УДК 351:346.548

Круглов В.В.
Харківський національний університет будівництва та архітектури

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ

У статті проаналізовано можливості забезпечення кібербезпеки шляхом використання механізмів державно-приватного партнерства (ДПП). Державно-приватне партнерство все частіше починають розглядати як вирішення багатьох проблем, пов'язаних із управлінням кібербезпекою. Кібербезпека покликана захистити критичну інфраструктуру та інші важливі суспільні функції проти різних складних загроз і є центральною проблемою в сучасній політиці безпеки. Держава в процесі реалізації ДПП у сфері кібербезпеки зміщує акцент з контрольних функцій у бік координації та мотивації виконання завдань безпеки приватним партнером. Завдання, які повинно вирішити державно-приватне партнерство у сфері кібербезпеки: забезпечення надійного доступу до Інтернет-мережі; регулювання технічної безпеки; проведення обміну інформацією щодо загроз; здійснення допомоги щодо вирішення ситуацій, пов'язаних із загрозами.

Ключові слова: *державно-приватне партнерство, інвестиції, партнерство, кібербезпека, проекти.*

Постановка проблеми. Завдання, які покладаються на державу у сфері безпеки, досить складні та знаходять своє вирішення практично у всіх сферах суспільної та економічної діяльності. Виклики сучасного світу інколи важко передбачити, результати різноманітних криз потребують значних засобів та коштів на ліквідацію наслідків. У мінливому та динамічному світі держава основною цінністю визначає безпеку людини, захист її прав та свобод. Принципи безпеки проектуються на сукупну діяльність у політичній, соціальній, економічній, екологічній, інформаційній та інших сферах.

Враховуючи невпинний технологічний прогрес цивілізації, діяльність держави, підприємств, громадян поступово переміщується у сферу інформаційно-комунікативних технологій (ІКТ). Зазначена тенденція, маючи на меті сучасні форми реалізації господарських відносин, комунікативних зв'язків, засобів обробки та зберігання інформації, ускладнює завдання держави щодо реалізації функцій безпеки. Наявні сітьові комунікації, серверне обладнання, вузькоспеціалізовані фахівці знаходяться у сфері приватного бізнесу, а отже, питання взаємодії з державою є нагальним та важливим, враховуючи роль ІКТ у розвитку економіки, електронного врядування, функціонування баз даних, обміні конфіденційною інформацією, забезпеченні роботи стратегічно важливих об'єктів та інфраструктури.

Підвищена увага приділяється світовою спільнотою та урядами більшості країн діям, спрямованим на підвищення кібербезпеки та забезпечення кіберстійкості найбільш вразливих елементів інфраструктури. Особливістю системних рішень у сфері інформаційних технологій є значна залежність від приватних суб'єктів господарської діяльності, які забезпечують системи зв'язку, роботу комп'ютерних мереж, розробку програмного забезпечення, створюють сучасне обладнання для сфери ІКТ. Така ситуація сприяє тісній співпраці держави та приватного сектору у межах моделей державно-приватного партнерства (ДПП).

Аналіз останніх досліджень і публікацій. Питання розвитку державно-приватного партнерство вивчали у своїх працях такі дослідники, як Б. Вагнер, М. Карр, К. Петерсен, Т. Тропіна та ін. Дослідженням проблематики кібербезпеки присвятили свої праці А. Клімбург, К. Мін, М. Хан та ін. Але незважаючи на значну кількість публікацій щодо зазначеної сфери діяльності, залишається не в повній мірі дослідженою проблематика застосування механізмів державно-приватного партнерства у сфері кібербезпеки.

Мета статті – розглянути та проаналізувати можливості забезпечення кібербезпеки шляхом використання механізмів державно-приватного партнерства.

Виклад основного матеріалу дослідження. Ступінь, в якій суспільство в даний час залежить від

інформаційних технологій у всіх аспектах повсякденного життя, створило нові і розширені вектори, через які може проявлятися злочинність [1].

