УДК 338.2: 005.3 (477)

Р. Ю. Прав,
аспірант, Міжрегіональна Академія Управління персоналом, м. Київ
ORCID ID. 0000-0001-8064-2836

DOI: 10.32702/2306-6814.2019.21.143

РОЛЬ МЕХАНІЗМУ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У РОЗВИТКУ КІБЕРБЕЗПЕКИ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ

R. Prav,
postgraduate student, Interregional Academy of Personnel Management, Kyiv

THE ROLE OF PUBLIC-PRIVATE PARTNERSHIP MECHANISM IN THE DEVELOPMENT OF UKRAINE'S CYBER SECURITY AT THE CURRENT STAGE

У статті проаналізовано необхідність впровадження механізму ДПП у сферу кібербезпеки України. Визначено поняття кібербезпеки та державно-приватного партнерства на сучасному етапі, основні суб'єкти та принципи кібербезпеки, її комплементарні категорії. Розглянуто основні кібератаки України за останній період та напрями кібербезпекових проектів у сфері ДПП.

Висвітлено завдання державно-приватного партнерства у сфері кібербезпеки та чинникі, що впливають на рівень впровадження кібербезпеки у Європейському Союзі. Розглянуто досвід розвинутих країн щодо застосування ДПП у сфері кібербезпеки, виділено основні напрями діяльності громадських інститутів-учасників ДПП у сфері кібербезпеки.

Сформульовано основні завдання діяльності громадської організації "Українська академія кібербезпеки" та запропоновано заходи, необхідні для подальшого впровадження механізмів державно-приватного партнерства у сфері забезпечення кібербезпеки.

The widespread use of computer and Internet technologies in all spheres of human life has many advantages, with increasing volume of threats that harm the country and the world. The article proved the need to address these issues with the aim to minimize, eliminate and prevent cyber threats. The necessity of introduction of the public-private partnership mechanism in the sphere of cybersecurity of Ukraine is analyzed.

The concepts of cybersecurity and public-private partnerships at the present stage, the main subjects and principles of cybersecurity, its complementary categories, and the regulatory frameworks for ensuring cybersecurity in domestic law are defined. The main cyberattacks of Ukraine in the recent period; the directions of cyber security projects in the field of public-private partnership and the new principles of public-private partnership are considered. It is determined that the main task of the government in the field of public-private partnerships is to give local communities the opportunity to solve their own problems and control the quality of public services.

The objectives of the public-private partnership in the field of cybersecurity and the factors affecting the level of implementation of cybersecurity in the European Union are highlighted, as well as two directions of cybersecurity projects in the field of public-private partnerships are considered.

The experience of developed countries on the application of public-private partnerships in the field of cybersecurity (USA, Germany, Estonia) is considered, the main directions of activity of public institutes — participants of public-private partnerships in the field of cybersecurity are highlighted.

The main tasks of the activity of the public organization "Ukrainian Cyber Security Academy" and the directions of activity of public institutes — participants of public-private partnerships in the field of cybersecurity are formulated. It is justified that public-private partnerships become the mechanism, that can improve the effectiveness of cyber defense, organize a wide range of private and civic structures. The public-private partnership addresses the following cybersecurity challenges: technical security and data protection, secure internet access, sharing of threats and attacks, assistance in resolving emerging issues in the Internet. The measures necessary for the further implementation of public-private partnership mechanisms in the field of cybersecurity are proposed.

Ключові слова: кібербезпека, державно-приватне партнерство, кіберризик, кібератака, інформаційні технології, принципи ДПП, комплементарні категорії, національна безпека, інноваційність.

Key words: cybersecurity, public-private partnership, cyber risk, cyberattack, information technology, public-private partnership principles, complementary categories, national security, innovation.

