УДК 51.86:659.3

МАЛАХОВ Г.Б., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-5333-0666.

ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ УКРАЇНИ

Анотація. *У статті досліджено зміст та форми державно-приватного партнерства у сфері кібербезпеки в Україні, актуальність даного напряму у контексті забезпечення кібербезпеки України. Проаналізовано досвід США та ЄС у сфері розвитку державно-приватного партнерства. Запропоновано актуальні напрями вдосконалення державно-приватного партнерства. Сформульовано пропозиції щодо вдосконалення чинного законодавства України щодо такого партнерства у сфері кібербезпеки.*

Ключові слова: *державно-приватне партнерство, шляхи удосконалення, кібербезпека, приватний сектор, інвестиції.*

Summary. *The article examines the content and forms of public-private partnership in the field of cyber security in Ukraine, the relevance of this direction in the context of cyber security of Ukraine. The experience of the USA and the EU in the field of public-private partnership development is analyzed. Actual areas of improvement of public-private partnership are proposed. Proposals for improving the current legislation of Ukraine regarding such a partnership in the field of cyber security have been formulated.*

Keywords: *public-private partnership, ways to improve, cyber security, private sector, investments.*

Постановка проблеми. Сьогодні державно-приватне партнерство (далі – ДПП) визнається як державами, так і недержавними суб'єктами ключовим елементом побудови дійсно ефективної системи кібербезпеки держави. Інтегрованість мереж державного та приватного секторів стає дедалі більш важливою для національної безпеки [1]. Україна максимально сприяє залученню до цього процесу представників приватного сектору, наукових та освітніх кіл, інститутів громадянського суспільства. У рамках ДПП залучаються інвестиції, які спрямовуватимуться на розбудову національної системи кібербезпеки. Стратегія кібербезпеки України містить згадки про розвиток ДПП.

У той же час, у цій Стратегії серед невирішених питань відзначається відсутність "дієвої моделі державно-приватного партнерства" у сфері кібербезпеки [2]. Також зазначається, що невирішеними залишаються питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів, що вказано як недолік попередньої Стратегії кібербезпеки 2016 року[2].

Результати аналізу наукових публікацій. Серед авторів наукових праць з питань розвитку ДПП слід зазначити таких українських науковців: В. Григоренко [3], Ю. Заскока [4], А. Марушак [5], А. Сороченко, В. Панченко [5], Р. Прав, Н. Ткачук [6], Б. Шулюк, В. Воротін, Я. Ізмайлов, І. Єгорова, Н. Малиновська, О. Крутій, О. Радченко, В. Козлов, Ю. Шимов, О. Федорчак, О. Кравченко та інші.

Спроба розпочати в Україні більш широку дискусію з цього питання, висвітлюючи, з одного боку, вже наявний досвід окремих західних держав у сфері побудови ДПП,

а з іншого – ключові українські проблеми в контексті створення КДПП, міститься в аналітичній доповіді “Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України” [1].

Значний внесок у розв’язання проблеми ДПП зробили зарубіжні вчені, серед яких слід виділити праці С. Ліндера [7], В. Коувенховена [8] та А. Ягасія [9].

Аналіз різних аспектів механізму державно-приватного партнерства, особливостей його становлення і розвитку в розвинутих країнах світу, також проводиться міжнародними організаціями і аналітичними центрами, серед яких слід виділити діяльність: Європейської економічної комісії ООН, Європейського інвестиційного банку, Міжнародної фінансової корпорації, Українського центру сприяння розвитку публічно-приватного партнерства, а також Національного інституту стратегічних досліджень, тощо. Проведений аналіз свідчить, що більшість досліджень механізму ДПП присвячені його економічній складовій і проводяться дослідниками у сферах культури, надання послуг, інфраструктурній галузі та інших [4].

Водночас, не достатньо дослідженими залишаються проблеми законодавчого, методичного та експертного забезпечення державно-приватного партнерства в сфері кібербезпеки України. Дискусійним залишається і питання того, в яких конкретно формах може реалізовуватись “справжнє” ДПП – тут так само відчувається брак методологічних напрацювань [1, с. 7]. Недостатніми є й організація і проведення наукових досліджень у сфері кібербезпеки. Ці обставини зумовлюють актуальність цієї статті.

