

Ласуков О. Є. здобувач НУЦЗ України

Lasukov O. zdobuvach NUTsZ Ukrainy

**МЕХАНІЗМИ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У
ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І
ОБОРОНИ УКРАЇНИ**

**PUBLIC-PRIVATE PARTNERSHIP MECHANISMS IN ENSURING THE
CYBERSECURITY OF UKRAINE'S SECURITY AND DEFENCE SECTOR
BODIES**

Статтю присвячено проблемі поєднання ресурсів держави та приватного сектору в кіберзахисті органів сектору безпеки і оборони України. Збройна агресія, що супроводжується активними діями в кіберпросторі, перетворила його на повноцінну сферу протистояння, де противник діє системно й наполегливо, а державні інституції дедалі більше залежать від технологій, експертизи та інфраструктури приватних компаній. Проте така взаємодія досі тримається переважно на ситуативних домовленостях. Мета роботи полягає в обґрунтуванні теоретичних засад і визначенні напрямів удосконалення механізмів державно-приватного партнерства у забезпеченні кібербезпеки зазначених органів. Встановлено, що результативність партнерства визначається не так формою договірних відносин, як рівнем взаємної довіри, чітким розмежуванням відповідальності та наявністю процедур обміну інформацією про загрози, узгоджених із режимом захисту державної таємниці. Запропоновано розглядати партнерство як багаторівневий механізм із нормативно-правовим, організаційним, інформаційним і кадровим складниками та окреслено умови його поступової інституціоналізації.

Ключові слова: кібербезпека, державно-приватне партнерство, сектор безпеки і оборони, кіберзахист, механізми державного управління, обмін інформацією про загрози, кіберстійкість.

The article examines the problem of combining state and private sector resources in the cyber defence of Ukraine's security and defence sector bodies. The armed aggression, accompanied by active operations in cyberspace, has turned it into a fully-fledged domain of confrontation, where the adversary acts systematically and persistently, while state institutions have become increasingly dependent on the technologies, expertise and infrastructure of private companies. Yet this interaction still rests largely on ad hoc arrangements. The purpose of the study is to substantiate the theoretical foundations and identify directions for improving public-private partnership mechanisms in ensuring the cybersecurity of these bodies. It has been established that the effectiveness of partnership depends less on the form of contractual relations than on the level of mutual trust, a clear division of responsibility and the

existence of threat information sharing procedures aligned with the state secrets protection regime. The partnership is proposed to be viewed as a multi-level mechanism comprising regulatory, organisational, informational and human resource components, and the conditions for its gradual institutionalisation are outlined.

Keywords: *cybersecurity, public-private partnership, security and defence sector, cyber defence, public administration mechanisms, threat information sharing, cyber resilience.*

Постановка проблеми. Стратегія кібербезпеки України розглядає кіберпростір як самостійну сферу ведення бойових дій, що стоїть в одному ряду із сушею, морем, повітрям і космосом, і прямо це визнає. Широке застосування інформаційних технологій у секторі безпеки і оборони робить оборону держави вразливішою [1]. Для самих безпекових органів це давно не абстракція. Атаки на енергетичні об'єкти, масове ураження інформаційних систем державних установ і підприємств шкідливим програмним забезпеченням показали, що в умовах збройної агресії Російської Федерації кіберзагроза перестала бути суто технічною проблемою.

Держава не здатна самотужки закрити всі ці ризики. Технології виявлення атак, аналітичні компетенції, кваліфіковані кадри значною мірою зосереджені в приватному секторі – у розробників програмного забезпечення, операторів телекомунікацій, компаній, що надають послуги із захисту інформації. Стратегія відносить державно-приватне партнерство до принципів забезпечення кібербезпеки [1], а нещодавно ухвалений Закон України «Про основні засади забезпечення кібербезпеки України» передбачає державно-приватну взаємодію серед способів забезпечення функціонування національної системи кібербезпеки [2]. Проте для органів, що належать до сектору безпеки і оборони [3], питання про умови й межі допуску приватних партнерів до захисту власних систем лишається відкритим.

Не додає ясності й загальне законодавство про державно-приватне партнерство. Воно побудоване навколо створення чи управління об'єктом, інвестицій приватного партнера і тривалих договірних відносин, а кібербезпеки серед сфер його застосування немає [4]. Для діяльності, де предметом співпраці є не споруда, а інформація, експертиза й швидкість реагування, такі конструкції придатні лише частково. Це й зумовлює актуальність дослідження.

