Адміністративне право і процес; фінансове право; інформаційне право

УДК 004.056.5

Жевелєва Ірина Сергіївна

кандидат юридичних наук, старший викладач

Навчально-науковий інститут інформаційної безпеки

Національної академії Служби безпеки України

Жевелева Ирина Сергеевна

кандидат юридических наук, старший преподаватель

Учебно-научный институт информационной безопасности

Национальной академии Службы безопасности Украины

Zhevelieva Iryna

PhD in Juridical Sciences, Senior Lecturer

Educational and Scientific Institute of Information Security

National Academy of Security Service of Ukraine

СПІВВІДНОШЕННЯ ПОНЯТЬ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА ТА ДЕРЖАВНО-ПРИВАТНОЇ ВЗАЄМОДІЇ У ПРОЦЕСІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

СООТНОШЕНИЕ ПОНЯТИЙ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА И ГОСУДАРСТВЕННО-ЧАСТНОГО ВЗАИМОДЕЙСТВИЯ В ПРОЦЕССЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ

RATIO OF THE CONCEPTS OF PUBLIC-PRIVATE PARTNERSHIP AND PUBLIC-PRIVATE INTERACTION IN THE PROCESS OF ENSURING THE NATIONAL SECURITY OF UKRAINE

Анотація. *У статті досліджується питання узгодження понять державно-приватного партнерства та державно-приватної взаємодії у процесі забезпечення національної, інформаційної та кібернетичної*

безпеки України. Здійснено аналіз та узагальнення законодавства та наукових публікацій щодо теми дослідження, на цій основі визначені основні недоліки законодавства про державно-приватне партнерство. Автором вказується на відсутність законодавчого трактування поняття державно-приватної взаємодії і термінологічного узгодження його із поняттям державно-приватного партнерства. Встановлено, що для ефективного здійснення державно-приватної взаємодії у сфері кібернетичної безпеки критичної інфраструктури мають бути законодавчо унормовані та узгоджені відповідні поняття. Проаналізовано стан реалізації Стратегії кібербезпеки України у частині питань обміну інформацією про кіберзагрози, побудови ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства у сфері кібербезпеки. Наведено офіційні статистичні дані. Висвітлено різні підходи до з'ясування питання співвідношення понять державно-приватного партнерства та державно-приватної взаємодії у процесі забезпечення національної безпеки України. Окреслено теоретико-методологічні передумови розкриття сутності поняття державно-приватного партнерства. Наведено приклади практики формування відповідних відносин у сфері державно-приватної взаємодії із забезпечення кібербезпеки України. Зроблено висновок про необхідність розгляду сутності поняття «державно-приватне партнерство», виходячи із його природи, через категорію «взаємодія». Наведено відмінності у використанні понять «державно-приватне партнерство» і «державно-приватна взаємодія», та доведено, що поняття державно-приватної взаємодії є родовим до поняття державно-приватного партнерства.

Ключові слова: *державно-приватне партнерство, державно-приватна взаємодія, співвідношення, узгодження.*

Аннотация. *В статье исследуется вопрос согласования понятий государственно-частного партнерства и государственно-частного взаимодействия в процессе обеспечения национальной, информационной и кибернетической безопасности Украины. Осуществлен анализ и обобщение законодательства и научных публикаций по теме исследования, на этой основе определены основные недостатки законодательства о государственно-частном партнерстве. Автором указывается на отсутствие законодательной трактовки понятия государственно-частного взаимодействия и терминологического согласования его с понятием государственно-частного партнерства. Установлено, что для эффективного осуществления государственно-частного взаимодействия в сфере кибернетической безопасности критической инфраструктуры должны быть законодательно урегулированы и согласованы соответствующие понятия. Проанализировано состояние реализации Стратегии кибербезопасности Украины в части вопросов обмена информацией о киберугрозах, построения эффективной системы подготовки кадров и действенной модели государственно-частного партнерства в сфере кибербезопасности. Приведены официальные статистические данные. Освещены различные подходы к выяснению вопроса соотношения понятий государственно-частного партнерства и государственно-частного взаимодействия в процессе обеспечения национальной безопасности Украины. Определены теоретико-методологические предпосылки раскрытия сущности понятия государственно-частного партнерства. Приведены примеры практики формирования соответствующих отношений в сфере государственно-частного взаимодействия по обеспечению кибербезопасности Украины. Сделан вывод о необходимости рассмотрения сущности понятия «государственно-частное партнерство», исходя из его природы, через категорию*

«взаимодействие». Приведены различия в использовании понятий «государственно-частное партнерство» и «государственно-частное взаимодействие», и доказано, что понятие государственно-частного взаимодействия является родовым к понятию государственно-частного партнерства.

