УДК: 351.86:659.3

[https://doi.org/10.52058/2708-7530-2021-9\(15\)-85-98](https://doi.org/10.52058/2708-7530-2021-9(15)-85-98)

Заскока Юрій Вікторович аспірант кафедр глобальної та національної безпеки ННІ Публічного управління та державної служби, КНУ імені Тараса Шевченка, вул. Антона Цедіка, 20, м. Київ, 03057, тел.: (067) 567-26-40, e-mail: 33xcupe@gmail.com, <https://orcid.org/0000-0001-8984-2623>

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО В СФЕРІ КІБЕРБЕЗПЕКИ УКРАЇНИ: СТАН ТА ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ

Анотація. У статті досліджено зміст та форми державно-приватного партнерства (ДПП) у сфері кібербезпеки в Україні, актуальність даного напрямку взаємодії держави та суб'єктів громадянського суспільства у контексті забезпечення кібернетичної безпеки України. Запропоновано актуальні напрями вдосконалення розробки партнерських угод між структурами сектора безпеки та оборони з вітчизняними ІТ-компаніями на принципах державно-приватного партнерства, серед яких: проведення комп'ютерно-технічних експертиз інформаційних ресурсів, збір цифрових доказів, розробка та впровадження програмного забезпечення для виявлення і запобігання кіберзагроз, моніторинг кіберпростору, технології аналізу великих даних (Big Data), формування законодавства щодо ДПП у сфері кібербезпеки, підготовка фахівців для даної сфери. Розкривається їх сутність та завдання у вирішенні даних актуальних завдань сфери кібербезпеки. Сформульовано пропозиції щодо вдосконалення чинного законодавства України щодо ДПП у сфері кібербезпеки.

У статті наголошується про необхідність розробки комплексної стратегії розвитку недержавного сектора забезпечення кібербезпеки, що враховує інтереси всіх сторін і в якій був би узагальнений позитивний вітчизняний та зарубіжний досвід організації ДПП в сфері забезпечення кібербезпеки.

Зазначається, що реалізація такої стратегії доцільна в рамках національної програми, яка передбачає: закріплення керівних принципів стимулювання державно-приватного партнерства в зазначеній сфері та оптимальних умов для довготривалого дотримання домовленостей і досягнення цільових показників та індикаторів; вдосконалення системи управління та координації відповідних процесів на національному, міжрегіональному, регіональному, муніципальному рівнях; забезпечення привілейованого доступу сторін до додаткових ресурсів, облік потенційних комерційних зисків для представників приватного сектора, заохочення ініціативних проєктів з розвитку взаємодії і об'єднання ресурсних можливостей; страхування потенційних ризиків тощо.

Ключові слова: державно-приватне партнерство, кібербезпека, кіберзахист, сектор безпеки та оборони, Стратегія кібербезпеки України.

Zaskoka Yurii Viktorovich Graduate student of the Departments of Global and National Security, Institute of Public Administration and Civil Service, Taras Shevchenko National University, Anton Tsedik St., 20, Kyiv, 03057, tel.: (067) 567-26-40, e-mail: 33xcupe@gmail.com, <https://orcid.org/0000-0001-8984-2623>

PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF CYBER SECURITY OF UKRAINE: STATE AND PROBLEMS OF PROVIDING

Abstract. The article examines the content and forms of public-private partnership (PPP) in the field of cybersecurity in Ukraine, the relevance of this area of interaction between the state and civil society in the context of cyber security of Ukraine. The current directions of improving the development of partnership agreements between the structures of the security and defense sector with domestic IT companies on the principles of public-private partnership are proposed, including: conducting computer and technical examinations of information resources, collecting digital evidence, developing and implementing software for detection and cyber threat prevention, cyberspace monitoring. Big Data analysis technologies, formation of PPP legislation in the field of cybersecurity, training of specialists in this field. Their essence and tasks in solving these current problems in the field of cybersecurity are revealed. Proposals for improving the current legislation of Ukraine on PPP in the field of cybersecurity have been formulated.

The article emphasizes the need to develop a comprehensive strategy for the development of the private sector of cybersecurity, which takes into account the interests of all parties and which would summarize the positive domestic and foreign experience of PPP in the field of cybersecurity.

It is noted that the implementation of such a strategy is appropriate within the national program, which provides for: consolidation of guidelines for stimulating public-private partnership in this area and optimal conditions for long-term compliance with agreements and achievement of targets and indicators; improving the management system and coordination of relevant processes at the national, interregional, regional, municipal levels; ensuring privileged access of the parties to additional resources, accounting for potential commercial benefits for the private sector, encouraging initiative projects to develop interaction and pooling of resource opportunities; insurance of potential risks, etc.

Keywords: public-private partnership, cyber security, cyber defense, security and defense sector, Cyber security strategy of Ukraine.