ПОСТАНОВКА ПРОБЛЕМИ

Останнім часом напрям розвитку нашої країни спрямований на технологічний прогрес та впровадження інформаційних технологій, які суттєво полегшують процеси пошуку та обміну інформацією. Широке використання в усіх сферах суспільного життя комп'ютерних і телекомунікаційних технологій, особливо інтернет-технологій має безліч переваг разом зі збільшенням обсягу загроз. Реалізація яких шкодить на рівні держави та на міжнародній арені. Що призводить до необхідності вирішення цих проблем з метою мінімізації, ліквідації та попередження кіберзагроз. Сьогодні кіберзлочинність, для якої не існує державних кордонів, загрожує не лише суспільству, а й посягає на національні інтереси. Спостерігається висока активність кібератак, діяльність злочинних угруповань, промислово-фінансових груп та осіб, працюючих у системі при здійсненні службової діяльності (інсайдерів). Випадки кіберзагроз стають частішими, краще організованими, легкими та дешевими в підготовці і реалізації. Саме тому потрібно шукати нові шляхи протидії, вдосконалювати механізми кібербезпеки країни, в тому числі впроваджуючи концепцію державно-приватного партнерства.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Розвиток державно-приватного партнерства досліджували вітчизняні й зарубіжні вчені: В.Г. Варнавський, М. Джеррард, А.С. Корчагіна, К.В. Павлюк, С.М. Павлюк, О.М. Полякова, В.В. Пучков, В.І. Якунін та ін., у працях яких проблеми взаємодії влади і бізнесу аналізуються з різних позицій. Значна кількість наукових публікацій з питань державно-приватного партнерства аналізує різноманітність форм, моделей і сфер його застосування — від соціальних та державних проектів до розробки перспективних технологій та освоєння інноваційних технологій. Але сьогодні залишаються дискусійними питання участі та ролі бізнесу у боротьбі з кібератаками та сприянні інноваційного розвитку держави. Дослідженням питань кібербезпеки займались такі відомі вчені: А. Клімбург, К. Мін, М. Хан, В.Г. Кіютін, А.П. Новіков, Д. Робинсон, В. Сомерс та ін.

Однак, незважаючи на значну кількість наукових досліджень у цій сфері, високий рівень опрацювання загальнотеоретичних питань, проблематика застосування механізмів державно-приватного партнерства у сфері кібербезпеки вимагає подальших досліджень.

МЕТА ДОСЛІДЖЕННЯ

Мета дослідження — дослідити та проаналізувати можливості впровадження та вдосконалення кібербезпеки шляхом використання механізмів державно-приватного партнерства.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Після надбання Україною незалежності практично усі органи влади використовують новітні інноваційні технології, формуючи електронний простір. Загалом "цифрова революція" разом з перевагами, має низку негативних аспектів, одним з яких є низький рівень кібербезпеки. Сьогодні забезпечення кібербезпеки України як захисту життєво важливих інтересів людини, суспільства та держави в інтернет-просторі, досягається за допомогою організаційно-правових, інформаційних, технічних заходів, у відповідності до концепції держави: захищений національний сегмент кіберпростору; нейтралізація посягань на внутрішні справи України з боку інших держав, посилення її обороноздатності; протидія кіберзлочинності; гарантії повноправної участі Ук-

раїни в загальноєвропейській системі забезпечення кібербезпеки; участь у боротьбі з кібертероризмом [3, с. 110]. Вибір інструментів і шляхів забезпечення кібербезпеки залежать від діяльності відповідальних суб'єктів, визначених у законодавстві, а саме взаємодії держави та населення.

Термін "кібербезпека" зазвичай стосується корпоративного управління, менеджменту та зосереджується на особливих формах складних атак й охоплює їх технічний і соціальний аспекти. Розглянемо кілька визначень цього поняття. ЄС офіційно визнає, що "кібербезпека зазвичай стосується заходів і дій, спрямованих на захист кіберпростору в цивільній і військовій сферах від загроз, які можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі або є пов'язаними з ними. Кібербезпека спрямована на збереження доступності та цілісності мереж та інфраструктури, а також конфіденційності інформації, яка міститься в них" [1].

В.Н. Фурашев визначає кібербезпеку як стан, здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, передусім — несвідомого, негативного впливу (управління) інформації [2, с.168]. На думку О.Г. Корченко, кібербезпека — це сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугрупувань розгортаються навколо інформаційного ресурсу, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем [4, с. 7] та які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної і кіберінфраструктури [4, с. 41].

У сучасних умовах кібербезпека та її забезпечення — необхідний актуальний комплексний вектор проведення виваженої державної політики в контексті реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 р. № 96/2016 [5]. З набуттям чинності цієї Стратегії кібербезпеки Україна зробила важливий крок по створенню національної системи кібербезпеки. На державному рівні зафіксовано, що пріоритетами й напрямами забезпечення кібербезпеки є: розвиток безпечного, стабільного та надійного кіберпростору; кіберзахист державних електронних інформаційних ресурсів і критичної інформаційної інфраструктури; розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки; боротьба з кіберзлочинністю тощо [6].