Ключевые слова: *государственно-частное партнерство, государственно-частное взаимодействие, соотношение, согласование.*

Summary. *The article examines the issue of ratio of the of the concepts of public-private partnership and public-private cooperation in the process of ensuring the national, information and cyber security of Ukraine. The analysis and generalization of the legislation and scientific publications on the research topic are carried out, on this basis the main shortcomings of the legislation on public-private partnership are determined. The author points out the lack of legislative interpretation of the concept of public-private interaction and its terminological coordination with the concept of public-private partnership. It is established that for the effective implementation of public-private cooperation in the field of cyber security of critical infrastructure, the relevant concepts must be legally regulated and harmonized. The state of implementation of the Cyber Security Strategy of Ukraine in terms of information exchange on cyber threats, building an effective training system and an effective model of public-private partnership in the field of cybersecurity is analyzed. Official statistics is given. Different approaches to clarifying the question of the relationship between the concepts of public-private partnership and public-private interaction in the process of ensuring the national security of Ukraine are highlighted. Theoretical and methodological prerequisites for revealing the essence of the concept of public-private partnership are outlined. Examples of the practice of forming appropriate relations in the field of public-private cooperation to ensure cyber security of Ukraine are given. It is concluded that it is necessary to consider the*

essence of the concept of "public-private partnership", based on its nature, through the category of "interaction". The differences in the use of the terms "public-private partnership" and "public-private interaction" are given, and it is proved that the concept of public-private interaction is generic to the concept of public-private partnership.

Key words: *public-private partnership, public-private interaction, relations, coordination.*

Постановка проблеми. Розвиток інформаційних технологій, усвідомлення важливості забезпечення безпеки діяльності об'єктів критичної інфраструктури, незалежно від форми власності, зумовлює розширення загроз безпеці України у сфері обігу державних і приватних електронних інформаційних ресурсів. Державно-приватне партнерство у цій сфері визначено одним із напрямів забезпечення реалізації пріоритетів національних інтересів України та забезпечення національної безпеки України. З прийняттям Закону України «Про основні засади забезпечення кібербезпеки України», разом із терміном «державно-приватне партнерство» почало використовуватися поняття «державно-приватна взаємодія», яке потребує подальшої конкретизації. Залишаються недостатньо розкритими ряд аспектів сутності і природи даного поняття, а також його співвідношення із загальноприйнятим терміном «державно-приватне партнерство».

Аналіз останніх досліджень і публікацій. Проблематика державно-приватного партнерства в різних сферах суспільного життя останнім часом набула особливої уваги. Дослідженням взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки займався С.Г. Петров [1]. Г.Ю. Зубко вивчав особливості здійснення публічно-приватного партнерства та взаємодії у сфері захисту критичної інфраструктури [2]. Міжнародний та український досвід державно-

приватного партнерства у сфері кібербезпеки був предметом дослідження Д.В. Дубова, В.О. Бойка, С.Л. Гнатюка, Т.О. Ісакової, М.А. Ожевана, А. В. Покровської [3]. С.В. Онишко окреслив теоретико-методологічні передумови розкриття сутності державно-приватного партнерства та проаналізував співвідношення даного поняття з рядом інших понять [4]. Незважаючи на вагомий науковий доробок, питання узгодження понять державно-приватного партнерства та державно-приватної взаємодіїї у сфері забезпечення національної безпеки України є недостатньо дослідженим, що обумовлює необхідність подальшого наукового пошуку.

Формулювання цілей статті (постановка завдання). Автором у даній науковій статті за мету ставиться розкрити співвідношення понять державно-приватного партнерства та державно-приватної взаємодії у процесі забезпечення національної безпеки України.

Виклад основного матеріалу. Прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [5], затвердження Стратегії кібербезпеки України [6], Стратегії національної безпеки України [7], Концепції створення державної системи захисту критичної інфраструктури [8] визначили вектор подальшого розвитку національного галузевого законодавства у відповідності до європейських стандартів. У цих документах увага акцентована, у тому числі, на нагальній необхідності розвитку державно-приватного партнерства для забезпечення державної безпеки. Проте, у Законі використовується термін «державно-приватна взаємодія» (далі – ДПВ), а у Стратегіях і Концепції – «державно-приватне партнерство» (далі – ДПП). Незрозумілим залишається питання трактування та співвідношення названих понять.

