УДК 342.52

ПЕТРОВ С.Г., *кандидат юридичних наук,* СБ України

ПРАВОВІ ОСНОВИ ВЗАЄМОДІЇ ДЕРЖАВНИХ ОРГАНІВ ТА ПРИВАТНИХ СУБ'ЄКТІВ ІЗ МЕТОЮ ЗАХИСТУ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Анотація. *У статті досліджуються питання взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки і зокрема захисту електронних інформаційних ресурсів України. З цією метою здійснено аналіз підходів в іноземних країнах, а також вітчизняного законодавства.*

Ключові слова*: кібербезпека, взаємодія, правові основи, електронні інформаційні ресурси України, державно-приватна взаємодія.*

Summary. *The article deals with the issues of interaction between public authorities and private entities with the aim of ensuring cybersecurity and protection of electronic information resources of Ukraine in particular. To this end, an analysis of approaches in foreign countries as well as domestic legislation, was carried out.*

Keywords*: Cybersecurity, Interaction, Legal Framework, Electronic Information Resources of Ukraine, Public-Private Interaction.*

Аннотация. *В статье исследуются вопросы взаимодействия государственных органов и частных субъектов с целью обеспечения кибербезопасности и в частности защиты электронных информационных ресурсов Украины. С этой целью осуществлен анализ подходов в иностранных государствах, а также отечественного законодательства.*

Ключевые слова: *кибербезопасность, взаимодействие, правовые основания, государственные электронные информационные ресурсы, государственно-частное взаимодействие.*

Постановка проблеми. Розвиток інформаційних технологій зумовлює розширення загроз безпеці України у сфері обігу державних електронних інформаційних ресурсів. Поширення фактів несанкціонованого доступу до таких відомостей, викрадення інформації з баз даних, знищення та модифікація даних у інформаційних системах, перехоплення інформації тощо зумовлює необхідність наукового обґрунтування питань взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України.

Стратегія кібербезпеки України передбачає необхідність взаємодії з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [1]. Питання ж захисту електронних інформаційних ресурсів України безпосередньо пов'язане із проблемою взаємодії державних і приватних суб'єктів у сфері кібербезпеки.

Результати аналізу наукових публікацій свідчать про те, що питання діяльності СБ України у сфері забезпечення інформаційної безпеки держави було предметом досліджень багатьох українських учених, а саме М.М. Галамби, О.Д. Довганя, О.О. Климчука, А.І. Марущака, В.В. Остроухова, В.М. Панченко, В.Г. Пилипчука, В.І. Польового, О.Б. Розвадовського, В.Б. Хлевицького, О.М. Юрченка та інших.

Питання взаємодії державного та приватного секторів у сфері кібербезпеки ще у 2014 році аналізували вітчизняні дослідники А.І. Марущак та В.М. Панченко з урахуванням іноземного досвіду і перспектив його використання для України [2].

І.Б. Жиляєв і А.І. Семенченко роблять акцент на необхідності врахування процесів децентралізації та деконцентрації влади, а також фінансово-економічних механізмів [3].

В.В. Круглов пропонує нове розуміння сектору безпеки як спільного підходу держави, приватного сектору та громадян, визначаючи одним із вирішень проблем кібербезпеки "використання моделей державно-приватного партнерства" [4].

Дослідники також звертають увагу на суто практичні питання державно-приватної взаємодії, наприклад, у контексті використання судових експертів задля попередження, виявлення та розслідування кіберзлочинів [5].

Останні наукові роботи з дотичної тематики визначають найбільш перспективними напрямами розвитку національної системи кіберзахисту, зокрема "створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль" [6, с. 106].

Проблематика державно-приватного партнерства для управління кіберзахистом і запобігання кіберзагрозам в умовах кризових ситуацій, надзвичайного стану, в особливий період актуалізувалося також у рекомендаціях парламентських слухань "Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України", у 2016 році [7].

Загалом, як бачимо, питання визначення правових основ взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України були предметом досліджень тільки частково.

Метою статті є розкриття правових основ взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України.

Виклад основного матеріалу. Насамперед, звернемо увагу на підходи в іноземних країнах до питань взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки загалом і захисту електронних інформаційних ресурсів зокрема. Національна стратегія захисту кіберпростору США, наприклад, окрім іншого визначає заходи, які мають зробити як урядові структури, так і приватні підприємства й користувачі для досягнення безпеки кіберпростору США [8]. Департамент внутрішньої безпеки США використовує програму Automated Indicator Sharing (AIS), яка забезпечує автоматизований обмін даними між державним і приватним секторами задля виявлення і локалізації кіберзагроз і кіберінцидентів [9]. Водночас, як вірно зазначають дослідники НІСД, така взаємодія, поряд із позитивними характеристиками, "викликає… занепокоєння з боку представників приватних компаній через односпрямованість інформаційного обміну, надмірну закритість державних органів" [10].

Подібна неоднозначність спостерігається і в Німеччині, де державно-приватне партнерство спрямоване "на встановлення взаємовигідних правил гри для операторів критично важливої інфраструктури", однак "значна кількість питань (особливо у сфері партнерства щодо об'єктів критичної інфраструктури) об'єктивно залишається невирішеною" [10].