Нормативні основи забезпечення кібербезпеки закріплено у Законі України "Про основні засади забезпечення кібербезпеки в Україні", а також в інших законодавчих актах. Напрями забезпечення кібербезпеки у роботі різних органів державної влади також відображені у законодавстві, наприклад, у статті 10 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" відображена роль державних органів влади у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. У законі зазначено, що спеціальний центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації має такі повноваження:

— розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

— визначає вимоги та порядок створення комплексної системи захисту;

— здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

— здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі [7].

Спеціальними суб'єктами забезпечення кібербезпеки є державні органи, які, крім загальних функцій, уповноважені на здійснення боротьби з кіберзлочинністю та кібертероризмом, а також на забезпечення кібернетичного захисту об'єктів національної критичної інфраструктури. До таких суб'єктів належать: Міністерство внутрішніх справ України; Служба безпеки України; Державна служба спеціального зв'язку та захисту інформації України; Міністерство юстиції України; Генеральна прокуратура України [8]. Необхідно також відмітити діяльність Національного банку України у сфері забезпечення кібербезпеки [9].

Суб'єкти системи забезпечення кібернетичної безпеки перебувають у тісній взаємодії між собою, але при цьому кожен із них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетентності та в межах повноважень, визначених законодавством. Незважаючи на це, загрози кібербезпеці актуалізуються через дію таких чинників, як недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки [5].

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах:

— верховенства права і поваги до прав та свобод людини і громадянина;

— забезпечення національних інтересів України;

— відкритості, доступності, стабільності та захищеності кіберпростору;

— державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту;

— пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам;

— пріоритетності запобіжних заходів;

— невідворотності покарання за вчинення кіберзлочинів;

— пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

— міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам,

Таблиця 1. Основні принципи державно-приватного партнерства

№	Принцип
1.	проектування і моделювання
2.	впровадження технологій випереджаючого розвитку
3.	відкритості і суспільної участі
4.	безперервності інноваційного розвитку
5.	пріоритетності і стратегічного інвестування

недопущення використання кіберпростору в протиправних та воєнних цілях;

— забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [3].

Останнім часом збільшується кількість кібератак в Україні. Визначимо головні з них: у 2017 році хакери атакували українські банки, компанію "Київенерго", "Запоріжжяобленерго", "Дніпроенерго" та Дніпровські електроенергетичні системи, державний "Ощадбанк", аеропорт — "Бориспіль" та комп'ютерні сервери Кабінету Міністрів, "Укрпошта" і "Укртелеком" теж зазнали хакерської атаки, комп'ютерні системи підприємств не працювали [12].

Жертвою вірусу Petya 27 червня 2017 року стали: аеропорт "Бориспіль", ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низка інших великих підприємств, Кабінет Міністрів України, медіахолдинг ТРК "Люкс", до складу якого входять "24 канал", "Радіо Люкс FM", "Радіо Максимум", різні інтернет-видання, а також сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та Служби спецзв'язку України [13].

Реалізація кібербезпеки шляхом використання ДПП передбачає залучення в якості приватного партнера суб'єктів господарської діяльності, що використовують елементи критичної інфраструктури, які залежать від ІКТ; виробників серверного обладнання, розробників програмних продуктів, операторів платіжних розрахунків. Необхідним є напрацювання відносин, пов'язаних з розкриттям конфіденційної, комерційної та персональної інформації, досягнення співвідношення інтересів партнерів, розробка контрольних та наглядових процедур [14, с. 57].

Термін "державно-приватне партнерство" відображає провідну роль держави у впровадженні проектів ДПП. Термін "державно-приватне партнерство" можна розглядати в широкому та вузькому розумінні. У широкому розумінні державно-приватне партнерство — це "система відносин держави та бізнесу, яка широко використовується як інструмент національного, міжнародного, регіонального, міського, муніципального, економічного і соціального розвитку" [1, с.12]. У вузькому розумінні державно-приватне партнерство — це "конкретні проекти, що реалізуються спільно державними органами і приватними компаніями на об'єктах державної та муніципальної власності" [1, с.12].

Державно-приватне партнерство є одним з принципів сучасної моделі публічного управління "New Public Management", яку провідні західні країни почали впроваджувати в кінці XX ст. Концепція "нового державного менеджменту", на думку М.В. Пасічника, — це модель державного управління, в основу якої покладено запозичення методів корпоративного управління, які застосовуються в бізнесі та некомерційних організаціях, вона орієнтована на підвищення гнучкості прийняття рішень у державному апараті, зниження його ієрархічності, делегування повноважень на нижчий рівень прийняття рішень і посилення механізмів зворотного зв'язку між державою та громадянами [15].