В Україні законодавчо регламентований прогресивний механізм співробітництва між державою та бізнесом – державно-приватне партнерство, який визначений як співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі

відповідних державних органів, що згідно із Законом України «Про управління об'єктами державної власності» здійснюють управління об'єктами державної власності, органів місцевого самоврядування, Національною академією наук України, національних галузевих академій наук (державних партнерів) та юридичними особами, крім державних та комунальних підприємств, установ, організацій (приватних партнерів), що здійснюється на основі договору в порядку, встановленому законодавством та відповідає ознакам державно-приватного партнерства.

Закон України «Про державно-приватне партнерство України» був прийнятий 1 липня 2010 року. Ним встановлено організаційно-правові засади взаємодії державних партнерів з приватними партнерами та основні принципи державно-приватного партнерства на договірній основі. Одним із пріоритетних напрямів розвитку державно-приватного партнерства визначено обмін інформацією. Формами здійснення державно-приватного партнерства законодавець визначив: 1) концесійний договір; 2) договір управління майном (виключно за умови передбачення у договорі, укладеному в рамках державно-приватного партнерства, інвестиційних зобов'язань приватного партнера); 3) договір про спільну діяльність; 4) інші договори. Наведений перелік форм не є вичерпним, з огляду на загрози національній безпеці, які виникли за період з його прийняття. Хоча базові положення даного закону відповідають сучасним європейським правовим нормам та практикам, існує необхідність у його перегляді і внесенні відповідних змін відповідно до викликів сьогодення. Зокрема, сфера забезпечення кібербезпеки у зазначеному законі не фігурує в переліку сфер застосування ДПП, крім цього, у законі поза увагою залишається необхідність здійснення і розвитку державно-приватного партнерства для забезпечення безпеки сфери критичної інфраструктури, хоча деякі сектори (підсектори) основних послуг критичної інфраструктури, які затверджені Постановою Кабінету Міністрів від 9

жовтня 2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», наведені.

Крім того, незважаючи на законодавче закріплення напрямів державно-приватного партнерства, його реалізація у процесі забезпечення безпеки суб'єктів господарювання значно ускладняється багаторівневістю і бюрократизацією регулювання, відсутністю відомчих нормативних актів, які регулюють вказані питання а також шаблоном недовіри до державних і правоохоронних органів, який існує у суспільстві. Крім того, державно-приватне партнерство є складним, як з організаційної, так і з фінансової та правової точки зору, інститутом. Він передбачає багатосторонні домовленості, розподіл ризиків, аналіз комерційних перспектив та індивідуальні схеми фінансування та юридичного втілення.

У Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020, розвиток державно-приватного партнерства вказано одним із напрямів забезпечення реалізації пріоритетів національних інтересів України та забезпечення національної безпеки України. Крім цього, у переліку основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки визначено створення ефективної системи безпеки та стійкості критичної інфраструктури, заснованої на чіткому розподілі відповідальності її суб'єктів та державно-приватному партнерстві.

У Концепції створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р, вказано, що нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури є нагальною проблемою [9].

У Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96/2016, зазначено, що забезпечення

кібербезпеки України, як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту. Важливим аспектом Стратегії є акцентування уваги на необхідності забезпечення взаємодії з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури. Мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту.

Кіберзахист критичної інфраструктури має полягати, насамперед, у налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвитку державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період, а також розробленні та запровадженні механізму обміну інформацією між державними органами, приватним

сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

У березні 2021 року робоча група при Національному координаційному центрі кібербезпеки Ради національної безпеки і оборони України схвалила проєкт Стратегії кібербезпеки України на 2021–2025 роки [10], який висвітлено на сайті РНБО України. Основою для розроблення цього документу стала Стратегія національної безпеки України та досвід кращої світової практики (були вивчені концептуальні положення стратегій з кібербезпеки країн ЄС, самого ЄС, США, Японії та ін.), ряд соціологічних опитувань та емпіричних досліджень, які були проведені наприкінці минулого та на початку цього року.