Аналіз останніх досліджень і публікацій. Проблема партнерства держави і бізнесу в кіберсфері має помітну наукову традицію. М. Данн Кавелті та М. Сутер, аналізуючи захист критичної інфраструктури, дійшли висновку, що партнерство не є універсальним рішенням, і запропонували мережеву модель урядування, в якій держава радше координує, ніж керує [5]. М. Карр показала, що очікування сторін тут часто розходяться. Держава вважає приватну інфраструктуру елементом національної безпеки, але не поспішає брати на себе мандат нагляду за безпекою мереж, а бізнес не готовий приймати відповідальність за безпеку держави [6]. Практичний бік справи розкрито в настановах ENISA, де побудову партнерства зведено до базових питань [7].

Серед вітчизняних праць варто назвати монографію Д. Дубова, який обґрунтував розгляд кіберпростору як нового виміру геополітичного суперництва і поставив питання захисту національних інтересів України в умовах протистояння в ньому [8]. А. Марущак і В. Панченко серед перешкод співпраці державного й приватного секторів виокремили бюрократизм, відмінності в технічному забезпеченні, загрозу розкриття комерційної таємниці та репутаційні ризики [9].

Утім, специфіка партнерства саме для безпекових і оборонних органів, де вимоги секретності й оперативності нерідко тягнуть у різні боки, вивчена значно менше. На цьому аспекті й зосереджено подальший виклад.

Виклад основного матеріалу. У вітчизняному правовому полі співіснують два близькі, але не тотожні терміни. Закон України «Про державно-приватне партнерство» описує партнерство як договірну конструкцію з доволі жорсткими ознаками (об'єкт, інвестиції приватного партнера, розподіл ризиків, тривалий строк співпраці) [4]. Закон України «Про основні засади забезпечення кібербезпеки України» оперує ширшою категорією державно-приватної взаємодії, яка до інвестиційної моделі не прив'язана [2]. Для сектору безпеки і оборони ця різниця має цілком практичне значення. Більшість того, що безпекові органи реально отримують від приватних компаній, – відомості про нові зразки шкідливого коду, експертні оцінки, допомога в розслідуванні інцидентів – у схему «об'єкт плюс інвестиції» просто не вкладається. Тому про партнерство тут доцільно говорити в широкому, управлінському значенні. Як про узгоджену й відносно стійку співпрацю, у межах якої сторони поєднують ресурси заради спільного результату та заздалегідь домовляються про розподіл відповідальності.

Під механізмом державно-приватного партнерства в цьому контексті ми розуміємо сукупність правових норм, організаційних структур, процедур і стимулів, через які держава залучає ресурси недержавних суб'єктів до кіберзахисту безпекових і оборонних органів, зберігаючи за собою функції координації та контролю. Визначення робоче. Проте воно дає змогу відразу відсікти дві крайнощі. Перша – уявлення про партнерство як про звичайну закупівлю, коли компанія постачає продукт і на цьому стосунки завершуються. Друга – думка, ніби бізнес може стати рівноправним учасником ухвалення рішень у сфері оборони. Жодна з них не відповідає ні природі сектору, ні логіці кіберзахисту.

Компанія зацікавлена в прибутку й репутації, орган безпеки – у виконанні завдання, і ці інтереси збігаються далеко не завжди. Крім того, режимом секретності, який обмежує не лише обмін інформацією, а й саму можливість пояснити партнерові, навіщо від нього щось потрібно. І нарешті, високою ціною відмови. Цивільна компанія може дозволити собі тимчасову недоступність сервісу, а для систем управління силами це неприйнятно. Звідси особлива роль довіри. Вона тут виступає не моральною категорією, а своєрідним ресурсом, який накопичується повільно, а втрачається миттєво.

Теоретичне підґрунтя такого підходу дає концепція мережевого урядування. М. Данн Кавелті та М. Сутер пропонують бачити державу не

диригентом, що керує кожним рухом оркестру, а координатором мереж, які значною мірою самоорганізуються [5]. Для цивільної критичної інфраструктури така модель виглядає природно. Для сектору безпеки і оборони її доводиться коригувати. Мережа тут неминуче ієрархізована, а доступ до неї розподілено нерівномірно. Держава не може поступитися керівною роллю там, де йдеться про секретну інформацію чи управління силами. Водночас спроба все зарегулювати відлякує саме тих партнерів, чия експертиза найцінніша. Знайти баланс між цими полюсами – мабуть, головне управлінське завдання.