Закон України "Про державно-приватне партнерство" від 1 липня 2010 р. № 2404-VI визначає державно-приватне партнерство як "співробітництво між Україною, територіальними громадами в особі відповідних органів державної влади та органів місцевого самоврядування (державними партнерами) та юридичними особами, крім державних та комунальних підприємств, або фізичними особами — підприємцями (приватними партнерами), що здійснюється на основі договору в порядку, встановленому цим Законом та іншими законодавчими актами" [17].

Сьогодні державно-приватне партнерство (далі — ДПП) визнається як державами, так і недержавними суб'єктами ключовим елементом побудови дійсно ефективної системи кібербезпеки держави. Майже кожна стратегія кібербезпеки (національного чи наднаціонального рівня) або ж відомчий візійний документ (який стосується кібербезпеки) містить згадки про бажання розвивати ДПП [18].

Основні принципи ДПП представлено у таблиці 1.

Поряд з розмаїттям форм реалізації, у міжнародній практиці визначають основні етапи ДПП: оцінка можливостей для надання послуг у рамках державно-приватного партнерства; підготовка до надання послуги або реалізації проекту в рамках державно-приватного партнерства; вибір партнера; переговорний процес та укладання договору; виконання та моніторинг контракту [5, с. 81].

Сьогодні впровадження концепції ДПП в Україні відбуваються повільно, незважаючи на те, що влада визначила ДПП одним з ключових механізмів реалізації політики модернізації економіки та вирішення важливих соціально-економічних проблем. Основними причинами можна назвати: слабку політичну координацію, корупцію, недоліки у нормативно-правовому регулюванні, економічну нестабільність, застарілість об'єктів інфраструктури, низкий рівень інвестицій, відсутність досвіду взаємодії держави та бізнесу у сфері кібербезпеки.

Завдання державно-приватного партнерства у сфері кібербезпеки:

— регулювати технічну безпеку та обробку даних;

— забезпечити надійний доступ до Інтернет-мережі;

— проводити обмін інформацією щодо загроз і вразливостей;

— здійснювати допомогу щодо вирішення ситуацій, пов'язаних із загрозами або незаконним контентом в Інтернет-мережі.

Таблиця 2. Напрямки діяльності громадських інститутів — учасників ДПП у сфері кібербезпеки

Напрями діяльності	*Завдання*
Сприяння державним органам	У здійсненні діяльності, пов'язаної із забезпеченням захисту інформації та інформаційної безпеки України
	У здійсненні науково-методичного управління підготовкою кадрів у сфері кібербезпеки, інформаційних технологій та захисту інформації
	В організації та створенні відповідної науково-дослідної бази, створенні підручників, іншої науково-методичної літератури, кіно- і відеофільмів
Удосконалення нормативної бази	Внесення пропозицій щодо розробки нормативно-правових актів у сфері захисту національного і міжнародного кіберпростору
Удосконалення ІТ-технологій	Внесення пропозицій щодо розробки, впровадження і застосування захищених інформаційних технологій і систем, передусім чергу на об'єктах критичної інформаційної інфраструктури, у сферах криптографічного та технічного захисту інформації
Внесення пропозицій держорганам і суб'єктам господарювання	Щодо заходів підвищення захищеності інформаційних технологій і систем
	Щодо тимчасового припинення розробки і впровадження технологій і систем, які не відповідають вимогам рівня захисту інформації
	Щодо розробки та проведення незалежних громадських експертиз
Наукова, освітня, юридична, консультаційна допомога	Надання допомоги державним органам, науковим установам, ЗВО, підприємствам, установам усіх форм власності, громадським організаціям, окремим громадянам щодо розробки, впровадження, застосування захищених інформаційних технологій і систем, передусім на об'єктах критичної інформаційної інфраструктури, захисту кіберпростору, криптографічного та технічного захисту інформації
Підготовка фахівців	Надання допомоги у підвищенні кваліфікації співробітників органів державної влади, фахівців-практиків
	Надання допомоги у підготовці наукових і науково-технічних кадрів, обдарованої молоді, виявлення і підтримка талановитих дослідників і спеціалістів-практиків, сприяння творчому зростанню молодих фахівців і науковців
Міжнародне співробітництво	Сприяння розвитку міжнародного співробітництва у сфері кібербезпеки

Принципи ДПП у сфері кіберпезпеки базуються на основі економічної ефективності та інноваційності; забезпеченні цілісності та доступності; приватності та свободи; відповідальності та прозорості; справедливості.