Відповідно до проєкту стан реалізації чинної Стратегії кібербезпеки України, за результатами експертних оцінок, не перевищує 40 %. Невирішеними досі залишилися, в тому числі, питання оперативного обміну інформацією про кіберзагрози, побудови ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства.

Актуальною тенденцією є проголошення необхідності взаємодії між державним і приватним сектором для формування ефективної моделі відносин у сфері кібербезпеки, заснованої на довірі. Для цього передбачається здійснення наступних заходів: 1) врегулювання на законодавчому рівні питання державно-приватного партнерства у сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проєктів у цій сфері; 2) запровадження на регулярній основі проведення консультацій заінтересованих сторін та надання методичної допомоги з питань утворення підрозділів кіберзахисту, галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти; 3) залучення на регулярній основі представників наукових установ, громадських організацій та незалежних

експертів у сфері кібербезпеки до розроблення нормативно-правових актів, нормативних документів та стандартів у цій сфері; 4) підвищення ефективності залучення громадськості до прийняття рішень у сфері кібербезпеки шляхом проведення відповідних опитувань (анкетувань) та розміщення їх результатів на інформаційних ресурсах Національного координаційного центру кібербезпеки та основних суб'єктів національної системи кібербезпеки; 5) стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури; 6) впровадження програми розвитку ринку товарів і послуг у сфері кібербезпеки, що включатиме стимулювання його розвитку та міжнародного визнання; 7) розробка системи оцінки новітніх технологій, що безпосередньо мають вплив на кіберстійкість країни, створення інструментів (стандартів, протоколів, сертифікатів тощо) з оцінки ефективності використання новітніх технологій з протидії кібератакам; 8) запровадження пілотних менторських програм підвищення кваліфікації фахівців державних органів, що безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту, шляхом залучення сертифікованих за міжнародними стандартами фахівців приватного сектору; 9) продовження практики щорічного проведення місяця кібербезпеки в Україні із залученням широкого кола профільних фахівців та експертів державних органів, академічних і освітніх установ, а також громадського та приватного секторів, закріпивши необхідність його проведення відповідним нормативно-правовим актом; 10) сприяння функціонуванню у всіх регіонах України постійно діючих діалогових майданчиків (конференцій, семінарів, форумів тощо), діяльність яких спрямована на розбудову довіри між суб'єктами забезпечення кібербезпеки; 11) сприяння впровадженню на підприємствах, в установах і

організаціях, незалежно від форми власності, культури кібербезпеки, що полягає у постійному підвищенні кіберобізнаності їх керівників та працівників; 12) сприяння взаємному визнанню результатів оцінки відповідності та сертифікації з кібербезпеки, здійснених відповідними органами як в Україні, так і за кордоном; 13) впровадження механізму оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування та як елемент подальшого впровадження системи кіберстрахування.

Як бачимо, перелік наведених заходів значно ширший за ті заходи, які регламентовані Законом України «Про державно-приватне партнерство». Це дозволяє зробити висновок про те, що поняття державно-приватної взаємодії є ширшим за поняття державно-приватного партнерства. Слід зазначити, що на даний час у правовому полі хаотично використовуються ці два поняття і відсутність правової регламентації ускладнює розуміння і впровадження у практику відповідних ініціатив.

Спеціально уповноваженим органом у системі центральних органів виконавчої влади з питань ДПП є Міністерство розвитку економіки, торгівлі та сільського господарства України (далі – Мінекономіки), на яке покладається обов'язок з формування та реалізації державної політики у сфері ДПП. За даними Мінекономіки, в Україні станом на 01.01.2021 на умовах ДПП укладено 192 договори, з яких реалізується 39 договорів (29 – концесійних договорів, 6 – договорів про спільну діяльність, 4 – інші договори), 153 договорів не реалізується (118 – не виконується, 35 – розірвані / закінчився термін дії). Згідно з даними Мінекономіки, станом на 01.01.2021 в Україні ДПВ у сфері забезпечення кібербезпеки відсутня (укладені тут договори можуть відноситися хіба що до тих угод, що фігурують у діаграмі у розділі «Інші») [11].