Постановка проблеми. Відносини влади і бізнесу в сучасному суспільстві зазнають суттєвих змін. У більшості країн взаємодія між органами державної влади та комерційними організаціями сприймається як найважливіша умова і одна з найбільш перспективних механізмів вирішення складних соціальних

проблем. В основному така взаємодія забезпечується через державно-приватне партнерство (ДПП), яке активно розвивається і в Україні. Однак до недавнього часу багато питань його практичної реалізації в правовому плані не були врегульовані.

Сьогодні розвиток державно-приватного партнерства у сфері в кібербезпеки - одне з пріоритетних завдань державної політики України відповідно до закону «Про основні засади забезпечення кібербезпеки України» (2017)[1]. У 2021 році прийнято нову Стратегію кібербезпеки України, в якій закорема наголошується, що серед невирішених питань даної сфери залишається відсутність «дієвої моделі державно-приватного партнерства» у сфері кібербезпеки.[2].

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. У тексті нової Стратегії національної безпеки 2021 року зазначається, що недоліками попередньої Стратегії кібербезпеки 2016 року було те, що участь у її реалізації «переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучалися інші державні органи, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучалися заклади освіти та наукові установи». [2].

Серед стратегічних завдань сектору безпеки у сфері кіберзахисту Стратегія визначила необхідність досягнення різних стратегічних цілей. Зокрема, для досягнення цілі – Розвиток асиметричних інструментів стримування – «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, всебічне 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». Для досягнення цілі - Формування нової моделі відносин у сфері кібербезпеки - Україна у взаємодії з приватним сектором сформує ефективну модель відносин у сфері кібербезпеки, засновану на довірі. [2].

Аналіз останніх досліджень і публікацій. Вивчення проблеми формування і розвитку державно-приватного партнерства і його застосування для реалізації масштабних суспільно значимих проектів, знаходиться на перетині різних наук, а саме: економіки, права, фінансів, державного та публічного управління, тощо. При цьому економічна складова партнерства між державою і приватним бізнесом в основному розглядається науковцями як базисна і така, що має основне значення. Вчені досліджують моделі, форми, фактори розвитку, переваги й

недоліки, галузеві й територіальні особливості, інвестиційні й нормативно-правові механізми, ризики, соціально-економічні наслідки, міжнародні та інші аспекти державно-приватного партнерства.

Аналіз різних аспектів механізму державно-приватного партнерства, особливостей його становлення і розвитку в розвинутих країнах світу, також проводиться міжнародними організаціями і аналітичними центрами: Європейської економічної комісії ООН, Європейського інвестиційного банку, Міжнародної фінансової корпорації, Українського центру сприяння розвитку публічно-приватного партнерства, фахівцями Національного інституту стратегічних досліджень, тощо.

Серед авторів наукових праць та досліджень питань розвитку державно-приватного партнерства слід зазначити таких українських науковців: А.Сороченко, Р.Прав, Б.Шулюк, В.Воротін, Я.Ізмайлов, І.Єгорова, Н.Малиновська, О.Крутий, О.Радченко, В.Козлов, Ю.Шимов, О.Федорчак, О.Кравченко та інші.

Аналіз праць науковців дозволяє дійти висновку, що механізм державно-приватного партнерства давно відомий та успішно впроваджується у світі. Довіра та партнерські відносин між державним та приватним партнерами дозволяють ефективно реалізовувати суспільно значущі проекти, при оптимальному розподілі ресурсів та дозволяють отримати вигоду всіма учасниками процесу, а також задовольнити потреби громадськості.

Проведений аналіз також свідчить, що більшість досліджень механізму державно-приватного партнерства присвячені його економічній складовій і проводяться дослідниками у сферах культури, надання послуг, інфраструктурній галузі та інших. Проблеми застосування державно-приватного партнерства в сфері кібербезпеки та кіберзахисту України не є достатньо дослідженими. Тож відсутність системних досліджень зазначеної проблематики, незважаючи на її виняткове значення для забезпечення кібербезпеки України, зумовлюють необхідність проведення нашого дослідження.

Мета статті. Автор статті ставить за мету дослідити зміст та форми державно-приватного партнерства (ДПП) у сфері кібербезпеки в Україні та охарактеризувати проблеми його забезпечення. Сформулювати актуальні напрями вдосконалення розробки партнерських угод між структурами сектора безпеки та оборони з вітчизняними ІТ-компаніями на принципах державно-приватного партнерства.

Виклад основного матеріалу. У 2017 року Рада національної безпеки і оборони України в рамках розвитку державно-приватного партнерства в сфері кібербезпеки [3] доручила безпосередньо Кабінету міністрів України [4] відпрацювати механізми залучення за допомогою аутсорсингу приватних компаній і приватних осіб до виконання завдань кіберзахисту державних електронних інформаційних ресурсів.

