними даними про ідентифікатори компрометації інформаційних систем у режимі реального часу. Порядок обміну інформацією між суб'єктами забезпечення кібербезпеки з використанням платформи MISP-UA здійснюється відповідно до Положення про порядок обміну інформацією з використанням адаптованого програмного продукту «Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" (MISP-UA)» [15];

– урядової команди реагування на комп'ютерні інциденти України CERT-UA – державної платформи, яка забезпечує постійний обмін інформацією про кіберзагрози. CERT-UA функціонує у складі Держспецзв'язку, а з 2009 року виступає акредитованим членом Форуму команд реагування на інциденти безпеки FIRST [20]. CERT-UA виконує роль технічного координатора державних органів, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів.

Експерти та науковці з кібербезпеки залучаються до участі в різних проєктах, зокрема до нормотворчої діяльності з підготовки проєктів законів щодо врегулювання питань ДПП у сфері кібербезпеки та залучення приватного сектору й громадянського суспільства до проведення заходів із стримування деструктивної діяльності в кіберпросторі, про що зазначено вище. Крім того, діяльність Експертної ради з інформаційної та кібербезпеки, яку створив Держспецзв'язку України, безпосередньо спрямована на пошук шляхів розв'язання проблемних питань у сфері кібербезпеки та кіберосвіти, створення нових проєктів тощо.

Державним майданчиком, спрямованим на поєднання діяльності державного та приватного секторів у сфері кібербезпеки, також є Національний координаційний центр з кібербезпеки при РНБО, який зокрема здійснює діяльність щодо організації та проведення наукових, експертних, навчальних заходів.

Окремо належить відзначити діяльність щодо виконання пункту 31 Плану заходів із створення кіберре-

зерву. Так, одним із новітніх заходів, спрямованих на реалізацію цього пункту, є реінтеграційна програма «Кіберзахисники». Національний координаційний центр з кібербезпеки при РНБО України, Міністерство у справах ветеранів, CRDF Global в Україні за підтримки U.S. Department of State започаткували й успішно реалізували програму професійного розвитку у сфері кібербезпеки, яка має соціальну мету, спрямовану на реінтеграцію ветеранів та їхнє працевлаштування. Результатом реалізації цієї програми є підготовка понад 100 фахівців із кібербезпеки [8; 11].

Підготовлених як за цією програмою, так і в закладах освіти або за іншими програмами кваліфікованих працівників державний сектор може залучати до заходів із протидії деструктивній діяльності в кіберпросторі. Оскільки на сьогодні немає окремого нормативно-правового акта, який регламентує залучення фахівців приватного сектору до ДПП (його розроблення передбачене Планом заходів), поширеною є практика прийняття фахівців із кібербезпеки на службу (військову, державну) до відповідних підрозділів органів безпеки й оборони або працевлаштування таких фахівців на підставі укладеного трудового договору.

На нашу думку, сьогодні є важливим подальше дослідження використання альтернативних форм залучення фахівців з урахуванням положень чинного законодавства. Такими формами є лізинг, аутсорсинг, аутстафінг, робота за викликом, проєктна робота за короткостроковими договорами, використання гіг-контрактів, віддалена робота тощо. Перевагами цих форм залучення, окрім сприяння зайнятості фахівців, є передача невластивих суб'єкту державного сектору функцій представникам приватного сектору. Це дасть змогу суб'єкту державного сектору зосередитися на виконанні основних функцій; економити витрати щодо пошуку, прийняття на роботу, навчання фахівців, обліку заробітної плати, оподаткування, звітності тощо, що загалом сприятиме оптимізації діяльності.

Важливий момент при виборі способу залучення фахівця з кібербезпеки – урахування його діяльності, яка може бути здійснена в таких формах: експерт під час проведення експертиз; спеціаліст під час розслідування кіберінцидентів (зокрема й під час розслідування у кримінальних провадженнях); спеціаліст-розробник програмного забезпечення; спеціаліст зі створення освітніх програм; викладач освітніх програм; експерт під час здійснення нормотворчої діяльності; спеціаліст щодо користування програмним забезпеченням; спеціаліст із кібербезпеки тощо.

Отже, в умовах дії правового режиму воєнного стану й постійної активної протидії агресії рф у кіберпросторі якісне формування інститутів ДПП та ДПВ можливе за умови координації та мотивації державою приватного сектору, який із часів початку гібридної війни й особливо повномасштабного вторгнення засвідчив свою активну громадянську позицію та готовність до співпраці з метою захисту держави.