Метою статті є удосконалення державно-приватного партнерства на базі аналізу нормативно-правової бази із забезпечення кібербезпеки, а також зарубіжного досвіду у цій сфері в контексті створення дієвої моделі такого партнерства.

Виклад основного матеріалу. Історичний тренд щодо участі приватного сектору в житті держави виник ще у кінці 70-х років ХХ ст. у країнах Заходу, що було пов’язано із глобальною економічною кризою того часу. І якщо перші проекти ДПП стосувалися передусім розвитку інфраструктури міст, екологічних проектів, охорони здоров’я та освіти, то в подальшому кількість сфер, до яких застосовується поняття ДПП, розширилось за рахунок нових або невідомих раніше форм співробітництва між державою та приватним сектором [7; 10].

Найбільш неоднозначним стало проникнення ДПП до сфери забезпечення державної безпеки, тобто туди, де держава традиційно зберігала свою монополію. Щоправда така монополія завжди була досить умовною: майже в усі періоди історії людства існували приклади специфічних державно-приватних відносин у сфері національної безпеки, однією з яких є відносини із забезпечення кібербезпеки [1, с. 6].

Ключове розуміння ДПП концентрується навколо мети та характеру такого партнерства.

Стівен Ліндер (Stephen Linder) характеризує цілі такого партнерства таким чином: “Метою ДПП є використання синергії у спільному інноваційному використанні ресурсів та застосуванні управлінських знань задля оптимального досягнення цілей усіх залучених сторін, якщо ці цілі не могли бути досягнуті без залучення цих сторін” [11]. Крім того, він слушно зазначає, що в межах ДПП обидві сторони, для забезпечення успішності партнерства, мають змінювати характер свого мислення – суб’єкти ДПП змушені думати та діяти як їх партнери, тобто державні учасники мають думати та діяти як підприємці, в т.ч. як бізнес має враховувати суспільний інтерес, і очікувати, що їм доведеться бути більш підзвітними громадськості [12].

Інший дослідник Вінсент Коувенховен (Vincent Kouwenhoven) конкретизує, що ДПП є неможливим без: взаємної довіри та встановлення обмежень, спрямованих на

недопущення зловживань; наявності чітких, недвозначних цілей та стратегії, яка зафіксована у документальному вигляді; чіткого розподілу ризиків; відповідальності, повноважень, а також функцій забезпечення партнерських бізнес-інтересів [8].

Доповнює цей підхід Арнав Ягасія (Arnav Jagasia), який вважає, що партнери мають ідентифікувати та визначити (detect) поведінку, яка викликає занепокоєння; учасники партнерства мають переконатися, що учасники – як від державного, так і приватного сектору – повністю погоджуються із засадами (standards) партнерства; ДПП має запропонувати механізм відповіді на ситуації після кіберзагроз (це включає аналіз атаки та виявлення рішень для обов'язкового вирішення уразливостей в атакованих системах) [9].

Водночас кібербезпекова сфера має свої унікальні аспекти, які ще не достатньо досліджені та не мають універсальних "рецептів" рішень (більше того, можливо, вони взагалі їх не мають) [1, с. 8]. Американська дослідниця М. Карр (Madeline Carr) звертає увагу, що навіть у США, де майже 15 років ДПП визначалось як ядро (cornerstone) національної системи кібербезпеки, сторонам так і не вдалося визначити параметри, характер та масштаби такого співробітництва [13].

Дискусійним залишається питання й про форми такої взаємодії, характер спільних дій, їх методологічне та організаційне забезпечення. Не менш дискусійним є питання, в яких саме сферах кібербезпеки може взагалі застосовуватись ДПП. Американські вчені виділяють чотири ключові сфери: 1) крадіжка даних у мережі (online identity theft); 2) індустріальне кібершпигунство; 3) захист критичної інфраструктури; 4) ботнети [14].

На думку українських дослідників, говорячи про таке партнерство, частіше за все мають на увазі дві макросфери: економіку в цілому (від якої залежить процвітання держави та її громадян) та критичну інфраструктуру (від роботи якої часто залежить безпека і держави, й її громадян). І перша, і друга сфери абсолютно переважно перебувають у руках приватних власників, але якщо кібератака на економічну міць держави матиме переважно фінансові наслідки, то кібератака на критичну інфраструктуру може призвести до людських жертв [1, с. 8].