З розвитком процесу цифровізації економіки та великою інтегрованістю

інтернет-ресурсів необхідність взаємодії з приватним сектором і громадськістю диктується і тим, що для проведення кібератак на інформаційні ресурси держорганів часто використовуються поставлені під віддалений контроль комп'ютери та електронні ресурси приватних користувачів. На думку Як українського експерту з кібербезпеки Анатолія Дробахи (в минулому - гендиректор «Укрспецзв'язку»), для вибудовування ефективної національної системи кібербезпеки заходів, що вживаються тільки державою недостатньо – потрібне ефективне державно-приватне партнерство і активна участь експертного співтовариства і громадянського суспільства у процесах кіберзахисту.

На вітчизняному ринку кібербезпеки вже діє досить багато великих компаній, які мають значний досвід і технічні напрацювання в зазначеній сфері, вони надають послуги з виявлення комп'ютерних атак, проведення розслідування обставин виявлених кіберінцидентів, формування доказів при виконанні обстеження комп'ютерних систем і проведенні комп'ютерних експертиз. Багато вітчизняних компаній, які зайняли міцні позиції в зазначеній сфері, не тільки демонструють високу ефективність, напрацювали багатий досвід, містять значний штат фахівців необхідної кваліфікації, але і проявляють зацікавленість в розширенні своєї діяльності, завоюванні нових сегментів ринку послуг кібербезпеки. Такі компанії поряд з структурами системи безпеки та оборони країни безумовно можуть і повинні включатися в систему забезпечення кібербезпеки України. Зрозуміло, в даній сфері в ролі головного регулятора повинні виступати державні структури, що зберігають за собою особливі функції захисту інтересів особистості, суспільства, держави. Однак, як показує практика, до виконання частини безпекових функцій цілком можливо залучати на законній основі комерційні організації, які бажають реалізувати свій потенціал в сфері протидії кібертероризму та захисту кіберпростору.

Основними формами реалізації ДПП при цьому можуть бути: 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.

У серпні 2019 року Рада національної безпеки і оборони України в рамках роботи робочої групи з реформ в сфері кібербезпеки пріоритетом державно-приватного партнерства визначила більший доступ приватних компаній на ринок послуг і сервісів кібербезпеки. Як зазначив радник секретаря РНБО України з питань кібербезпеки Андрій Зюзя, «в умовах стрімкого розвитку ІТ-технологій в світі питання кібербезпеки і кіберзахисту стосується не тільки державного

сектора, а й кожного громадянина, який має смартфон або користується комп'ютером або планшетом» [5]. Результатом роботи робочої групи стало рішення про внесення змін до чинного законодавства України у зазначеній сфері та проведення ретельного аналізу досвіду США та країн ЄС у сфері розвитку державно-приватного партнерства.

На сьогодні українськими держструктурами у взаємодії з бізнес-спільнотою реалізується ряд тематичних проєктів в сфері інформаційної безпеки.

Так з 2018 року в Україні під патронажем Держспецзв'язку України та Комітету електронних комунікацій Торгово-промислової палати України започатковано проведення щорічного національного «Місяця кібербезпеки». У жовтні 2019 року він був проведений вдруге, участь у ньому взяли близько 100 компаній з України, США, Ізраїлю, Німеччини та ОАЕ. Серед ключових подій місячника були:

1. Міжнародний форум «Кібербезпека. Захисти свій бізнес!»;
2. «LEGAL CYBERSECURITY FORUM»;
3. PKI-форум з проблематики електронного підпису та інфраструктури відкритих ключів (Public Key Infrastructure,).

У березні 2020 р під патронатом Ради національної безпеки і оборони України розпочалися регіональні заходи Національного «Місяця кібербезпеки», основні заходи якого пройшли в жовтні 2020 р в тому числі 3-й Міжнародний форум «Кібербезпека. Захисти свій бізнес!». Всі ці заходи присвячені підвищенню обізнаності приватного бізнесу і пересічних користувачів про кібербезпеку і розвитку приватно-державного партнерства.

Загальнонаціонального масштабу набула в Україні також і інформаційна кампанія з підвищення обізнаності громадян про ефективні методи захисту користувачів інтернету, що проводиться з 2019 р під патронатом Ради з національної безпеки і оборони, Держспецзв'язку України та Національної поліції і за підтримки Великобританії і США. Перший етап інформаційної кампанії в 2019 був присвячений створенню захищених паролів (хеш-тег # ПарольГраєРоль), в березні 2020 р стартував другий етап, присвячений питанням двофакторної аутентифікації.