**Висновки.** У результаті проведеного дослідження належить конста-

тувати, що питання забезпечення кібербезпеки держави є одним із ключових аспектів забезпечення її обороноздатності та стабільності. Основні стратегічні документи України визначають державно-приватне партнерство та державно-приватну взаємодію у сфері кібербезпеки як інститути, здатні зміцнити спроможності держави ефективно протидіяти загрозам національній безпеці.

Наразі в Україні відбувається активний розвиток ДПП та ДПВ у сфері кібербезпеки, причому його особливістю є спрямування від практичної реалізації заходів, пошуку ідей, створення ініціатив, їх відпрацювання та реалізації до визначення та регламентації діяльності цих інститутів у нормативно-правових актах.

Основні напрями ДПП та ДПВ у процесі їхньої реалізації характеризуються одночасним розвитком, перетинанням, взаємодоповненням і симбіозом. Вивчення норм законів і наукових публікацій за вказаною темою дає підстави для підтримки позиції інших науковців щодо ототожнення цих понять.

Щодо основних напрямів ДПП та ДПВ у сфері кібербезпеки (обмін інформацією шляхом створення відповідних платформ; навчання та підвищення кваліфікації кадрів у цій сфері; підвищення цифрової грамотності громадян) ведеться активне експертне та громадське обговорення, що постійно висвітлюється в медіазасобах. Це є свідченням активного розвитку співпраці державного та приватного секторів у сфері кібербезпеки та необхідності подальшого нормативного врегулювання цього питання.

Актуальним є вирішення питання внормування залучення фахівців приватного сектору з кібербезпеки до протидії російській агресії проти України. Пропонуємо при цьому врахувати можливості використання альтернативних форм працевлаштування фахівців із кібербезпеки, таких як лізинг, аутсорсинг, аутстафінг, робота за викликом, проєктна робота за короткостроковими договорами, використання гіг-контрактів, віддалена робота, залежно від функцій, у виконанні яких є потреба.

На сучасному етапі держава шукає шляхи та здійснює активні дії щодо формування кіберрезерву. Насамперед у цій діяльності зусилля спрямовані на залучення до кіберрезерву ветеранів і ветеранок, які мають практичний досвід захисту держави.

Подальші дослідження інституту державно-приватного партнерства у сфері кібербезпеки слід спрямувати на вивчення іноземного досвіду нормативно-правового регулювання зазначених суспільних відносин.

## Список використаних джерел

1. Бухарєв В. В. Адміністративно-правові аспекти забезпечення кібербезпеки в Україні : дисертація … кандидата юридичних наук : 12.00.07. Суми, 2018. 221 с.

2. Гнатюк С. Л. Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. URL: https://www.niss.gov.ua/sites/default/files/2017-12/kiberbezpek-d3e61.pdf (дата звернення: 01.08.2024).

3. Гребенюк М. В., Леонов Б. Д. Досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право.* 2018. № 2 (25). С. 45–50.

4. Григоренко В. А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки. URL : https://doi.org/10.37750/2616-6798.2021.2(37).238405.

5. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналітична доповідь / за заг. ред. Д. Дубова. Київ : НІСД, 2018. 84 с. URL: https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf (дата звернення: 01.08.2024).

6. Дідич О. Р., Наумко О. М. Державно-приватне партнерство у забезпеченні національної безпеки в умовах повномасштабного вторгнення. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2023/2_2023/20.pdf (дата звернення: 03.08.2024).

7. Дубов Д. Формуючи нову стратегію кібербезпеки України: чи можемо уникнути помилок першої спроби стратегування. URL: https://niss.gov.ua/sites/default/files/2021-01/tezy-dubov-2.pdf (дата звернення: 03.08.2024).

8. Завершення програми «Кіберзахисники 2024». URL: https://cyberlab.ua/archives/5879 (дата звернення: 02.08.2024).

9. Заскока Ю. В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. URL: http://perspectives.pp.ua/index.php/np/article/view/467/470 (дата звернення: 02.08.2024).

10. Зміцнюючи національну кібербезпеку. Про кластер. URL: https://cybersecuritycluster.org.ua/about/ (дата звернення: 01.08.2024).