Сучасне відношення країн ЕС до проблематики кібернетичної безпеки пройшло доволі тривалий шлях — від розуміння до комплексного бачення систем захисту. На нього значною мірою вплинуло кілька чинників, які визначили засади, пріоритети і сучасні горизонти. Основними з яких є:

— новизна, складність і чисельність викликів та загроз, що постали на початковому етапі при формування основоположних засад кібернетичної безпеки ЄС;

— позитивне сприйняття ЄС орієнтирів щодо поточного і майбутнього розвитку правового забезпечення кібернетичної безпеки, окреслених низкою універсальних і регіональних міжнародних організацій;

— зосередження на правових питаннях, пов'язаних із кібернетичною і інформаційною безпекою, переважно на позиціях захисту загальновизнаних прав людини;

— поступове поширення різноманітних злочинів, пов'язаних із використанням нових цифрових технологій і необхідністю попередження злочинності та створення кримінального правосуддя у боротьбі із "високотехнологічною" та "комп'ютерною" злочинністю;

— наявність переважно норм soft law ("м'якого права") з питань кібернетичної та інформаційної безпеки, що містились у резолюціях міжнародних органів та організацій, у спільних заявах, деклараціях, комюніке [19].

Розвиток державно-приватного партнерства у сфері кібербезпеки є одним з основних та ефективних інструментів створення систем кібербезпеки/кіберзахисту. Цей інструмент застосовується в міжнародній практиці. Сучасну модель ДПП формує Департамент внутрішньої безпеки США (DHS). Для швидкого і своєчасного обміну індикаторами інформації про загрози між державним і приватним секторами у Департаменті створено автоматизовану програму з кіберзагроз [20].

Федеральний уряд Німеччини на реалізацію завдання захисту критичної інфраструктури (Національна стратегія для захисту критичної інфраструктури, CIP) на стратегічному та операційному рівні розробив План державно-приватного партнерства KPITIC (Umsetzungsplan KRITIS). З 2007 р. державно-приватне співробітництво "UP KRITIS" почало реалізовуватися урядом у співпраці з операторами критичної інфраструктури. Головна мета Плану KPITIC — покращення захисту критичної інфраструктури у різних секторах безпеки [18, с. 78].

В Україні під час формування Планів дій з реалізації Стратегії кібербезпеки теж слід зосередитися на розширенні заходів по реалізації ДПП. Зокрема слід розробити план, аналогічний KPITIC, і визначити в ньому такі завдання:

— проведення тренінгів для сторін державно-приватного партнерства;

— підготовка спільних рекомендацій для обох секторів у сфері кібербезпеки;

— кризові комунікації;

— взаємодія з міжнародними партнерами;

— інформування вітчизняних партнерів про європейські інститути щодо захисту критичної інфраструктури;

— визначення механізму приєднання інших учасників до плану ДПП.

Позитивним для України у сфері кібербезпеки є досвід Естонії. У цій країні створена Ліга кібербезпеки, яка має повноваження від імені держави відбивати кібератаки. До неї входять добровольці-фахівці, які працюють в ІТ-сфері, але у вільний час моніторячи кіберпростір, допомагають державі формувати кібербезпеку.

Досвід іноземних країн та особливості українських реалій свідчать, що розв'язання основних завдань кібербезпеки неможливе без створення:

1) міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки;

2) центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін та впливу на їх ІТС;

3) органів власної інформаційної і кібербезпеки — державних установ (відомств) та комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного кіберпростору [21, с. 8—9].

У 2016 році на основі державно-приватного партнерства було засновано громадську організацію "Українська академія кібербезпеки". Згідно із статутом, основна мета організації — вивчення, узагальнення і розповсюдження національних і міжнародних наукових, освітніх і науково-технічних досягнень у сфері кібербезпеки, захисту інформації в інформаційно-телекомунікаційних системах, безпечного використання інформаційних технологій і систем, зокрема на об'єктах критичної інформаційної інфраструктури, сприяння найбільш повному використанню цих досягнень в інтересах забезпечення інформаційної безпеки України та її соціально-економічного розвитку, сприяння розвитку і відтворенню інтелектуального потенціалу українського суспільства [22].