Одними з перших українських приватних операторів у сфері кібербезпеки, що виконують функції комерційних центрів реагування на кіберінциденти, стали компанія CYS-Centrum (створена на початку 2016 г.), а також створені в 2017 р: компанія «Октава Кіберзахіст» - відкрила центр управління кібербезпекою та надає послуги з централізованого управління коштами кібербезпеки, аналізу та моделювання майбутніх ризиків; компанія Hascen, яка надає послуги з виявлення вразливостей і забезпечення кіберзахисту та має у штаті близько 1200 висококваліфікованих хакерів з усього світу. За експертними оцінками, обсяг інвестицій компанії «Октава Кіберзахіст» в створення центру управління кібербезпеки Security Operation Center, що базується на технологічних рішеннях американської корпорації Cisco, оцінювався в суму близько 1 млн дол. [6].

У числі успішних і ефективних корпоративних проєктів управління кібербезпекою експерти виділяють системи розроблені і запущені в експлуатацію найбільшими українськими операторами зв'язку Vodafone Ukraine, «Київстар» і Lifecell. Так, розроблена телекомунікаційною компанією Lifecell в 2017 р система екстреного інформування в умовах надзвичайних ситуацій Emergency Notification System (ENS) була передана для апробування кіберполіції України. На її основі планується сформувати систему екстреного оповіщення про кіберзагрози, що об'єднує сотні державних і приватних компаній стратегічного значення.

Провідні українські ІТ-компанії в останні роки розробили і пропонують держструктурам, бізнесу і приватним користувачам власні антивірусні програмні продукти. Одним з перших таких продуктів, сертифікованих Держспецзв'язком України на відповідність вимогам державних стандартів технічного захисту інформації, стало ПЗ «Zillya! Антивірус для Бізнесу» компанії Zillya, що забезпечує комплексний захист корпоративних комп'ютерних мереж від всіх типів кіберзагроз (включаючи троянські програми, мережеві хробаки, вірусні загрози, експлойти, бекдори) з можливістю централізованого управління і щоденного оновлення антивірусних баз. Також компанією розроблений веб-антивірус «Zillya! Антивірус та Інтернет Захист» / «Zillya! Internet Security».

Проблемою для більшості українських установ і організацій є обов'язкове використання комплексних систем захисту інформації (КСЗІ) для інформації з обмеженим доступом та захищеного доступу до мережі інтернет, передбачене вимогами законів «Про інформацію» та «Про захист інформації в інформаційно-телекомунікаційних системах». У серпні 2017 року Указом президента України №254 / 2017 було введено в дію рішення Ради національної безпеки і оборони[7], посилити для державних органів і організацій вимоги до закупівлі послуг доступу до мережі інтернет. Закуповувати їх дозволялося тільки в операторів (провайдерів), які мали атестати відповідності систем захисту інформації встановленим вимогам.

При цьому українські оператори і провайдери телекомунікаційних послуг зобов'язувалися за власний рахунок встановити захищені вузли доступу до мережі інтернет з комплексними системами захисту інформації. За оцінками українських експертів і громадських організацій, зокрема Інтернет Асоціації України, впровадження і використання більш вдосконалих технічних рішень в сфері інформаційної безпеки стало серйозним тягарем для приватних організацій і провайдерів послуг, що обмежило конкурентність ринку. Орієнтовна вартість комплексної системи захисту інформації (КСЗІ) від несанкціонованого доступу, в залежності від архітектури і рівня захищеності, в середньому оцінювалася в межах 60 000-100 000 грн, а вартість робіт з побудови КСЗІ для захищеного вузла доступу до мережі інтернет в мінімальній комплектації оцінювалася в 300-400 тис. грн. Підтвердження відповідності становило близько 10-15% вартості системи.

У жовтні 2019 р політику Держспецзв'язку України в сфері впровадження

систем захисту інформації та їх атестації піддав критиці віце-прем'єр України з цифрової трансформації Михайло Федоров, який відзначив, що вона ґрунтувалася на застарілій нормативній базі, яка не відповідає технічному рівню сучасних систем, і штучному завищенні вимог - «існуюча практика створення КСЗІ є відкритою торгівлею красивими папірцями і не має нічого спільного з кібербезпекою».[8]

Своєрідні форми сприяння українським держструктурам і спецслужбам в підвищенні кіберзахищеності обирають окремі патріотичні хакерські групи. Хакерських спільноту «Український КіберАльянс» в підтримку інформаційної безпеки України в 2017-2019 рр. проводилися ініціативні флешмоби #F*ckResponsibleDisclosure і #паравозікоблячко, націлені на виявлення вразливостей в об'єктах критичної інформаційної інфраструктури українських держструктур і організацій стратегічного значення. Як відзначали хактивісти, в ході флешмобів їм вдалося виявити понад тисячу вразливостей державних інформаційних ресурсів і систем (в тому числі у НАЕК «Енергоатом», що входить до структур Держспецзв'язку України, команди реагування на кіберінциденти CERT-UA, Національної поліції, судів), дані про яких передавалися до відповідних відомств, що допомагало згодом удосконалити рівень їх кіберзахищеності. При цьому хактивісти нерідко практикували і подальше публічне розкриття виявлених вразливостей, що викликало неоднозначну і негативну реакцію державних структур.