При цьому є низка факторів, які є спільними для структур обох секторів, які можуть стати аргументом для формування ефективної моделі ДПП: організації мають негативний досвід бути атакованими і тепер хочуть усунути вразливості; організації розуміють, що вони дублюють зусилля; організації визнають, що існує недостатня координація чи/та обмін інформацією в певних секторах; організації визнають наявність провалів у забезпеченні всіх етапів життєвого циклу безпеки; організації визнають, що загрози розвиваються разом із подальшим злиттям комунікацій та інформаційних технологій, а отже, потребують спільної відповіді, а не розподіленої по окремих секторах; організації визнають злиття загроз від тероризму та кібератак; організації визнають, що загрози еволюціонують та зміщуються з національного/секторального рівня на міжнародний; спостерігається брак довіри між конкурентами в межах географічних, секторальних або тематичних сфер, а отже, існує потреба у створенні довіреної структури для вирішення цієї проблеми [1, с. 12].

Важливим компонентом посилення спроможностей держави у сфері забезпечення кібербезпеки є саме побудова конструктивного діалогу у форматі державно-приватного партнерства [3, с. 156]. Користь від спільної робити з кібербезпеки взаємна як для державного, так і приватного секторів.

Візьмемо як приклад досвід США, оскільки саме ця країна є піонером у галузі ДПП. Так як приватний сектор контролює більшу частину критичної інфраструктури США, що часто є привабливою для дій кіберзлочинців, багато приватних компаній уже

мають програми з кібербезпеки, володіють спеціальними знаннями та досвідом у вирішенні потенційних загроз. Державний сектор, зі свого боку, має ширші можливості для розслідування кіберзлочинів та переслідування кіберзлочинців [1, с. 15].

Уперше питання необхідності спільного з приватним сектором захисту кіберпростору було висвітлено у Директиві про рішення Президента США "Про захист критичної інфраструктури" № 63 (Critical Infrastructure Protection, Presidential Decision Directive 63 (PDD) від 1998 р., де визначено захист критичної інфраструктури та ключових ресурсів (CIKR) як національну ціль, реалізація якої уможливила співпрацю між урядом та приватним сектором з метою захисту кіберсистем [15].

Відповідно до цієї Директиви, для кожного з основних секторів економіки, які є вразливими до інфраструктурної атаки, федеральний уряд призначає представника сектору для зв'язків з приватним сектором (Sector Liaison Offi cial), який після обговорення та узгодження з суб'єктами приватного сектору визначає Координатора сектору (Sector Coordinator) для представлення приватного сектору. Разом ці дві особи, а також відомства та корпорації, які вони представляють, сприяють розробленню галузевого плану національної інфраструктури шляхом: оцінки вразливості сектору до кібер- або фізичних атак; надання рекомендацій щодо усунення вразливості; пропозиції щодо системи виявлення та запобігання спробам потужних атак; розроблення плану для оповіщення про атаки, з подальшим швидким відновленням мінімально необхідного потенціалу після атаки [1, с. 15-16].

Цією ж Директивою в рамках національної системи попередження та обміну інформацією з питань кібербезпеки в межах ФБР був створений Центр захисту державної інфраструктури (National Infrastructure Protection Center, NIPC), функцією якого є оцінка загроз, попередження, виявлення вразливостей державної критичної інфраструктури та сприяння правоохоронним органам у розслідуванні та реагуванні кіберінцидентів [1, с. 22]. Крім того, цей Центр встановлює партнерські відносини безпосередньо з компаніями приватного сектору та зі структурами з обміну та аналізу інформації, які створені приватним сектором.

Більшість обмінів інформацією приватного сектору проводяться за допомогою центрів обміну та аналізу інформації, які створюються як неприбуткові організації, і являють собою ресурс для збору інформації про кіберзагрози для об'єктів критично важливої інфраструктури та забезпечення двостороннього обміну інформацією між приватним та державним сектором [1, с.19]. Ключовим напрямом діяльності є двосторонній обмін інформацією: партнери надають індикатори зафіксованих кіберзагроз та інформацію про кіберінциденти та виявлені вразливі місця Міністерству внутрішньої безпеки США [1, с. 20].