Закон України «Про основні засади забезпечення кібербезпеки України» одним із шляхів забезпечення функціонування національної

системи кібербезпеки визначає *державно-приватну взаємодію* у запобіганні кіберзагрозам об'єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період. У даному законі вживається виключно термін «державно-приватна взаємодія», визначення якого відсутнє, і зі змісту не зрозуміло, чи є така взаємодія різновидом державно-приватного партнерства, згідно з визначеннями та нормами чинного законодавства.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом: 1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій; 2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту; 3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів; 4) партнерства та координації команд реагування на комп'ютерні надзвичайні події; 5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки; 6) надання консультативної та практичної допомоги з питань реагування на кібератаки; 7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет; 8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки; 9)

періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки; 10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки; 11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, IT-компаніями з метою виконання заходів кібероборони в кіберпросторі.

Національним інститутом стратегічних досліджень для з'ясування питання співвідношення понять державно-приватного партнерства та державно-приватної взаємодії було зроблено ряд інформаційних запитів до державних і правоохоронних органів України. Так, Міністерство оборони України пропонує розглядати ці два поняття окремо, використовуючи обидва. Відповідно до запропонованих визначень, ДПП більшою мірою спрямоване на формування довірчих відносин між державним та приватним секторами, а ДПВ – на вирішення конкретних проблем державного та приватного секторів.

Національний банк України також звертає увагу на різницю в цих поняттях, акцентуючи на тому, що спроба змінити/замінити поняття ДПВ на ДПП «призведе до звуження поняття державно-приватної взаємодії у сфері кібербезпеки та змінить концептуальні підходи і принципи такої взаємодії» [3, с. 54].

Служба безпеки України в цьому питанні відштовхується від того, що «поняття «взаємодія» є найбільш близьким до взаємовідносин, які необхідно збудувати між органами державної влади та суспільством для налагодження взаєморозуміння, довіри та організації ефективної роботи у напрямку захисту життєво важливих інтересів людини і громадянина, суспільства і держави, національних інтересів України у кіберпросторі в умовах ведення потужної кібервійни, яку здійснює Російська федерація».

Це зумовлено тим, що «ДПВ є одним з головних принципів забезпечення кібербезпеки держави, який передбачає широку співпрацю з громадянським суспільством у сфері кібербезпеки і кіберзахист вказаний принцип ґрунтується на спільній відповідальності держави та приватного сектору за стан забезпечення кібербезпеки, що передбачає передачу приватному партнеру частини ризиків, а також внесення останнім відповідних інвестицій у сферу забезпечення кібербезпеки держави. Принцип державно-приватної взаємодії, в першу чергу, спрямований на підвищення ефективності діяльності як державних, так і недержавних суб'єктів у сфері забезпечення кібербезпеки за умов їх належної співпраці, а також посилення спроможностей національної системи кібербезпеки України» [3, с. 55].

Як бачимо, питання співвідношення понять ДПП та ДПВ усе ще залишається актуальним як для нормативно-правового поля, так і для самої державної управлінської системи.

Автор погоджується з думкою Петрова С.Г., який вважає, що, якщо державно-приватна взаємодія є іншим за змістом поняттям, ніж державно-приватне партнерство, то відповідні відносини потребують регулювання іншими правовими нормами. Зважаючи ж на особливості такої взаємодії у сфері кібербезпеки загалом і захисту державних електронних інформаційних ресурсів зокрема, потребує визначення не тільки відповідна термінологія, а й питання обміну даними про кіберінциденти та кібератаки, стандартів кібербезпеки, державних/приватних вимог до сертифікації відповідного обладнання та рішень тощо [1, с. 109].

У зарубіжній практиці сутність ДПП трактують із двох позицій: по-перше, як система відносин держави і бізнесу, інструмент економічного і соціального розвитку на всіх рівнях та, по-друге, як конкретні проекти, реалізовані спільно державними органами і приватними компаніями на базі об'єктів державної і муніципальної власності [4, с. 10]

На думку Онишка С.В. саме у взаємодії слід вбачати природу та її здатність представляти той системно-об'єднуючий механізм, у межах якого функціонують різні форми зв'язку між державними і ринковими інститутами, зокрема, така з них, як партнерство. В основі такого бачення лежить філософський постулат, що саме природою визначається сутність, а не навпаки, та природа є джерелом, внутрішнім двигуном для бачення процесу набуття якісної визначеності певними системами. Взаємодія – це одна із основних філософських категорій, що відображає процеси впливу різних об'єктів один на одного, їхню взаємну обумовленість і зміну стану або взаємоперехід, а також заснування одного об'єкта іншим. Значення взаємодії полягає в намаганні погоджених дій різник ланок системи, об'єднати і максимально використати їхні зусилля і можливості, досягти ефективних результатів у коротший термін та з меншими витратами сил і засобів [4, с. 11]. Погодимось із думкою Онишка С.В., що поняття «взаємодія», є родовим поняттям до «партнерства» і розкриває природу різних форм взаємодії ринкових і державних інститутів, які, своєю чергою, сформовані з адекватних інструментів і важелів для досягнення поставлених завдань соціально-економічного розвитку.