Однією з сучасних нагальних проблем є допуск до аудиту державних органів в сфері кіберзахисту. На сьогодні, монополію щодо оцінки захищеності державних інформаційних ресурсів України має тільки Держспецзв'язок України. Національні ІТ-компанії вважають, що до цього слід допустити краудсорсінгові платформи, але, звичайно, з обмеженням.

Реформа законодавчого забезпечення кіберзахисту просувається недостатньо швидко і не дуже структуровано. Необхідно визначити єдину модель такої реформи, яку узгодять представники як державних органів, так і приватного сектора. Основними цілями для такої моделі повинні бути в першу чергу закріплення міжнародних стандартів в національній системі кіберзахисту, а також дерегуляція і демонополізація держсектора в сфері кіберзахисту.

Пропонуємо актуальні напрями вдосконалення розробки партнерських угод між структурами сектора безпеки та оборони з вітчизняними ІТ-компаніями на принципах державно-приватного партнерства:

1. *Проведення комп'ютерно-технічних експертиз інформаційних ресурсів органів державної влади.* Основна її частина дуже трудомістка і потребує застосування складного обладнання і наявності у експерта спеціальних знань. З цієї причини проводити весь їх обсяг силами виключно державних лабораторій важко. У той же час є приватні компанії, які на високому рівні виконують комп'ютерно-технічні експертизи і готові нарощувати їх кількість. Однак достатньої системності в цій роботі немає, а тому частина експертиз, які цілком

могли б бути здійснені комерційними організаціями, до них не потрапляє. Зміцнення ДПП в цій галузі серед іншого дозволило б створювати більш потужні спеціалізовані кіберлабораторії, що забезпечують виконання комп'ютерно-технічних експертиз будь-якої складності.

2. *Збір цифрових доказів.* Фахівці ряду великих компаній що володіють достатнім досвідом готові з використанням найсучаснішого обладнання кваліфіковано здійснювати обстеження комп'ютерних систем, які зазнали протиправних дій, з дотриманням встановлених вимог збирати і аналізувати дані, на підставі яких може бути прийнято рішення про порушення кримінальної справи. Їх результати при дотриманні певних умов можуть бути згодом долучені до справи в якості цифрових доказів. Ці ж дані можуть бути покладені в основу внутрішнього розслідування кіберінциденту. Важливо, що в подібних випадках є можливість організувати збір значущих даних про інцидент «по гарячих слідах», що нерідко є основною умовою успішного розслідування, і уникнути помилок, що робляться недостатньо підготовленими слідчими і призводять до визнання зібраних доказів недійсними.

3. *Розробка та впровадження програмного забезпечення для виявлення і запобігання кіберзагроз.* Не потребує доказів той факт, що краще попередити вчинення злочину або припинити злочинні дії, ніж боротися з їх наслідками. Окремі вітчизняні компанії пропонують високотехнологічні продукти для виявлення і попередження різних кіберзагроз, засновані на актуальних даних кіберрозвідки і аналізі реальних хакерських атак. Із застосуванням названих засобів може проводитися захист інформаційних ресурсів критично важливих об'єктів, досягатися підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування. При розробці зазначених коштів додатково вирішується завдання підвищення конкурентоспроможності перспективних українських інформаційних технологій, зміцнення вітчизняного науково-технічного потенціалу в галузі забезпечення інформаційної безпеки. Для мінімізації ризиків і забезпечення скоординованих дій при виникненні кризових ситуацій вкрай важливо забезпечити взаємодію з органами кібербезпеки сектору безпеки та оборони, в першу чергу, в плані обміну оперативною інформацією. Підвищеної актуальності останнім часом набуває впровадження зазначених систем в інформаційному захисті банківського сектору, забезпечити яку для держави самостійно вкрай важко. Додамо, що заходи щодо запобігання кіберзлочинів можуть передбачати консалтинг та аудит систем інформаційної безпеки підприємств і організацій різних форм власності. Важливо забезпечити і просвітництво кіберспівтовариства, оповіщення його через інформаційні інтернет-ресурси про оптимальні способи захисту від нових загроз, впровадження ефективних мережевих інструментів збору і направлення до органів сектору безпеки та оборони заяв про протиправні дії в кіберпросторі, які враховують специфіку різних груп мережевих користувачів. Комерційні організації також могли би брати активну участь у забезпеченні захищеності громадян від

інформаційних загроз, в тому числі за рахунок формування культури особистої інформаційної безпеки також.