Позитивним прикладом сучасних моделей паритетної взаємодії державного та приватного секторів у сфері забезпечення кібербезпеки є створення на базі Департаменту внутрішньої безпеки США автоматизованої програми відстеження кіберзагроз, яка надає змогу забезпечити автоматизований обмін інформацією між державним і приватним секторами [3, с. 158].

Також у США з метою прогнозного супроводження діяльності державних інституцій та приватного сектору у сфері забезпечення кібербезпеки створено некомерційний дослідний центр "TechAmerica Foundation", який об'єднує фахівців та експертів 1200 компаній з метою визначення орієнтовно-планових обсягів щорічного фінансування кібероборони, при цьому акценти діяльності постійно передбачають значне збільшення витрат виходячи із потенційних та реальних кіберзагроз [3, с. 158].

Окремим документом, що фіксує процедури співпраці між приватними компаніями та урядовими установами у сфері інформаційної безпеки є “Акт про обмін інформацією у сфері кібербезпеки” (Cybersecurity Information Sharing Act, CISA), затверджений Конгресом наприкінці 2015 р. [16]. Відповідно до нього організації, які на добровільній основі обмінювалися інформацією про кіберзагрози між собою і Федеральним урядом, отримали право обмеженої відповідальності. Документ надає додатковий захист компаніям, що добровільно вирішили ділитися даними про кіберзагрози з урядовими установами [1, с. 19].

Цікавим видається досвід ЄС у цій площині. На рівні ЄС метою ДПП є створення платформи для кібербезпеки різних секторів (таких як енергетика, охорона здоров’я, транспорт та фінанси, а також включення у цей процес органів влади, науково-дослідних центрів та інших зацікавлених сторін), яка розвивала б дослідницький та інноваційний потенціал приватного сектору [1, с. 23].

Основою ініційованого Європейською Комісією загального плану дій слугують: Стратегія єдиного цифрового ринку 2015 р. (Digital Single Market Strategy for Europe) [17], Кіберстратегія Європейського Союзу 2013 р. (Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace) [18] та Директива ЄС щодо мережевої та інформаційної безпеки (NIS Directive on security of network and information systems) [19]. Невипадково у стратегічних документах ЄС з кібербезпеки неодноразово наголошується на важливості розбудови державно-приватного партнерства в боротьбі з кібератаками і кіберзлочинністю [3, с. 159].

Ухвалена у 2013 р. Європейська стратегія кібербезпеки визначила головні напрями політики Європейського Союзу у сфері забезпечення безпеки кіберпростору [20].

Відповідно до цієї Стратегії Європейська Комісія запропонувала перший всеосяжний елемент законодавства ЄС щодо кібербезпеки [1, с. 24] – Директиву ЄС щодо мережевої та інформаційної безпеки (NIS Directive on security of network and information systems), ухвалену Європейським Парламентом 6 липня 2016 р., яка набрала чинності в серпні 2016 р. [21].

Ця Директива передбачила створення координаційного механізму реагування держав-членів у співпраці з приватним сектором на погрози та власне самі кібератаки, тим самим сприяючи стратегічному співробітництву та обміну інформацією і підтримуючи рівень довіри між учасниками процесу. Комісія також запустила державно-приватну платформу на рівні ЄС – т.зв. платформу мережевої та інформаційної безпеки (Network and Information Security public private Platform) для визначення ефективної практики кібербезпеки з метою сприяння подальшому впровадженню Директиви [1, с. 24-25].

На основі узагальнення здобутків зарубіжного досвіду ДПП у сфері забезпечення кібербезпеки можна виділити такі його складові: основною його метою є побудова конструктивного діалогу та плідної співпраці, реальна довіра між приватним сектором та державними інституціями; заохочення співпраці між державними та приватними організаціями на ранніх етапах дослідницького та інноваційного процесу [3, с. 160].

Досвід США та ЄС у цій сфері є корисним для України, органи влади якої постійно працюють над кібербезпекою на національному та міжнародному рівні. Наша країна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини,

Забезпечення розвитку державно-приватного партнерства у сфері в кібербезпеки є одним з пріоритетних завдань національної політики України.