Держава несе відповідальність за реалізацію політики у сфері безпеки, що вимагає відповідних дій по захисту національних та суспільних інтересів. Але сучасні загрози, такі як кібертероризм, кіберзлочинність, інформаційні війни, змушує державу шукати партнерів для забезпечення ефективного виконання своїх функцій стосовно протидії злочинній діяльності з використанням комп'ютерних технологій.

Кібер-ризик є і буде залишатися одним з найнагальніших завдань, пов'язаних із четвертою промисловою революцією. Представники державного та приватного сектору визнають, що пом'якшення зазначеного ризику потребує продовження співпраці [2, с. 3].

Розробка та розповсюдження програм, які приносять шкоду комп'ютерній техніці, «слідкують» за діями користувачів, викрадають персональні дані, досягло величезних масштабів. Тільки в 2016 році було випущено 357 мільйонів нових варіантів шкідливих програм, а «банківські трояни», призначені для крадіжки даних входу в обліковий запис, можна було купити всього за 500 доларів США [3]. Якщо врахувати те, що кількість пристроїв, які мають доступ до Інтернет-мережі, невпинно зростає, то результати кіберзлочинів можуть мати суттєві негативні наслідки.

Прикладами нанесення шкоди є атака WannaCry, яка торкнулася 300 тисяч комп'ютерів в 150 країнах; Petya і NotPetya, що викликало величезні корпоративні втрати. За даними Merck, FedEx і Maersk, втрати в третьому кварталі 2017 р. становили близько 300 мільйонів доларів США в результаті NotPetya. Крім фінансових втрат, атака WannaCry порушила критичну та стратегічну інфраструктуру по всьому світу, включаючи урядові органи, залізниці, банки, постачальників телекомунікаційних послуг, енергетичні компанії, автовиробників і лікарні [4].

Кібербезпека є діями щодо захисту критичної інфраструктури та інших важливих суспільних функцій проти APT (advanced persistent threat – «розвиненої стійкої загрози» або цільової кібератаки) та інших складних зовнішніх атак [5].

А. Клімбург [6] стверджує, що, сфери кібербезпеки хоч і представляють різні грані однієї і тієї ж проблеми, кожне з полів має свій особливий фокус і лексику. Кібербезпеку можна назвати широкою концепцією, яка включає безпеку як в онлайн-режимі, так і в автономному режимі, або тільки безпеку в Інтернеті [7].

Кібербезпека стає центральною проблемою в сучасній політиці безпеки. У 2017 р. кібер-загрози знову опинилися в числі найбільших загроз в світовій оцінці загроз з боку США [8]. Кібербезпека стоїть на порядку денному уряду Великобританії, про що свідчать недавні інвестиції в розмірі 1,9 млрд фунтів стерлінгів в п'ятирічну стратегію кібербезпеки, яка була введена в дію в лютому 2017 року з офіційним відкриттям Національного Центру кібербезпеки [9].

Початкове розуміння повністю саморегулівного та надійного, децентралізованого Інтернету піддалося сильним випробуванням через структурні вразливості, недоступні будь-якому окремому суб'єкту [10]. Ці вразливості все частіше використовуються зростаючим числом користувачів-злочинців, які надають свої послуги і шкідливі продукти для продажу та широкого доступу. Це вимагає більш багатопланових і скоординованих підходів до управління для підвищення кібербезпеки в Інтернеті [11].

Якщо розглянути питання більш детально, то бачимо, що кіберпростір створюється, а кібербезпека забезпечується на рівні фізичної інфраструктури – в межах логічних інтерфейсів, які використовуються для запуску і підключення цих інфраструктур та рівні поточного контенту (інформації), який зберігається в цих мережах і на рівні користувачів (як індивідуальних, так і корпоративних), які працюють або залежать від цих систем. Технічні рівні мають вирішальне значення для системної кібербезпеки, але не обов'язково залежать від державного втручання [12].