4. *Моніторинг кіберпростору.* Особливе місце у формуванні системи виявлення в кіберпросторі оперативно значимої інформації займає організація комплексу заходів, що об'єднуються поняттям «моніторинг мережевих інформаційних ресурсів». Основними напрямками моніторингу, що дозволяє отримувати значні обсяги цінної з точки зору протидії кібербезпеки інформації, є: автоматизований пошук мережевих ресурсів, що містять заборонену до поширення інформацію; дослідження матеріалів виявлених ресурсів, пов'язаних з діяльністю злочинних співтовариств; спостереження за закритими для загального доступу місцями мережевого спілкування деструктивної спрямованості. Істотно підвищити ефективність украй трудомісткого моніторингу, здійснюваного органами сектору безпеки та оборони, може залучення до його проведення спеціалізованих комерційних структур. Об'єднання зусиль дозволить отримувати найбільш повну картину оперативної обстановки в сфері протидії кіберзлочинності в результаті акумулювання інформації, що надходить з численних джерел, сформованих в державних структурах і приватному секторі.

При підвищенні рівня взаємної довіри можливе створення об'єднаних інформаційних систем з обміном даними за єдиним регламентом у випадках виявлення певних подій. Постійний моніторинг забезпечує: збір максимально повної інформації про об'єкти оперативного інтересу з формуванням «електронного дос'є» на потенційних кіберзлочинців, виявлення і візуалізацію неявних зв'язків з іншими об'єктами і подіями кримінального характеру; виявлення нових способів і інструментів скоєння злочинів; спостереження за активністю численних мережевих груп кримінальної спрямованості з визначенням їх спеціалізації, ступеня організованості, розподілу ролей, характеру неочевидних зв'язків між фігурантами і їх причетності до тих чи інших подій; виявлення місць концентрації кримінально налаштованих осіб і прихованих каналів їх спілкування і координації діяльності [8].

Спостереження за станом оперативної обстановки в кіберпросторі здійснюється, наприклад на базі Департаменту кіберполіції, де з 2017 року створено цілодобовий «call-центр» для прийому заяв та звернень від громадян про злочини та правопорушення, що вчиняються в глобальній мережі.

5. *Технології аналізу великих даних (Big Data).* Розвиток інформаційних технологій призвів до зміни способів обробки інформації. Вектор інтенсифікації отримання оперативно значущих відомостей сьогодні зміщується в бік аналізу Великих Даних. Розвиток аналітичного інструментарію для ефективного обробки отриманих масивів даних неможливо без залучення компаній, що спеціалізуються на розробці відповідного програмного забезпечення. Одночасно необхідно запровадити опрацювання в рамках ДПП організаційних механізмів і технологій об'єднання інформації з численних розрізнених об'ємних неструктурованих джерел, а також збору додаткових даних за встановленими

умовами.

6. *Формування законодавства.* Не менш важливі і зусилля щодо зближення позицій бізнес-спільноти та органів влади в правовій сфері кібербезпеки, просуванні спільних законодавчих ініціатив. В рамках ДПП можуть формуватися робочі групи з представників органів сектору безпеки та оборони країни, що відповідають за сферу кібербезпеки та комерційних структур для обговорення спільних законопроектів.

Маючи глибоке розуміння процесів, пов'язаних з розвитком інформаційних технологій, фахівці великих ІТ-компаній здатні ефективно брати участь в створенні продуманих і зрозумілих законів, що забезпечують правове регулювання суспільних відносин у сфері використання кіберпростору.

На наш погляд, на такій основі в законодавстві повинні з'явитися правові норми, ясно і чітко закріплюють процедури регулювання участі недержавних структур в зборі цифрових даних, їх спільного обробітку, використанні її результатів і формуванні доказової бази у кримінальних справах. Тут гостро стоїть цілий ряд питань, пов'язаних із забезпеченням прав громадян; з визначенням меж повноважень зазначених суб'єктів в кіберпросторі; з регламентацією взаємодії з операторами зв'язку, провайдерами інтернет-ресурсів, власниками інформаційних систем. Підтвердив свою надійність великим партнерам держава могла б на законних підставах передати частину повноважень на здійснення в кіберпросторі певних дій, спрямованих на отримання, обробку та використання даних в інтересах кіберборотьби. Одночасно повинна бути закріплена система державної атестації і сертифікації таких компаній, що беруть на себе відповідні зобов'язання і несуть відповідальність за виконання вимог закону.