На національному рівні під пріоритетними завданнями державно-приватного партнерства в сфері кібербезпеки, як правило, розуміють розширення взаємодії держструктур з приватними науковими установами, громадськими об'єднаннями та волонтерським організаціями, в тому числі в підготовці кадрів, а також підвищення цифрової грамотності громадян і культури безпеки поведінки в кіберпросторі [4]. З цього приводу СБУ зазначає, що "державно-приватна взаємодія є одним з головних принципів забезпечення кібербезпеки держави, який передбачає широку співпрацю з громадянським суспільством у сфері кібербезпеки і кіберзахисту. …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" [22].

Нова Стратегія кібербезпеки України визначає пріоритети забезпечення кібербезпеки України та стратегічні цілі, що мають бути досягнуті протягом періоду реалізації цієї Стратегії. Зазначається, що для формування потенціалу стримування (С) необхідним є досягнення стратегічних цілей, серед яких виділяється ціль С.4. "Розвиток асиметричних інструментів стримування" – "Україна створить необхідні умови для забезпечення стримування агресивних дій у кіберпросторі проти України шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу приватного сектору" [2].

Для досягнення цієї цілі Україна має запровадити асиметричні інструменти стримування шляхом: врегулювання на законодавчому рівні питання щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі; розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі; запровадження на постійній основі оцінки стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановлення обов'язковості та періодичності проведення такої оцінки з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору; проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів [2].

У Стратегії передбачається, що для досягнення стратегічних цілей Україна у взаємодії з приватним сектором сформує ефективну модель відносин у сфері кібербезпеки, засновану на довірі, шляхом 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 проектів у цій сфері [2].

Основні шляхи державно-приватного партнерства у сфері в кібербезпеки визначені у ст. 10 Закону України "Про основні засади забезпечення кібербезпеки України", де згадується: 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, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі [23].

З приводу останнього слід зауважити, що в Україні на ринку кібербезпеки діє досить багато асоціацій, ІТ-компаній, структур громадянського суспільства, які мають значний досвід і техніко-технологічні напрацювання в зазначеній сфері, надають послуги з виявлення комп'ютерних атак, розслідування обставин виявлених інцидентів, формування доказів при виконанні обстеження комп'ютерних систем і проведенні комп'ютерних експертиз. Чимало вітчизняних ІТ-компаній, які посіли міцні позиції в зазначеній сфері, не тільки демонструють високу ефективність, напрацювали багаторічний досвід, мають значний штат компетентних фахівців та експертів необхідної кваліфікації, але й проявляють зацікавленість у розширенні своєї діяльності, опануванні нових сегментів ринку послуг кібербезпеки [3, с. 160].

Як у Законі України "Про основні засади забезпечення кібербезпеки України", так і в Стратегії кібербезпеки України держава декларує готовність до системної роботи щодо розвитку ДПП у сфері забезпечення кібербезпеки.

Іншим важливим законодавчим актом є Закон України "Про державно-приватне партнерство", за змістом якого проекти ДПП повинні відповідати таким основним критеріям: 1) мати довготривалий характер (понад п'ять років); 2) передбачати передання приватному партнеру частини ризиків у процесі реалізації проектів; 3) мати вищі техніко-економічні показники ефективності, ніж у разі реалізації без участі приватного партнера [24]. Але, на жаль, сфера забезпечення кібербезпеки у зазначеному законі не фігурує в переліку сфер застосування ДПП (стаття 4). Не достатньо визначеними залишаються й форми такої взаємодії.

Серед основних форм реалізації ДПП виділяються: контракти на виконання визначених робіт і надання послуг, взаємне консультування, інформаційний обмін, спільне ведення баз даних, незалежна експертиза проектів нормативно-правових актів, підготовка і внесення спільних пропозицій щодо реалізації державної політики в кіберпросторі, захисту внутрішнього ринку ІТ-послуг, державну підтримку підприємств ІТ-бізнесу, інформаційне забезпечення державних і комерційних підприємств, громадських об'єднань і громадян з питань забезпечення кібербезпеки тощо. Інструменти ДПП можуть бути ефективно задіяні для залучення приватних інвестицій у фінансування високобюджетних проектів [4]. До речі, зарубіжний досвід свідчить, що державно-приватні інвестиції активно спрямовуються на дослідницькі програми щодо

розробки інструментів та прототипів у сфері посилення кіберзахисту та його складових [3, с. 160].