Політика кібербезпеки зводиться до ключових цінностей: безпека, конфіденційність, справедливість, економічна цінність і підзвітність. Безпека визначає захист активів (матеріальних і нематеріальних) від заподіяння шкоди. Збиток може являти собою втрату доступності, цілісності та розголошення конфіденційності активів, що призводить до зменшення вартості для законних власників активу. Конфіденційність є можливістю окремої особи, групи або організації обмежити інформацію про себе. Межі конфіденційності варіюються в залежності від контексту і країни. Сфера конфіденційності частково перетинається з безпекою, яка може включати поняття належного використання, а також захист інформації. Справедливість визначає ступінь, в якій суб'єкти всередині держави будуть піддаватися симетричній (необхідній) політиці, включаючи належний

процес. Економічна цінність – сума грошового і загального прибутку, викликаного або зупиненого певним вибором політики. Більш низькі витрати від діяльності в кіберпросторі можуть також сприяти підвищенню економічної цінності. Підзвітність – ступінь, за який підприємство (фізична особа, група, організація) може нести відповідальність за наслідки, що випливають з його дії або бездіяльності. Підзвітність державного і приватного секторів окремо розмежовується відповідно до конкретних моделей політики [2].

Пошук ключових елементів, які характеризують кібербезпеку та формують її забезпечення, наводять на думку про досить глибинний перетин інтересів держави як гаранта безпеки та приватних виробників та споживачів безпечного контенту. Дискусія щодо можливих меж втручання держави у віртуальні приватні сфери обміну інформацією, рух програмних продуктів, банківські (фінансові) дані демонструє необхідність формування партнерських відносин задля протистояння можливим кібернетичним загрозам, які постійно посилюються у світі. Можливості механізмів державно-приватного партнерства, на нашу думку, дають надію на створення чітких правил та моделей співпраці державного та приватного сектору у сфері кібербезпеки.

ДПП все частіше починають розглядати як вирішення багатьох проблем, пов'язаних з управлінням кібербезпекою. Державно-приватні партнерства служать способом організації, який може поліпшити гнучкість і надійність, включаючи більш широке коло громадянських і приватних суб'єктів.

Карр стверджує, що співпраця в ДПП тягне за собою «ринковий підхід» до кібербезпеки, яка є частиною національної безпеки [13]. Аналогічним чином ДПП розглядається як спосіб «передати» обов'язки безпеки приватному сектору на ринкових принципах [14, с. 299].

Для забезпечення кібербезпеки державним і приватним суб'єктам необхідно взаємодіяти одне з одним [15]. Це відображено в зростаючій кількості політичних ініціатив і публічних заяв, в яких підкреслюється цінність партнерських відносин між державним і приватним секторами для посилення або забезпечення кібербезпеки [16].

У стратегічних документах ЄС з кібербезпеки неодноразово підкреслювалася роль ДПП і співпраці приватного сектора в боротьбі з кібератаками і кіберзлочинністю [17]. ENISA опублікувала Керівництво з ефективної практики з конкретними рекомендаціями, які повинні надати допомогу державним та приватним зацікавленим сторонам в їх зусиллях по створенню і функціонуванню ДПП у сфері кібербезпеки [18].

У сучасній практиці пропонуються завдання державно-приватних взаємодій у сфері забезпечення кібербезпеки. Відповідно до функціональної логіки це такі завдання: надійне забезпечення доступу до Інтернету (ІКТ); спільне регулювання технічної безпеки, а також обробки даних; обмін інформацією про загрози і вразливості; взаємна допомога у вирішенні відомих загроз або незаконного контенту в кіберпросторі [19, с. 227].

У партнерській взаємодії приватні підприємства покликані добровільно ділитися знаннями про національну безпеку і взяти на себе відповідальність за забезпечення ефективного управління кібер-загрозами [13]. Обмін знаннями через ДПП розглядається як спосіб управління невизначеністю ризиків кібербезпеки [20, с. 1140]. Порядок денний ЄС з внутрішньої безпеки [21] стверджує, що співпраця з приватним сектором має вирішальне значення для структурування загальних зусиль по боротьбі з онлайн-злочинністю.