7. *Підготовка фахівців.* У Стратегії національної безпеки України підкреслюється важливість розвитку людського капіталу, професійної освіти фахівців сектору безпеки та оборони. Дійсно, як зазначалося вище, рішення багатьох питань протидії кіберзлочинності можливо лише при умови відповідного кадрового забезпечення цієї діяльності. Затребуваність фахівців в сфері обробки даних сьогодні вкрай висока. Це високооплачувана категорія кваліфікованих співробітників, що володіють аналітичними навичками та глибокими знаннями в сфері інформаційних технологій, математики, статистики, економіки, соціології. Стандарти, за якими йде підготовка фахівців для кіберструктур сектору безпеки та оборони, повинні передбачати отримання глибоких знань про методи добування в сучасному інформаційному середовищі відомостей, необхідних для розкриття і розслідування кіберінцидентів, і формування відповідних умінь і навичок. Підвищити якість підготовки фахівців можливо за рахунок залучення до неї кваліфікованих представників ІТ-індустрії. Великі компанії мають можливість брати участь у підвищенні кваліфікації співробітників правоохоронних органів по конкретних напрямках протидії кіберзлочинності, проводити семінари, на яких обговорювалися б найбільш

актуальні проблеми і результати відповідних наукових досліджень.

Співпраця в цій сфері дає основу і для спільної розробки та реалізації усіма зацікавленими сторонами практичних рекомендацій з різних питань протидії кіберзлочинності, узагальнюючих позитивний досвід усіх його учасників.

Можна спостерігати, що окремі компанії вже досить успішно взаємодіють з державними органами на названих напрямках. У той же час очевидно, що з урахуванням наростання загроз в інформаційній сфері цих процесів слід надати системний характер. Прискорити це можливо через об'єднання ключових гравців ринку систем кібербезпеки в асоціації.

Створення організаційної структури, що дозволяє всім зацікавленим сторонам виступати через єдиного представника, доцільно для забезпечення координації інтересів організацій приватного сектора, консолідації їх зусиль на найважливіших напрямках протидії кіберзлочинності. Асоціація здатна виробити оптимальні форми взаємодії з усіма суб'єктами такого протидії: органами, що формують політику забезпечення інформаційної безпеки на різних рівнях; організаціями, що мають можливість сприяти у вирішенні завдань ДПП (провайдери доступу, власники інформаційних систем і ін.); потенційними клієнтами; громадськими організаціями та ін.

Виступаючи в ДПП від імені всіх учасників асоціації, її єдиний представник повинен організувати майданчик для ефективної взаємодії органів влади, інфраструктурних компаній і банків організацій, що беруть участь у створенні і розвитку асоціації. Об'єднані зусилля тут направляються на: підвищення рівня компетенцій членів асоціації в протидії кіберзлочинності через надання інформаційної, методичної та освітньої підтримки; опрацювання відображають інтереси членів асоціації пропозицій щодо розвитку нормативно-правової та методологічної бази в сфері протидії кіберінцидентам; залучення до участі в асоціації нових членів; вирішення інших завдань.

Висновки. Проаналізувавши останні численні заходи, що характеризують стан справ у здійсненні державно-приватного партнерства у сфері кіберзахисту України можна констатувати, що сфера кібербезпеки не тільки стає привабливою для представників бізнесу, але і в цілому є пріоритетним напрямком його розвитку. Україна потребує оновлення законодавства щодо державно-приватного партнерства (Закон України «Про державне приватне партнерство» 2010 року[9]) та внесення змін у статтю 4 даного закону, що визначає сфери застосування державно-приватного партнерства, де сфера кібербезпеки є відсутньою.

Підводячи підсумок, відзначимо, що викладене, на наш погляд, підтверджує необхідність розробки комплексної стратегії розвитку недержавного сектора забезпечення кібербезпеки, що враховує інтереси всіх сторін і в якій був би узагальнений позитивний вітчизняний та зарубіжний досвід організації ДПП в сфері забезпечення кібербезпеки. Думаємо, реалізація такої стратегії доцільна в рамках національної програми, яка передбачає: закріплення керівних принципів стимулювання державно-приватного партнерства в зазначеній сфері та

оптимальних умов для довготривалого дотримання домовленостей і досягнення цільових показників та індикаторів; вдосконалення системи управління та координації відповідних процесів на національному, міжрегіональному, регіональному, муніципальному рівнях; забезпечення привілейованого доступу сторін до додаткових ресурсів, облік потенційних комерційних зисків для представників приватного сектора, заохочення ініціативних проєктів з розвитку взаємодії і об'єднання ресурсних можливостей; страхування потенційних ризиків тощо.

Перспективи подальших розвідок у даному напрямі автор бачить у розробки змісту та концептуальних основ *стратегії розвитку недержавного сектора забезпечення кібербезпеки* як комплексного документу та стимулюванні наукового дискурсу навколо цієї проблематики як першого кроку до вирішення проблеми вдосконалення ДПП у сфері кібербезпеки.