На нашу думку, державно-приватне партнерство та державно-приватна взаємодія – це близькі, але не тотожні поняття. Державно-приватне партнерство пропонуємо вважати однією із форм державно-приватної взаємодії, що полягає у відносинах між державними і приватними партнерами, при реалізації яких ресурси обох партнерів об'єднуються з відповідним розподілом ризиків, відповідальності та винагород (відшкодувань) між ними, для взаємовигідної співпраці на довгостроковій основі у створенні (відновленні) нових та/або модернізації (реконструкції) наявних об'єктів, які потребують залучення інвестицій, і користування (експлуатації) такими об'єктами.

За наявності неоднозначності у правовому регулюванні питань державно-приватної взаємодії існують непоодинокі приклади практики формування відповідних відносин. У Службі безпеки України розроблена і застосовується платформа для збирання, обробки та обміну інформацією про інциденти кібербезпеки, а також технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури в режимі реального часу –MISP-UA. За допомогою цієї платформи ведеться державно-приватна взаємодія для спільного захисту інформаційної та кібербезпеки держави. На MISP-ua вже зареєстровано більш, ніж 300 користувачів, серед яких державні і приватні підприємства: M.E.Doc (яка стала першою приватною структурою-користувачем), Укренерго, Укргідроенерго, ДП «Антонов» та ін. Крім того, за ініціативи СБ України започатковано проект CyberCrime@EAPIII спільно з Радою Європи, який серед іншого спрямований на покращення співробітництва правоохоронних і спеціальних органів країн-членів Східного партнерства з приватним ІТсектором у сфері використання електронних доказів у досудових розслідуваннях і протидії кіберзагрозам загалом.

МВС України ще у 2015 році підписало Меморандум про взаєморозуміння з корпорацією "Майкрософт" щодо захисту даних, інформаційної та кібербезпеки. Департамент кіберполіції Національної поліції України залучає експертів для обміну даними, проведення тренінгів для співробітників, взаємодіє з академічною спільнотою, наприклад, Харківським національним університетом радіоелектроніки, Національним аерокосмічним університетом ім. М.Є. Жуковського "ХАІ". Національний банк України створив Центр кіберзахисту (CSIRT-NBU), на базі якого долучає представників банківської спільноти до питань формування критеріїв та методології віднесення об'єктів критичної інфраструктури банківської системи України до критичної інфраструктури та вирішення питань організації кіберзахисту в банківській системі України [1, с. 110].

Висновки і перспективи подальших дослідженьу даному напрямку. Таким чином, незважаючи на проголошення вектору розвитку державно-приватного партнерства для забезпечення національної безпеки України, нині реалізація його у сферах інформаційної та кібернетичної безпеки суб'єктів господарювання практично відсутня. Незважаючи на відсутність законодавчого трактування поняття, державними та правоохоронними органами реалізуються окремі заходи державно-приватної взаємодії. Проблемою є законодавча неузгодженість понять ДПП та ДПВ та відсутність правового змісту самого поняття «державно-приватна взаємодія». Для створення платформи державно-приватної взаємодії у сфері кібербезпеки державою ухвалені лише базові нормативні акти, проте не налагоджено діалог з експертними колами та суспільством і не створено жодних інституційно-правових інструментів такої взаємодії.

Ми пропонуємо вважати державно-приватну взаємодію родовим поняттям до державно-приватного партнерства. Така взаємодія повинна полягати у співпраці та інклюзивному діалозі всіх суб'єктів забезпечення національної безпеки, зокрема в рамках державно-приватного партнерства, задля досягнення стратегічних цілей, вироблення узгоджених планів та проєктів у сфері кібербезпеки; впровадженні сучасних принципів, методів, підходів та механізмів публічного управління у сфері кібербезпеки, партнерських відносинах між державою, бізнесом та суспільством;

Література

1. Петров С.Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право*.2019. № 4(31). С. 107-112.
2. Зубко Г.Ю. Публічно-приватне партнерство у сфері безпеки стратегічної інфраструктури України. *Юридичний науковий журнал*. 2020. № 2. DOI https://doi.org/10.32782/2524-0374/2020-2-2/3

3. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. К. : НІСД, 2018. – 84 с.
4. Онишко С. В. До питання теоретико-методологічного забезпечення розбудови державно-приватного партнерства. *Наукові записки Національного університету «Острозька академія». Серія «Економіка»* : науковий журнал. Острог : Вид-во НаУОА, грудень 2017. № 7(35). С. 8–11.
5. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 30.05.2021).
6. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення 30.05.2021).
7. Стратегія національної безпеки України : Указ Президента України від 14 вересня 2020 року № 392/202. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення 30.05.2021).
8. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 6.12.2017 № 1009-р: веб-сайт. URL: https://zakon.rada.gov.ua/laws /show/1009-2017-%D1%80 (дата звернення 30.05.2021).
9. Жевелєва І. С. Правові засади забезпечення інформаційної безпеки об'єктів критичної інфраструктури. *Міжнародний науковий журнал "Інтернаука". Серія: "Юридичні науки". 2020. № 5.* DOI: 10.25313/2520-2308-2020-5-6007.

10. Проєкт Стратегії кібербезпеки України на 2021 – 2025 роки. веб-сайт: URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення 30.05.2021).
11. Стан здійснення ДПП в Україні веб-сайт: URL: https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=9fc90c5e-2f7b-44b2-8bf1-1ffb7ee1be26&title=StanZdiisnenniaDppVUkraini (дата звернення 30.05.2021).

References

1. Petrov S.Gh. Pravovi osnovy vzajemodiji derzhavnykh orghaniv ta pryvatnykh sub'jektiv iz metoju zakhystu elektronnykh informacijnykh resursiv Ukrajiny. Informacija i pravo. 2019. # 4(31). S. 107-112.
2. Zubko Gh.Ju. Publichno-pryvatne partnerstvo u sferi bezpeky strateghichnoji infrastruktury Ukrajiny. Jurydychnyj naukovyj zhurnal. 2020. # 2. DOI: 10.32782/2524-0374/2020-2-2/3
3. Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyj dosvid ta mozhlyvosti dlja Ukrajiny : analit. dop. / za zagh. red. D. Dubova. K. : NISD, 2018. 84 s.
4. Onyshko S. V. Do pytannja teoretyko-metodologhichnogho zabezpechennja rozbudovy derzhavno-pryvatnogho partnerstva. Naukovi zapysky Nacionaljnogho universytetu «Ostrozjka akademija». Serija «Ekonomika» : naukovyj zhurnal. Ostrogh : Vyd-vo NaUOA, ghrudenj 2017. # 7(35). S. 8–11.
5. Pro osnovni zasady zabezpechennja kiberbezpeky Ukrajiny: Zakon Ukrajiny vid 5 zhovtnja 2017 roku # 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennja 30.05.2021).

6. Strateghija kiberbezpeky Ukrajiny : Ukaz Prezydenta Ukrajiny vid 15 bereznja 2016 roku # 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (data zvernennja 30.05.2021).
7. Strateghija nacionaljnoji bezpeky Ukrajiny : Ukaz Prezydenta Ukrajiny vid 14 veresnja 2020 roku # 392/202. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (data zvernennja 30.05.2021).
8. Pro skhvalennja Koncepciji stvorennja derzhavnoji systemy zakhystu krytychnoji infrastruktury: Rozporjadzhennja Kabinetu Ministriv Ukrajiny vid 6.12.2017 # 1009-r: veb-sajt. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80 (data zvernennja 30.05.2021).
9. Zhevelieva I. S. Pravovi zasady zabezpechennja informacijnoji bezpeky ob'jektiv krytychnoji infrastruktury. Mizhnarodnyj naukovyj zhurnal "Internauka". Serija: "Jurydychni nauky". 2020. # 5. DOI: 10.25313/2520-2308-2020-5-6007.
10. Projekt Strateghiji kiberbezpeky Ukrajiny na 2021 – 2025 roky. veb-sajt: URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (data zvernennja 30.05.2021).
11. Stan zdijsnennja DPP v Ukrajini veb-sajt: URL: https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=9fc90c5e-2f7b-44b2-8bf1-1ffb7ee1be26&title=StanZdiisnenniaDppVUkraini (data zvernennja 30.05.2021).