Певні елементи удосконалення ДПП містяться в проєкті Закону України "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" (реєстр. № 8087 від 29.09.2022 р.). Зокрема, положення проекту передбачають створення національної системи реагування на інциденти кібербезпеки, зміст якої передбачає: порядок надання приватними командами реагування послуг з управління інцидентами кібербезпеки для операторів критичної інфраструктури, органів державної влади та місцевого самоврядування; взаємодію в установленому порядку з суб'єктами приватного сектору, в тому числі, з іноземними суб'єктами господарювання, з питань реагування; закріплення обов'язку операторів критичної інфраструктури повідомляти про всі значні інциденти кібербезпеки, кібератаки щодо об'єктів критичної інформаційної інфраструктури [25].

Серед ключових напрямів у сфері ДПП СБУ відповідно до своєї компетенції виділяє: надання власникам та операторам критичної інфраструктури інформації щодо виявлення кібератак та/або кіберінцидентів, вразливостей власних систем кіберзахисту; розроблення організаційно-правових засад та безпосереднє залучення фахівців приватного сектору (в т. ч. хактивістів) до проведення негласних перевірок готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів; організація на базі провідних ІТ-компаній тренінгів та навчальних програм з підвищення кваліфікації для фахівців СБ України; забезпечення виконання операторами та провайдерами телекомунікацій положень Конвенції РЄ про кіберзлочинність у частині термінового збереження та надання на вимогу компетентного правоохоронного органу даних, необхідних для протидії кіберзлочинності [22].

На сьогодні проблемним питанням залишається відсутність ефективного правового механізму щодо отримання в інтересах забезпечення національної безпеки від операторів та провайдерів телекомунікацій комп'ютерних даних, необхідних для своєчасного реагування на кіберзагрози, у т.ч. попередження і локалізації кіберінцидентів та кібератак на критичну інформаційну інфраструктуру [6, с. 106].

Висновки.

ДПП визнається як ключовий елемент кібербезпекової системи держави, який вимагає максимального ресурсного забезпечення. Хоча більшість розвинених країн мають тією чи іншою мірою працюючі форми ДПП, однак майже в кожному випадку вони формуються у режимі ad-hoc і під значним впливом історичного досвіду кожної конкретної країни. Зокрема, позитивним вбачається законодавчий досвід США у площині взаємного обміну інформацією про кіберзагрози між урядом та приватним сектором. У ЄС у межах пошуку ефективних форм ДПП проводяться програми консультацій з великим, малим та середнім бізнесом, асоціаціями, дослідницькими інституціями, громадським сектором, органами державної влади та органами регіонального рівня, що може стати основою відповідного процесу, якого потребує Україна [1, с. 71].

Питання створення загальнонаціональної системи ДПП все ще залишається надзвичайно складним. ДПП потребує удосконалення в контексті створення дієвої моделі державно-приватного партнерства у сфері кібербезпеки. Серед актуальних напрямів розвитку ДПП доцільно виділити:

- формування довіри приватного сектору до державних суб'єктів забезпечення кібербезпеки в контексті створення основи для "обміну інформацією", контролю за інформацією з обмеженим доступом;

- ініціювання проектів, які б могли розвивати ДПП в нашій країні, у т.ч. активізація залучення інвестицій у цивільний сектор кібербезпеки, покращення фахової підготовки спеціалістів у цій сфері, спільної діяльності щодо організації дієвого кіберзахисту [3, с. 161], залучення експертів до розслідування кіберінцидентів;
- створення стратегії ДПП у сфері забезпечення кібербезпеки, зміст якої передбачатиме: формування цілей ДПП (як для держави, так і приватного сектору); визначення критеріїв, за яких ДПП стане привабливим рішенням для обох сторін; здійснення системних заходів, спрямованих на посилення довіри учасників ДПП один до одного; допомога з боку неурядових структур та науково-експертного співтовариства обом сторонам у формуванні довгострокових стратегій такого партнерства; пошук ефективних підходів до визначення ризиків для кожної із сторін, а також відповідальності сторін;
- реалізація законодавчо визначених (ст. 10 Закону України "Про основні засади забезпечення кібербезпеки України") шляхів державно-приватного партнерства у сфері в кібербезпеки;
- визначення взаємовідношення державно-приватного партнерства та державно-приватної взаємодії у сфері кібербезпеки. Зокрема, чи є така взаємодія різновидом державно-приватного партнерства, та відповідно, чи підпадає під дію Закону України "Про державно-приватне партнерство" [6, с. 109]; у разі такого визнання внесення до переліку сфер застосування державно-приватного партнерства, визначених у статті 4 цього Закону сферу кібербезпеки та кіберзахисту [1, с. 76; 6, с.109];
- механізми та процедури галузевого регулювання захисту об'єктів кібербезпеки з врахуванням можливості ДПВ у цій сфері (зокрема, запровадження недержавних галузевих регуляторів, що довело свою ефективність у міжнародних практиках) [1, с. 76].