Література:

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 5 жовтня 2017 року. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013>
3. Про рішення Ради національної безпеки і оборони України від 13 лютого 2017 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: Указ Президента України № 32/2017 URL: <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text>
4. Введено в дію рішення РНБО по захисту від кібератак. URL: https://jurliga.ligazakon.net/news/163845_vvedeno-v-dyu-rshennya-rnbo-po-zakhistu-vd-kiberatak
5. У РНБО обговорили питання кібербезпеки Укрінформ. URL: <https://www.ukrinform.ua/rubric-politics/2755663-u-rnbo-obgovorili-pitanna-kiberbezpeki.html>
6. У Києві відкрився комерційний центр управління кібербезпеки. URL: <https://translate.google.com/?hl=uk&sl=ru&tl=uk&text=%D0%92%20%D0%>
7. Про рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: Указ Президента України від 13 лютого 2017 року № 32/2017». URL: <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text>
8. Бюрократизм і корупція. Міністерство цифрової трансформації почне реформу Держспецзв'язку. URL: <https://biz.nv.ua/ukr/tech/byurokratizm-i-korupciya-ministerstvo-cifrovoji-transformaciji-pochne-reformu-derzhspeczv-yazku-50047903.html>
9. Про державно-приватне партнерство: Закон України № 2404-VI від 1 липня 2010 року. URL: <https://zakon.rada.gov.ua/laws/show/2404-17#Text>

References:

1. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" : vid 5 zhovtnia 2017 roku, № 2163-VIII [Law of Ukraine "On the basic principles of cybersecurity in Ukraine" from October 5, 2017, № 2163-VIII]. (n.d.). zakon.rada.gov.ua. Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].

2. Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy №447/2021 [On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cyber Security Strategy of Ukraine": Decree of the President of Ukraine №447/2021]. Retrieved from <https://www.president.gov.ua/documents/4472021-40013> [in Ukrainian].

3. Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 13 liutoho 2017 roku «Pro zahrozy kiberbezpeti derzhavy ta nevidkladni zakhody z ikh nejtralizatsii»: Ukaz Prezydenta Ukrainy № 32/2017 [On the decision of the National Security and Defense Council of Ukraine of February 13, 2017 "On threats to cybersecurity of the state and urgent measures to neutralize them": Decree of the President of Ukraine № 32/2017]. Retrieved from <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> [in Ukrainian].

4. Vvedeno v diiu rishennia RNBO po zakhystu vid kyberatak [The decision of the National Security and Defense Council on protection against cyberattacks is put into effect]. Retrieved from https://jurliga.ligazakon.net/news/163845_vvedeno-v-dyu-rshennya-rnbo-po-zakhystu-vd-kiberatak [in Ukrainian].

5. U RNBO obhovoryly pytannia kiberbezpeky Ukrinform. [The National Security and Defense Council discussed cybersecurity issues of Ukrinform]. Retrieved from: <https://www.ukrinform.ua/rubric-politics/2755663-u-rnbo-obgovorili-pitanna-kiberbezpeki.html>

6. U Kyievi vidkryvsia komertsijnyj tsentr upravlinnia kiberbezpeky [A commercial cybersecurity management center has opened in Kyiv]. Retrieved from: <https://translate.google.com/?hl=uk&sl=ru&tl=uk&text=%D0%92%20%D0%>

7. Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 10 lypnia 2017 roku «Pro stan vykonannia rishennia Rady natsional'noi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro zahrozy kiberbezpeti derzhavy ta nevidkladni zakhody z ikh nejtralizatsii»: Ukaz Prezydenta Ukrainy №254/2017. [On the decision of the National Security and Defense Council of Ukraine of July 10, 2017 "On the status of implementation of the decision of the National Security and Defense Council of Ukraine of December 29, 2016" On threats to cybersecurity and urgent measures to neutralize them ": Decree of the President of Ukraine]. Retrieved from: <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text>

8. Biurokratyzm i koruptsiia. Ministerstvo tsyfrovoi transformatsii pochnе reformu Derzhspetsv'iazku.[Bureaucracy and corruption. The Ministry of Digital Transformation will start the reform of the State Special Communications] Retrieved from:<https://biz.nv.ua/ukr/tech/byurokratizm-i-korupciya-ministerstvo-cifrovoji-transformaciji-pochne-reformu-derzhspeczv-yazku-50047903.html>

9. Zakon Ukrainy "Pro derzhavno-pryvatne partnerstvo" vid 1 lypnia 2010 roku № 2404-VI [Law of Ukraine "About public-private partnership" from July 1, 2010, № 2404-VI (n.d.). zakon.rada.gov.ua. Retrieved from: <https://zakon.rada.gov.ua/laws/show/2404-17#Text> [in Ukrainian].