Як приклад сучасних моделей взаємодії державного та приватного сектору, є реалізація окремих питань Департаментом внутрішньої безпеки США. Для сприяння швидкому і своєчасному обміну індикаторами інформації про загрози між державним і приватним секторами Департамент внутрішньої безпеки США (DHS) створив автоматизовану програму по кіберзагрозам для сприяння співпраці між державним і приватним секторами. Програма DHS є нововведенням в наступних ключових аспектах: Automated Indicator Sharing (AIS) – автоматизований обмін показниками полегшує обмін між державним і приватним секторами, використовуючи загальне звернення від великих компаній, коли обмін інформацією є одностороннім; загрози на швидкостях мережі можуть бути вирішені майже так само швидко, як вони матеріалізуються [2]. Існують аналогічні приклади державно-приватного партнерства в європейських країнах (Великобританія, Нідерланди).

Комунікаційні та інформаційні системи розглядаються більшістю країн як елемент критичної інфраструктури. На жаль, українське законодавство не визначило наповненість поняття «критична інфраструктура» та її елементів, тим самим питання взаємодії держави та приватних суб'єктів в межах державно-приватного партнерства у сфері кібербезпеки має не урегульованість правових механізмів. Але в цілому держава в процесі реалізації ДПП у сфері кібербезпеки

зміщує акцент із контрольних функцій у бік координації та мотивації виконання завдань безпеки приватним партнером. Процес управління захистом інформаційної інфраструктури включатиме: визначення та передання цілей та пріоритетів; визначення необхідності дій; вибір інструментарію; перевірка ефективності дій.

Зважаючи на складність викладеного питання, 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. На цьому шляху необхідним є напрацювання відносин, пов'язаних з розкриттям конфіденційної, комерційної та персональної інформації, досягнення співвідношення інтересів партнерів, розробка контрольних та наглядових процедур.

Висновки. Таким чином, можна зазначити, що все більше уваги держава приділяє завданням щодо реалізації заходів із кібербезпеки інформаційної інфраструктури. Класичні підходи з державного регулювання сфери безпеки в сучасному світі не відзначаються високою ефективністю. Новим баченням є розуміння сектору безпеки як спільного підходу держави, приватного сектору та громадян. Одним із рішень проблем кібербезпеки стає використання моделей державно-приватного партнерства. Філософія такого підходу визначається забезпеченням окремих функцій держави на основі ринкових механізмів, які може реалізовувати приватний партнер, що має фінансові, технічні та інтелектуальні можливості. Завдання, які повинні вирішити ДПП у сфері кібербезпеки: забезпечити надійний доступ до Інтернет-мережі; регулювати технічну безпеку та обробку даних; проводити обмін інформацією щодо загроз і вразливостей; здійснювати допомогу щодо вирішення ситуацій, пов'язаних із загрозами або незаконним контентом в Інтернет-мережі. Ціннісні принципи політики кіберпезпеки базуються на основі економічної ефективності та інноваційності; забезпеченні цілісності та доступності; приватності та свободи; відповідальності та прозорості; справедливості.

Формування можливостей співпраці держави та приватних суб'єктів у сфері кібербезпеки у формі ДПП в значній мірі буде залежати від розробки законодавчих актів, які визначають принципи безпеки щодо критичних інфраструктур, підходи до питань взаємодії державних та приватних партнерів у сфері ІКТ та методології визначення кібер-ризиків.

Список літератури:

1. Wells D., Brewster B., Akhgar B. Challenges priorities and policies: mapping the research requirements of cybercrime and cyberterrorism stakeholders. Combatting Cybercrime and Cyberterrorism. Springer, Cham, 2016. P. 39–51.

2. Cyber Resilience. Playbook for PublicPrivate Collaboration. WEF, 2018. 71 p.

3. Internet Security Threat Report, volume 22. April 2017. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (дата звернення: 07.05.2018).