Друга методологічна опора – проблема розподілу відповідальності. М. Карр звертає увагу на своєрідні «ножиці» очікувань. Держава хоче, щоб приватні власники мереж дбали про національну безпеку, але уникає прямого мандату, а бізнес готовий співпрацювати, проте відповідальності за державні інтереси на себе не бере [6]. О. Гівенс і Н. Буш застерігають від іншої пастки – розриву між декларованим і реальним партнерством [10]. Угоди підписано, робочі групи створено, а справжнього обміну цінною інформацією так і не виникає. Знайома картина. Для безпекових органів обидві проблеми загострюються, адже ціна помилки тут вища, а довіру важче вибудувати через закритість самих органів.

Третій елемент теоретичної рамки стосується типології партнерств. Дослідження Центру стратегічних і міжнародних досліджень показало, що проєктні партнерства з чітко визначеною метою, строками та підтримкою керівництва зазвичай успішніші за процесні, розраховані на тривалу співпрацю з менш чітко окресленими цілями [11]. Серед чинників стійкості там названо підтримку вищого керівництва, лідерство всередині самого партнерства, продуману інституційну конструкцію, баланс стимулів і вигод, а також вдало обраний момент для запуску. Настанови ENISA пропонують близьку за духом логіку. Перш ніж створювати партнерство, слід відповісти, навіщо воно потрібне, хто в ньому бере участь, як воно працюватиме, що саме робитиме і коли [7].

Варто враховувати й ширший контекст. Якщо, слідом за Д. Дубовим, розглядати кіберпростір як новий вимір геополітичного суперництва [8], то питання партнерства перестає бути суто відомчим. Компанії, що працюють на українському ринку кібербезпеки, самі стають учасниками цього суперництва, хочуть вони того чи ні. Їхні продукти, канали оновлення, центри обробки даних цілком можуть опинитися в полі зору іноземних спецслужб. Для держави це означає, що вибір партнера – рішення не лише технічне, а й стратегічне.

Нарешті, методологічно важливо не відривати тему від вітчизняного контексту. Стратегія кібербезпеки України поєднує принцип державно-приватного партнерства з принципами пріоритетного розвитку вітчизняного науково-технічного потенціалу та демократичного цивільного контролю над військовими формуваннями і правоохоронними органами [1]. Ці три принципи фактично задають межі, у яких партнерство для сектору безпеки і оборони взагалі можливе. Концепція розвитку сектору безпеки і оборони України серед завдань його реформування називає створення національної системи кібербезпеки та підвищення рівня координації і взаємодії [3]. Отже, співпраця з

бізнесом тут не самоціль, а інструмент набуття тих спроможностей, яких від сектору очікують.

Спираючись на ці положення, механізм партнерства доцільно розглядати як багаторівневий. Нормативно-правовий складник визначає, хто і на яких підставах може бути партнером, які обов'язки та гарантії виникають у сторін. Організаційний охоплює структури координації й процедури спільної роботи. Інформаційний складник – це правила обміну даними про загрози з урахуванням режимів доступу. Кадровий стосується способів залучення, підготовки та утримання фахівців. Окремо жоден із них не працює. Добре виписана норма без організаційної платформи лишається декларацією, а платформа без правил обміну інформацією швидко перетворюється на майданчик для доповідей.

Якщо перейти від теорії до практики, найочевиднішим напрямом партнерства є обмін інформацією про кіберзагрози. Стратегія кібербезпеки передбачає запровадження механізму обміну інформацією про загрози критичній інформаційній інфраструктурі між державними органами, приватним сектором і громадянами, а також протоколів спільних дій суб'єктів забезпечення кібербезпеки, зокрема інформаційного обміну в режимі реального часу під час виявлення атак [1]. Приватні компанії, що обслуговують велику кількість клієнтів, нерідко першими помічають нові зразки шкідливого програмного забезпечення. Безпекові органи, навпаки, володіють відомостями про цілі й методи противника, яких комерційний сектор не має. Проблема в тому, що ці два масиви інформації живуть за різними правилами.