Реалізації зазначених напрямів сприятиме розвиток дискусій між обома сторонами партнерства із залученням фахівців та науковців у цій сфері.

Використана література

1. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberb ezpeka.pdf

2. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 19.09.2023).

3. Григоренко В.А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки. *Інформація і право*. № 2(37)/2021. С.155-161.

4. Заскока Ю.В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. *Наукові перспективи*. 2021. № 9 (15). URL: http://perspectives.pp.ua/index.php/np/article/view/467/470

5. Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. *Інформаційна безпека людини, суспільства, держави*. 2014. № 3(16). С. 58-59.

6. Ткачук Н.А. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки. *Інформація і право*. 4(27)/2018. С. 104-111. URL: https://ippi.org.ua/tkachuk-na-pravove-regulyuvannya-vza%D1%94modii-sluzhbi-bezpeki-ukraini-z-privatnim-sektorom-u-sferi-zabe

7. Linder S. Coming to terms with the Public-Private Partnership – A grammar of multiple meanings. Public-Private Policy Partnerships / P. Vaillancourt Rosenau (Ed.). The MIT Press, Cambridge MA, 2000. P. 19-36.

8. Kouwenhoven V., Public-Private Partnership: A model for the management of Public-Private cooperation Modern Governance / J. Kooiman (Ed.). New Government-Society Interactions, Sage, London, 1993. P. 119-130.

9. A Look into Public Private Partnerships for Cybersecurity. URL: https://publicpolicy.wharton.upenn.edu/live/news/1815-a-look-into-public-private-partnerships-for.

10. Cavelty Myriam Dunn, Suter Manuel. Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. December, 2009. Vol. 2, Is. 4. P. 179-187.

11. Linder S., Vaillancourt P. Rosenau, Mapping the terrain of the Public-Private Policy Partnership. Public-Private Policy Partnerships. P. Vaillancourt Rosenau (Ed.). The MIT Press, Cambridge, MA, 2000. P. 1-19.

12. Linder, S. H. Coming to Terms With the Public-Private Partnership: A Grammar of Multiple Meanings. *American Behavioral Scientist*. 1999. № 43(1). P. 35-51. DOI: 10.1177/0002764992195 5146.

13. Madeline Carr. Public-Private partnerships in national cyber-security strategies. URL: https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

14. Moore T. Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. URL: https://www.nap.edu/read/12997/chapter/3

15. Presidential Decision Directive/NSC-63. URL: https://fas.org/irp/off docs/pdd/pdd-63.htm

16. Cybersecurity Information Sharing Act of 2015. URL: https://www.congress.gov/bill/114 thcongress/senate-bill/754/text

17. Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the Committee of the regions. URL: http://eur-lex. europa.eu/legal-content/EN/ TXT/?uri=celex%3A52015DC0192

18. Повідомлення про стратегію кібербезпеки Європейського Союзу – відкритий та безпечний кіберпростір. URL: https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-europeanunion-%E2 %80 %93-open-safe-and-secure-cyberspace

19. Директива про захист мережевих та інформаційних систем (Директива щодо ННД) URL: https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

20. Стратегія кібербезпеки Європейського Союзу: відкритий та безпечний кіберпростір. URL: http://eur-lex.europa.eu/procedure/EN/202369

21. Директива Європейського Парламенту та Ради (ЄС) 2016/1148 від 6 липня 2016 року щодо заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri= uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

22. Лист Служби безпеки України № 30/5/2-3288 від 05.03.18 р. на запит НІСД № 293/54 від 31.01.18 р.

23. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19

24. Про державно приватне партнерство: Закон України від 01.07.10 р. № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text

25. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проєкт Закону України (реєстр. № 8087 від 29.09.2022 р.). URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881 (дата звернення: 19.09.2023).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~