Основні завдання діяльності громадської організації "Українська академія кібербезпеки":

— сприяння державно-приватному партнерству у сфері кібербезпеки, розвитку та інтеграції науки, освіти й виробництва в сфері захисту національного і міжнародного кіберпростору, розробки, впровадження і застосування захищених інформаційних технологій і систем на об'єктах критичної інформаційної інфраструктури, криптографічного та технічного захисту інформації;

— об'єднання зусиль вчених і спеціалістів наукових установ, вищих навчальних закладів, державних органів, підприємств, установ і організацій усіх форм власності, професійна діяльність яких пов'язана із забезпеченням кібербезпеки та захистом інформації в інформаційно-телекомунікаційних системах з впровадженням, застосуванням та безпечним використанням інформаційних технологій і систем, в інтересах забезпечення інформаційної безпеки України;

— інформування громадськості про необхідність забезпечення захисту кіберпростору України, її членства у відповідних міжнародних інституціях, що опікуються заходами проти кіберзагроз [22].

Загалом можна виділити такі напрями діяльності громадських інститутів-учасників ДПП у сфері кібербезпеки (табл. 2).

Наразі громадська організація "Українська академія кібербезпеки" здійснює організацію заходів з підвищення кваліфікації працівників органів державної влади. Налагоджено взаємодію зі структурними підрозділами Служби безпеки України, Держслужби спеціального зв'язку та захисту інформації, Національної поліції, Генерального штабу Збройних Сил України. Мета і завдання, які ставить Громадська організація "Українська академія кібербезпеки" спрямовані на досягнення основного завдання — створення Національної системи кібербезпеки [22]. Дослідники вказують, що ДПП означає ринковий підхід до кібербезпеки, яка є частиною національної безпеки [23, с. 49]; спосіб передачі обов'язків безпеки приватному сектору на ринкових принципах [24, с. 299]. Державно-приватне партнерство передбачає партнерську взаємодію приватних організацій з державними органами, за якої вони мають добровільно обмінюватися знаннями про національну безпеку, брати на себе відповідальність за забезпечення ефективної протидії кіберзагрозами [23, с. 50].

Ми вважаємо, що для забезпечення подальшого впровадження механізмів державно-приватного партнерства у сфері забезпечення кібербезпеки необхідні такі заходи:

— проведення в нашій країні реформ, які перетворять її на сучасну конкурентоспроможну європейську державу та виведуть з кризи;

— боротьба з корупцією на всіх рівнях державної влади та місцевого самоврядування;

— усунення недоліків у нормативно-правовому регулюванні ДПП та кібербезпеки;

— інформаційно-аналітичне забезпечення суб'єктів кібербезпеки та підвищення ефективності моніторингу у цій сфері;

— забезпечення тісної співпраці держави, приватного сектору та суспільства для стратегічного планування забезпечення кібербезпеки;

— підготовка рекомендацій щодо реалізації проектів ДПП для усіх суб'єктів забезпечення кібербезпеки;

— посилення прогностичної функції системи управління кібернетичною безпекою;

— підготовка кваліфікованих спеціалістів з державного управління для практичної реалізації проектів ДПП;

— вивчення позитивного міжнародного досвіду ДПП та можливостей його застосування в Україні.

ВИСНОВКИ І ПЕРСПЕКТИВИ ДОСЛІДЖЕННЯ

Можемо зробити висновок, що сьогодні держава приділяє достатню увагу вдосконаленню процесів кібер-

безпеки, але регулювання безпеки залишається неефективним. Тому особливо актуальним стає залучення до вирішення цих питань бізнесу та громадян, використовуючи модель державно-приватного партнерства. Бізнес як приватний учасник має технічний, фінансовий, інтелектуальний, людський капітал, який може допомогти державі у вирішенні певних ринкових проблем. Державно-приватне партнерство вирішує такі завдання у сфері вдосконалення кібербезпеки: технічка безпека та захист даних, надійний доступ до інтернету, обмін даними щодо загроз та атак, допомога у вирішенні виникаючих проблем у інтернет-просторі. Політика кібербезпеки засновується на таких принципах: інноваційності та ефективності, цілісності та доступності, свободи та справедливості, відповідальності та прозорості. Сьогодні розвиток механізму взаємодії бізнесу і держави цілком залежить від вітчизняної законодавчої бази по питанням кібербезпеки та впровадженні інноваційних підходів. Подальші дослідження, на нашу думку, повинні бути спрямовані на наукове обгрунтування інноваційних форм впровадження механізму ДПП у сфері кібербезпеки України.

Література:

1. Європейська комісія, Спільне звернення до Європейського парламенту, Ради, Європейського соціально-економічного комітету та Комітету регіонів — Стратегія ЄС із кібербезпеки: відкритий, надійний і безпечний кіберпростір, Брюссель, 2 липня 2013 р., с. 3. URL: http://ec.europa.eu/information_ society/newsroom/cf/dae/document.cfm?doc_id=166 (дата звернення 10.10.2019).

2. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". Правова інформатика. 2014. № 2 (42). С. 1—9.

3. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. Інформаційне право. 2017. № 7. С. 109—110.

4. Корченко О.Г., Бурячок В.Л., Гнатюк С.О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. Ukrainian Scientific Journal of Information Security. 2013. № 19. С. 40—44.

5. Стратегія кібербезпеки України: затверджена Указом Президента України від 15 берез. 2016 р. № 96. Офіційний вісник України. 2016. № 23.

6. Концепція розвитку сектору безпеки і оборони України: затверджена Указом Президента України від 14 берез. 2016 р. № 92. Офіційний вісник України. 2016. № 23.

7. Про захист інформації в інформаційно-телекомунікаційних системах: закон від 05.07.1994 № 80/94 ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.

8. Діордіца І.В. Поняття та зміст національної системи кібербезпеки, Інформаційне право. URL: http://goal-int.org/ ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/ (дата звернення 10.10.2019).

9. Про Національний банк України: закон від 11.10.2017 № 679 XIV. Відомості Верховної Ради України. 1999. № 29. Ст. 238.

10. Herring M.J., Willett K.D. Active cyber defense: a vision for real-time cyber defense. J Inform Warfare, 2014. 13 (2). P. 46—55.

11. Marvell S. The real and present threat of a cyber breach demands real-time risk management. Acuity Risk Management. 2015. P. 26—27.

12. Кібератака на Україну: СБУ залучила міжнародних експертів, 27 червня 2017 р. URL: http://espreso.tv/ news/2017/06/27/kiberataka_na_ukrayinu_sbu_zaluchyla_mizhnarodnykh_ekspertiv (дата звернення 10.10.2019).

13. Хакерські атаки на Україну. 2017. URL: https://ru.wikipedia.org/wiki/Хакерские_атаки_на_Украину_ (дата звернення 10.10.2019).

14. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. Вчені записки ТНУ ім. В.І. Вернадського. Серія: Державне управління. 2018. № 3, т. 29 (68). С. 57—61.

15. Пасічник М.В. Механізми впровадження нового публічного менеджменту: досвід США. Державне управління: теорія та практика. 2009. № 1. URL: http://www.academy.gov.ua/ej/ej9/doc_pdf/Pasichnyk_-MV.pdf. (дата звернення 10.10.2019).

16. Трофимова И.Н. Трансформация отношений центральной и местной власти в процессе децентрализации управления (опыт европейских стран). ARS ADMINISTRANDI. 2011. № 2. URL: http://ars-administrandi.com/article/Trofimova_ 2011_2.pdf (дата звернення 10.10.2019).

17. Закон України "Про державно-приватне партнерство": від 1 лип. 2010 р. № 2404-VI. — URL: http://zakon0.rada.gov.ua/laws/show/2404-17 (дата звернення 10.10.2019).

18. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналітична доповідь / за заг. ред. Д. Дубова, Київ: НІСД, 2018. 84 с.

19. Забара І.М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій. Журнал європейського і порівняльного права. 2017. Вип. 3. С. 1—13.

20. Cyber Resilience. Playbook for Public Private Collaboration. WEF, 2018. 71 p.

21. Бурячок В.Л. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. Інформаційна безпека: виклики і загрози сучасності: зб. матеріалів наук.-практ. конф., 5 квіт. 2013 р. Київ: Наук.-вид. центр НА СБ України, 2013. 416 с.

22. Офіційний сайт "Українська академія кібербезпеки". URL: https://uacs.kiev.ua (дата звернення 10.10.2019).

23. Carr M. Public-private partnerships in national cyber-security strategies. International Affairs. 2016. № 92 (1). P. 43—62.

24. Bures O. Contributions of private business to the provision of security in the EU: beyond public-private partnerships. Crime, Law and Social Change, 2017, no 67 (3). P. 289—312.

References:

1. European Commission (2013), "Joint Statement to the European Parliament, the Council, the European Social and Economic Committee and the Committee of the Regions — EU Cybersecurity Strategy: Open, Reliable and

Secure Cyberspace", available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm? doc_id=166 (Accessed 10 October 2019).

2. Baranov, O.A. (2014), "About interpreting and defining "cybersecurity", Pravova informatyka, vol. 2 (42), pp. 1—9.

3. Diorditsa, I.V. (2017), "Cybersecurity system: essence and purpose", Informatsiine pravo, vol. 7, pp. 109—110.

4. Korchenko, O.H. Buriachok, V.L. and Hnatiuk, S.O. (2013), "State Cyber Security: Characteristics and Problem Aspects", Ukrainian Scientific Journal of Information Security, vol. 19, pp. 40—44.