Розв'язати це протиріччя, на нашу думку, можна через дворівневу модель. Відкритий контур охоплює технічні індикатори компрометації, знеособлені описи інцидентів, загальні рекомендації щодо захисту. До нього можна допускати широке коло партнерів, а сам обмін вести за заздалегідь погодженими правилами маркування, які показують, кому й за яких умов дозволено передавати отримані відомості. Закритий контур передбачає роботу з інформацією з обмеженим доступом, і доступ до нього мають лише ті компанії, що отримали дозвіл на провадження діяльності, пов'язаної з державною таємницею, а їхні працівники – відповідний допуск [12]. Схема на перший погляд проста. Її перевага в тому, що вона не змушує органи безпеки обирати між закритістю та корисністю.

Є ще одна, менш помітна умова успішного обміну – взаємність. Компанія, яка регулярно передає відомості про інциденти, але не отримує жодного зворотного зв'язку, досить швидко втрачає інтерес. Тож державна сторона має бути готова ділитися принаймні узагальненими результатами аналізу, пояснювати, як використано надану інформацію, і визнавати внесок партнерів там, де це не суперечить вимогам безпеки.

Показовим орієнтиром тут є європейський досвід. Директива Європейського Союзу щодо безпеки мережевих та інформаційних систем зобов'язує держави-члени визначити компетентні органи та команди реагування на комп'ютерні інциденти, налагодити їхню співпрацю, а операторів основних послуг – вживати належних заходів безпеки й повідомляти про суттєві інциденти [13]. По суті, добровільний обмін інформацією тут частково стає обов'язковим.

Пряме копіювання такої моделі для сектору безпеки і оборони навряд чи можливе, проте сам принцип – визначені обов'язки партнерів в обмін на передбачувані правила гри – заслуговує на увагу, тим більше що Стратегія орієнтує на сумісність зі стандартами ЄС і НАТО [1].

Особливої уваги потребує поведінка партнерства в кризових умовах. Стратегія кібербезпеки окремо згадує розвиток державно-приватного партнерства в запобіганні кіберзагрозам, реагуванні на кібератаки та усуненні їхніх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період [1]. Для сектору безпеки і оборони це, мабуть, найчутливіший аспект. Домовлятися про взаємодію тоді, коли атака вже триває, запізно. Порядок залучення приватних фахівців, канали зв'язку, повноваження сторін і межі доступу до систем мають бути погоджені заздалегідь і відпрацьовані на навчаннях, інакше в критичний момент партнерство існуватиме лише на папері.

Другий напрям – залучення приватної експертизи до оцінювання захищеності власних систем. Ідеться про незалежний аудит, тестування на проникнення, аналіз вразливостей програмного забезпечення, яке використовують органи сектору. Стратегія прямо говорить про розвиток системи незалежного аудиту інформаційної безпеки та запровадження кращих світових практик [1]. Для безпекових органів тут принципові дві речі. Перша – чітке розмежування. Що може перевіряти зовнішній виконавець, а що залишається виключно у сфері відповідальності власних підрозділів. Друга – перевірка самих партнерів. Стратегія вже передбачає обмеження участі в заходах із забезпечення інформаційної та кібербезпеки суб'єктів господарювання, що перебувають під контролем держави-агресора, а також використання їхньої продукції для захисту державних інформаційних ресурсів [1]. Цей принцип, як видається, варто розвинути до повноцінної процедури оцінювання надійності постачальників і підрядників, яка враховувала б структуру власності, походження програмних компонентів і попередню історію співпраці.

Третій напрям стосується людей. Жодна технологія не компенсує нестачі фахівців, а конкурувати з приватним сектором за кадри державні органи можуть далеко не завжди. Звідси інтерес до гнучких форм. Спільних кібернавчань, стажувань, залучення цивільних експертів як консультантів, формування резерву фахівців, готових підключитися до роботи в кризовий період. Стратегія передбачає і проведення кібернавчань суб'єктів сектору безпеки і оборони, і розвиток системи підготовки кадрів для його потреб [1]. Участь бізнесу та закладів освіти здатна наповнити ці заходи реальним змістом. Варто пам'ятати й про громадянське суспільство. Той самий документ допускає залучення волонтерських організацій до системи своєчасного виявлення кіберзагроз [1]. Завдання держави – дати цій енергії зрозумілі легальні рамки.