4. The Global Risks Report 2018. 13th Edition. Geneva, 2018. 80 p.

5. Christensen K. K., Petersen K. L. Public–private partnerships on cyber security: a practice of loyalty. International Affairs. 2017. № 93(6). P. 1435–1452.

6. Klimburg A. National cyber security framework manual. NATO Cooperative Cyber Defense Center of Excellence Publication. Tallinn, 2012. 235 p.

7. e Silva K. Europe's fragmented approach towards cyber security. Internet Policy Review. 2013. № 2(4). DOI: 10.14763/2013.4.202.

8. Coats D. R. Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence. Office of the Director of National Intelligence. United States, 2017. 28 p.

9. Kim J. Cyber-security in government: reducing the risk. Computer Fraud & Security. 2017. № 2017(7). P. 8–11.

10. Mueller M., Schmidt A., Kuerbis B. Internet security and networked governance in international relations. International Studies Review. 2013. № 15(1). P. 86–104.

11. Von Solms R., Van Niekerk J. From information security to cyber security. Computers & Security. 2013. № 38. P. 97–102.

12. DeNardis L. Hidden levers of Internet control: An infrastructure-based theory of Internet governance. Information, Communication & Society. 2012. № 15(5). P. 720–738.

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

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

15. Tropina T. Public–private collaboration: Cybercrime, cybersecurity and national security. Self-and co-regulation in Cybercrime, cybersecurity and national security. Springer, Cham, 2015. P. 1–41.

16. Min K. S., Chai S. W., Han M. An International Comparative Study on Cyber Security Strategy. International Journal of Security and Its Applications. 2015. № 9(2). P. 13–20.

17. Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 2013. 20 p.

18. Good Practice Guide on Cooperative Models for Effective Public Private Partnerships. Uropean Network and Information Security Agency (ENISA), 2011. 76 p.

19. Bossong R., Wagner B. A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union. Security Privatization. Springer, Cham, 2018. P. 219-247.

20. Christensen K. K., Petersen K. L. Public–private partnerships on cyber security: a practice of loyalty. International Affairs. 2017. № 93(6). P. 1435–1452.

21. The European Agenda on Security. Strasbourg, 2015. – 21 p.

ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

В статье проанализированы возможности обеспечения кибербезопасности путем использования механизмов государственно-частного партнерства (ГЧП). Государственно-частное партнерство все чаще начинают рассматривать как решение многих проблем, связанных с управлением кибербезопасностью. Кибербезопасность призвана защитить критическую инфраструктуру и другие важные общественные функции от различных сложных угроз и является центральной проблемой в современной политике безопасности. Государство в процессе реализации ГЧП в сфере кибербезопасности смещает акцент с контрольных функций в сторону координации и мотивации выполнения задач безопасности частным партнером. Задачи, которые должно решить государственно-частное партнерство в сфере кибербезопасности: обеспечение надежного доступа к сети Интернет; регулирования технической безопасности; проведение обмена информацией об угрозах; оказание помощи в решении ситуаций, связанных с угрозами.

Ключевые слова: *государственно-частное партнерство, инвестиции, партнерство, кибербезопасность, проекты.*

PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF CYBERSECURITY

The article analyzes the possibilities of providing cybersecurity by using mechanisms of public-private partnership (PPP). Public-private partnerships are increasingly considered as a solution to many of the problems associated with cybersecurity management. Cybersecurity is meant to protect critical infrastructure and other important public functions against various complex threats and is a central issue in today's security policy. The state, in the process of implementing PPP in the field of cybersecurity, shifts focus from control functions towards coordinating and motivating the fulfillment of security tasks by a private partner. The tasks to be solved by public-private partnership in the field of cybersecurity: ensuring reliable access to the Internet; technical safety regulation; exchange of information on threats; assistance in dealing with threats.

Key words: *public-private partnership, investments, partnership, cybersecurity, projects.*