11. «Кіберзахисники 2024»: понад 100 ветеранів та ветеранок зможуть допомогти Україні у сфері кіберзахисту. URL: https://mva.gov.ua/prescenter/category/86-novini/kiberzahisniki-2024-ponad-100-veteraniv-y-veteranok-zmozhut-dopomogti-ukraini-u-sferi-kiberzahistu (дата звернення: 02.08.2024).

12. Марущак А. І., Панченко В. М. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід і перспективи для України. *Інформаційна безпека людини, суспільства, держави.* 2014. № 3 (16). С. 56–63.

13. Про державно-приватне партнерство : Закон України від 01.07.2010 № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text (дата звернення: 02.08.2024).

14. Про затвердження Плану заходів на 2023–2024 роки з реалізації Стратегії кібербезпеки : розпорядження КМУ від 19.12.2023 № 1163-р. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (дата звернення: 03.08.2024).

15. Про затвердження Положення про порядок обміну інформацією з використанням адаптованого програмного продукту «Malware Information Sharing Platform and Threat Sharing "Ukrainian Advantage" (MISP-UA)» : наказ Центрального управління Служби безпеки України від 07.12.2023 № 503. URL: https://zakon.rada.gov.ua/laws/show/z2164-23#Text (дата звернення: 02.08.2024).

16. 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: 02.08.2024).

17. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 25.03.2021 № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021?find=1&text=%D0%BA%D1%96%D0%B1%D0%B5%D1%80#w1_1 (дата звернення: 02.08.2024).

18. 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: 02.08.2024).

19. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n12 (дата звернення: 02.08.2024).

20. Про CERT-UA. URL: https://cert.gov.ua/about-us (дата звернення: 03.08.2024).

21. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. URL: https://geostrategy.org.ua/analityka/analitychna-zapyska/spivrobitnyctvo-ukrayina-yes-nato-z-protydiyi-gibrydnym-zagrozam-u-kiber-sferi/pdf (дата звернення: 02.083.2024).

22. Тарасюк А. В. Теоретико-правові основи забезпечення кібербезпеки України : дисертація … доктора юридичних наук : 12.00.07. Київ, 2021. 461 с.

*Стаття надійшла до редакції 07.08.2024*

**UDC 044.946.5.056**

**Panasiuk T. I., Petrenko S. V.**

**CURRENT STATE OF PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF CYBERSECURITY: UKRAINIAN EXPERIENCE**

The article examines the current state of the public-private partnership (PPP) institution and public-private interaction (PPI) in the field of cybersecurity in Ukraine. The normative legal acts regulating these issues have been analysed, in particular, the laws of Ukraine "On Public-Private Partnership" and "On the Basic Principles of Ensuring Cybersecurity of Ukraine." The study of the provisions of these laws and scientific publications on the topic indicates that the concepts of PPP and PPI can currently be equated, as both partnership and interaction manifest in joint activities aimed at achieving a common goal. Furthermore, the existing normative standards highlight identical forms of PPP and PPI: the exchange information on cybersecurity incidents, the implementation of joint scientific and research projects, and training and qualification improvement of personnel in this field.

Based on the analysis of Ukraine's key strategic documents on national security, it is substantiated that one of the ways to strengthen the cybersecurity system is the use of Public-Private Partnership (PPP) in this area.

Special attention is focused on studying the forms of involvement of cybersecurity experts from the private sector in cooperation with state bodies. Considering the current experience of involving experts from the private sector through enlistment in military service within relevant security and defense institutions or appointment to state service based on a employment contract, the study suggests exploring alternative cooperation models.

The experience of interaction between the public and private sectors in the field of cybersecurity over recent years has been also summarized in the article. Thus, the exchange of information on cybersecurity incidents has been conducted through the coordination platform of the National Cybersecurity Cluster, the MISP-UA platform, as well as the Ukrainian government's Computer Emergency Response Team (CERT-UA). Highlighting the active involvement of public and private sectors in terms of training and improving specialist qualifications, the study indicates effective steps towards fulfilling state tasks and forming a cyber reserve. In particular, the achievements of the completed reintegration program “Cyber Defenders,” designed to train cybersecurity experts from among veterans of russian-Ukrainian war, have been explored.

***Key words:*** *public-private partnership, public-private interaction, cyber reserve, national security, private sector, cybersecurity strategy.*