Четвертий напрям – науково-технічна кооперація. Принцип пріоритетного розвитку вітчизняного потенціалу для сектору безпеки і оборони має не лише економічний, а й суто безпековий зміст, адже залежність від іноземних, а тим паче сумнівних за походженням рішень сама по собі є вразливістю. Спільні дослідницькі проекти з вітчизняними компаніями й науковими установами,

замовлення на розроблення спеціалізованих засобів захисту, пілотні випробування добре вписуються в логіку проєктних партнерств, які, судячи із зарубіжного досвіду, приживаються легше за безстрокові [11].

Окремо слід сказати про інституційну платформу. Стратегія передбачила створення Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України [1], а закон визначив основних суб'єктів національної системи кібербезпеки [2]. Досвід загальноєвропейського партнерства EP3R підказує, що найкраще працюють невеликі робочі групи з вузьким завданням і визначеним строком, прості, але формальні правила, закладені на самому початку, відчутні стимули для участі компаній та публічне визнання досягнутих результатів [14].

Ще одна практична деталь – узгодженість самих державних учасників. Коли кілька органів сектору незалежно один від одного звертаються до тих самих компаній із подібними запитами, для бізнесу це означає зайві витрати й плутанину, а для держави – розпорошення зусиль. Доцільним видається принцип єдиного контактного пункту. Партнер має розуміти, куди повідомляти про інцидент і від кого чекати запиту, а розподіл отриманих відомостей між органами вже є внутрішньою справою держави.

Окреме питання – що отримує від такої співпраці приватна сторона. Якщо відповіді немає, партнерство тримається на ентузіазмі, а ентузіазм – ресурс вичерпний. Серед можливих стимулів варто назвати доступ до узагальнених даних про загрози, яких компанія не отримала б самостійно, участь у спільних навчаннях, репутаційні вигоди від співпраці з державою, прозорі й передбачувані правила участі в оборонних замовленнях. Не менш важливий і зворотний бік – відповідальність. М. Карр показує, що невизначеність у розподілі відповідальності та підзвітності є однією з найвразливіших ланок партнерських моделей у кіберсфері [6]. Тому в угоді варто прямо визначати, хто і за що відповідає в разі інциденту, як компенсуються витрати і в яких випадках приватний партнер не несе відповідальності за дії, вчинені на прохання державного органу.

Логіка поступової інституціоналізації, яку ми пропонуємо, виглядає так. Спочатку – проєктні партнерства під конкретні завдання, як спільне навчання, аудит окремої системи, розроблення засобу захисту. Вони дають змогу напрацювати довіру й зрозуміти, хто з партнерів справді надійний. Далі – закріплення успішних форматів у відомчих положеннях і типових угодах, де прописано розподіл відповідальності, порядок поводження з інформацією та гарантії для приватної сторони. Особливо це стосується захисту комерційної таємниці, адже побоювання щодо її розкриття дослідники відносять до помітних перешкод для співпраці [9]. І лише на завершальному етапі має сенс говорити про спеціальне законодавче регулювання, яке узагальнить практику, а не випереджатиме її.

Висновки. Проведене дослідження дає підстави для кількох висновків. Для органів сектору безпеки і оборони України державно-приватне партнерство в кіберсфері є не питанням вибору, а умовою формування необхідних спроможностей, оскільки значна частина технологій, експертизи та кадрів

зосереджена поза державним сектором. Водночас чинна модель державно-приватного партнерства, побудована навколо інвестиційних проєктів, відповідає потребам кіберзахисту лише частково. Основним правовим підґрунтям тут виступає ширша категорія державно-приватної взаємодії, закріплена законодавством про кібербезпеку.

Теоретичний аналіз показав, що партнерство в цьому секторі має поєднувати мережеву логіку координації з неминучою ієрархічністю самих безпекових і оборонних органів. Його результативність визначається не формою договору, а довірою, розподілом відповідальності та процедурами обміну інформацією, узгодженими з режимом захисту державної таємниці. Механізм партнерства доцільно розглядати як єдність нормативно-правових, організаційних, інформаційних та кадрових складників.