5. President of Ukraine (2016), Decree "Ukraine's cybersecurity strategy", Ofitsiinyi visnyk Ukrainy, vol. 23.

6. President of Ukraine (2016), Decree "The concept of development of the security and defense sector of Ukraine", Ofitsiinyi visnyk Ukrainy, vol. 23.

7. Verkhovna Rada of Ukraine (1994), The Law of Ukraine "On the protection of information in information and telecommunication systems", Vidomosti Verkhovnoi Rady Ukrainy, vol. 31, p. 286.

8. Diorditsa, I.V. (2016), "The concept and content of the national cyber security system", Informatsiine pravo, available at: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/ (Accessed 10 October 2019).

9. Verkhovna Rada of Ukraine (1999), The Law of Ukraine "About the National Bank of Ukraine", Vidomosti Verkhovnoi Rady Ukrainy, vol. 29, p. 238.

10. Herring, M.J. and Willett, K.D. (2014), "Active cyber defense: a vision for real-time cyber defense", J Inform Warfare, vol. 13 (2), pp. 46—55.

11. Marvell, S. (2015), "The real and present threat of a cyber breach demands real-time risk management", Acuity Risk Management, pp. 26—27.

12. espreso.tv (2017), "Cyberattack on Ukraine: SBU attracts international experts", available at: http://espreso.tv/news/2017/06/27/kiberataka_na_ukrayinu_sbu_zaluchyla_mizhnarodnykh_ekspertiv (Accessed 10 October 2019).

13. wikipedia (2017), "Hacker attacks on Ukraine", available at: https://ru.wikipedia.org/wiki/Khakerskye_ataky_na_Ukraynu_ (Accessed 10 October 2019).

14. Kruhlov, V.V. (2018), "Public-Private Partnership in Cybersecurity", Vcheni zapysky TNU im. V.I. Vernadskoho. Seriia: Derzhavne upravlinnia, vol. 3, no. 29 (68), pp. 57—61.

15. Pasichnyk, M.V. (2009), "Mechanisms for implementing new public management: US experience", Derzhavne upravlinnia: teoriia ta praktyka, vol. 1, available at: http://www.academy.gov.ua/ej/ej9/doc_pdf/Pasichnyk_MV.pdf. (Accessed 10 October 2019).

16. Trofymova, Y.N. (2011), "Transformation of central and local government relations in the process of decentralization of governance (experience of European countries)", ARS ADMINISTRANDI, vol. 2, available at: http://ars-administrandi.com/article/Trofimova_2011_2.pdf (Accessed 10 October 2019).

17. Verkhovna Rada of Ukraine (2010), The Law of Ukraine "On Public-Private Partnership", available at: http://zakon0.rada.gov.ua/laws/show/2404-17 (Accessed 10 October 2019).

18. Dubov, D. (2018), Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy [Public-Private Partnership in Cybersecurity: International Experience and Opportunities for Ukraine], NISD, Kyiv, Ukraine.

19. Zabara, I.M. (2017), "Formation of modern legal foundations of European Union cyber security in the conditions of diffusion of new innovative technologies", Zhurnal yevropeiskoho i porivnialnoho prava, vol. 3, pp. 1—13.

20. WEF (2018), Cyber Resilience, Playbook for Public Private Collaboration WEF, Cologny, Switzerland.

21. Buriachok, V.L. (2013), "Characteristic features and problematic aspects of cyber security", Informatsijna bezpeka: vyklyky i zahrozy suchasnosti: zbirnyk materialiv naukovo-praktychnoi konferentsii [Information Security: Challenges and Threats of the Present: Collection of Proceedings of the Scientific and Practical Conference], Naukovo-vydavnychyj tsentr NA SB Ukrainy, Kyiv, Ukraine, 5 Apr.

22. Official site of the "Ukrainian Cybersecurity Academy" (2019), available at: https://uacs.kiev.ua (Accessed 10 October 2019).

23. Carr, M. (2016), "Public-private partnerships in national cyber-security strategies", International Affairs, vol. 92 (1), pp. 43—62.

24. Bures, O. (2017), "Contributions of private business to the provision of security in the EU: beyond public-private partnerships", Crime, Law and Social Change, vol. 67 (3), pp. 289—312.

Стаття надійшла до редакції 31.10.2019 р.