До основних практичних напрямів належать обмін інформацією про загрози за двоєвною моделлю з відкритими і закритими контурами, залучення приватної експертизи до аудиту захищеності, спільна підготовка фахівців і науково-технічна кооперація з вітчизняними розробниками. Обов'язковою умовою будь-якої з цих форм є процедура перевірки надійності партнерів. Інституціоналізацію варто вести поступово, від проєктних форматів через типові угоди до спеціального регулювання, що узагальнить напрацьовану практику.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. Офіційний вісник Президента України. 2016. № 10. Ст. 198.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 403.
3. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» : Указ Президента України від 14.03.2016 № 92/2016.
4. Про державно-приватне партнерство : Закон України від 01.07.2010 № 2404-VI.
5. Dunn Cavelty M., Suter M. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. 2009. Vol. 2, No. 4. P. 179–187. DOI: 10.1016/j.ijcip.2009.08.006.
6. Carr M. Public–private partnerships in national cyber-security strategies. *International Affairs*. 2016. Vol. 92, No. 1. P. 43–62.
7. Cooperative Models for Effective Public Private Partnerships : Good Practice Guide / European Network and Information Security Agency. ENISA, 2011. ISBN 978-92-9204-054-3.
8. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.

9. Марущак А. І., Панченко В. М. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. Інформаційна безпека людини, суспільства, держави. 2014. № 3 (16).
10. Givens A. D., Busch N. E. Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. *International Journal of Critical Infrastructure Protection*. 2013. Vol. 6, No. 1. P. 39–50. DOI: 10.1016/j.ijcip.2013.02.002.
11. Public-Private Partnerships for Critical Infrastructure Protection / Center for Strategic and International Studies. Washington, DC : CSIS, 2013.
12. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII.
13. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*. 2016. L 194. P. 1–30.
14. EP3R 2010–2013: Four Years of Pan-European Public Private Cooperation / European Union Agency for Network and Information Security. ENISA, 2014.

References:

1. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 15.03.2016 № 96/2016 [On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine of 15.03.2016 No. 96/2016]. (2016). *Ofitsiynyi visnyk Prezydenta Ukrainy*, 10, art. 198 [in Ukrainian].
2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine of 05.10.2017 No. 2163-VIII]. (2017). *Vidomosti Verkhovnoi Rady Ukrainy*, 45, art. 403 [in Ukrainian].
3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 bereznia 2016 roku «Pro Kontseptsiiu rozvytku sektoru bezpeky i oborony Ukrainy»: Ukaz Prezydenta Ukrainy vid 14.03.2016 № 92/2016 [On the decision of the National Security and Defense Council of Ukraine of March 4, 2016 "On the Concept of Development of the Security and Defense Sector of Ukraine": Decree of the President of Ukraine of 14.03.2016 No. 92/2016]. (2016) [in Ukrainian].
4. Pro derzhavno-pryvatne partnerstvo: Zakon Ukrainy vid 01.07.2010 № 2404-VI [On public-private partnership: Law of Ukraine of 01.07.2010 No. 2404-VI]. (2010) [in Ukrainian].
5. Dunn Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 2(4), 179–187. <https://doi.org/10.1016/j.ijcip.2009.08.006>
6. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43–62.

7. European Network and Information Security Agency. (2011). Cooperative models for effective public private partnerships: Good practice guide. ENISA.
8. Dubov, D. V. (2014). Kiberprostir yak novyi vymir heopolitychnoho supernytstva [Cyberspace as a new dimension of geopolitical rivalry]. Kyiv: NISD [in Ukrainian].
9. Marushchak, A. I., & Panchenko, V. M. (2014). Vzaiemodiia derzhavnoho ta pryvatnoho sektoriv u sferi kibernetychnoi bezpeky: inozemnyi dosvid ta perspektyvy dlia Ukrainy [Interaction of the public and private sectors in the field of cyber security: Foreign experience and prospects for Ukraine]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy*, 3(16) [in Ukrainian].
10. Givens, A. D., & Busch, N. E. (2013). Realizing the promise of public-private partnerships in U.S. critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, 6(1), 39–50. <https://doi.org/10.1016/j.ijcip.2013.02.002>
11. Center for Strategic and International Studies. (2013). Public-private partnerships for critical infrastructure protection. Washington, DC: CSIS.
12. Pro derzhavnu taiemnytsiu: Zakon Ukrainy vid 21.01.1994 № 3855-XII [On state secrets: Law of Ukraine of 21.01.1994 No. 3855-XII]. (1994) [in Ukrainian].
13. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (2016). *Official Journal of the European Union*, L 194, 1–30.
14. European Union Agency for Network and Information Security. (2014). EP3R 2010–2013: Four years of pan-European public private cooperation. ENISA.