Звернемо увагу на наукову роботу М. Карр і О. Бурес, у яких пропонується запроваджувати ринковий підхід до кібербезпеки у формі державно-приватного партнерства [11, с. 299]. Адже подібний підхід впроваджується у Великій Британії з акцентом на заходи посилення взаємної довіри у межах механізму державних закупівель, а також у забезпеченні державних структур якісними послугами у сфері цифрових технологій [10]. Зважаючи на виділення 1,9 млрд фунтів стерлінгів на

п’ятирічну стратегію кібербезпеки та відкриття Національного Центру кібербезпеки Великої Британії [12], питання взаємодії отримують належне фінансове підґрунтя.

Акцент на співпрацю державних органів з приватним сектором як засіб боротьби з он-лайн-злочинністю роблять і дослідники приватно-публічного партнерства в ЄС [13]. Дійсно, з 2013 року Стратегія кібербезпеки ЄС підкреслює роль взаємодії держави і приватного сектора в боротьбі з кібератаками і кіберзлочинністю [14]. Стратегія єдиного цифрового ринку 2015 р. [15] та Директива ЄС щодо мережевої та інформаційної безпеки [16], яка вступила в силу у серпні 2016 року, поглибили таку взаємодію. А Директива ЄС 2016/1148 від 6 червня 2016 року про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у ЄС [17] додала вимоги щодо окремих напрямів подібної взаємодії.

Перейдемо до розгляду вітчизняного законодавства щодо досліджуваного питання. Закон України “Про основні засади забезпечення кібербезпеки України” [18, ст. 10] регламентує питання державно-приватної взаємодії у сфері кібербезпеки. Однак, по-перше, зміст поняття “державно-приватна взаємодія” не повною мірою узгоджується з поняттям “державно-приватне партнерство”, закріпленим у Законі України “Про державно-приватне партнерство”. Відповідно, як вірно зазначають представники Національного інституту стратегічних досліджень (далі – НІСД), “не зрозуміло, чи є така взаємодія різновидом державно-приватного партнерства… і чи потрапляє вона під його дію” [10]. По-друге, механізми такої взаємодії і їх особливості для сфери кібербезпеки чітко не виписані.

Якщо державно-приватна взаємодія у сфері кібербезпеки є видом державно-приватного партнерства, то мають “спрацьовувати основні постулати відповідного механізму, наприклад, надання прав управління (користування, експлуатації) об’єктом партнерства або придбання, створення (будівництво, реконструкція, модернізація) об'єкта партнерства з подальшим управлінням (користуванням, експлуатацією), за умови прийняття та виконання приватним партнером інвестиційних зобов’язань відповідно до договору, укладеного в рамках державно-приватного партнерства; фіксація у договірних відносинах “державного інтересу”; довгостроковість відносин (від 5 до 50 років); передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства тощо [19].

Якщо ж державно-приватна взаємодія є іншим за змістом поняттям, то відповідні відносини потребують регулювання іншими правовими нормами. Зважаючи ж на особливості такої взаємодії у сфері кібербезпеки загалом і захисту державних електронних інформаційних ресурсів зокрема, потребує визначення не тільки відповідна термінологія, а й питання обміну даними про кіберінциденти та кібератаки, стандартів кібербезпеки, державних/приватних вимог до сертифікації відповідного обладнання та рішень тощо.

Висловимо позицію про те, що за відсутності закону про кіберзахист критичної інформаційної інфраструктури, питання державно-приватної взаємодії у сфері кібербезпеки не можуть бути урегульовані належним чином. Безумовно, прийняття Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [20] є позитивним кроком до створення підґрунтя для державно-приватної взаємодії у сфері кібербезпеки, однак видається за необхідне врегулювання відповідних питань на рівні закону, за попереднім узгодженням із приватними суб’єктами правових механізмів взаємодії (наприклад, участі т.зв. “білих хакерів” у захисті державних та приватних інтересів) та наданням їм певних повноважень і, можливо, преференцій.

Відзначимо активну позицію громадянського суспільства і представників ІТ-бізнесу у налагодженні плідної взаємовигідної співпраці у сфері кібербезпеки. Так, наприклад, Інтернет Асоціація України (ІнАУ) у 2018 році виступила ініціатором "Меморандуму порозуміння про взаємодію у боротьбі з кіберзлочинністю та злочинами, пов'язаними з цифровими доказами", який мав бути підписаний між Нацполіцією України, СБ України, РНБО України та ІнАУ й іншими представниками ринку телекомунікацій [21]. Безумовно, такий крок є важливим для розвитку державно-приватної взаємодії у сфері кібербезпеки в Україні, хоча на сьогодні зазначений Меморандум ще не підписаний.

За наявності неоднозначності у правовому регулюванні питань державно-приватної взаємодії існують непоодинокі приклади практики формування відповідних відносин. Так, зокрема, у Службі безпеки України розроблена і застосовується платформа для збирання, обробки та обміну інформацією про інциденти кібербезпеки, а також технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури в режимі реального часу – "Malware Information Sharing Platform" (MISP). З розпорядниками окремих об'єктів критичної інфраструктури підписані Меморандуми щодо надання доступу до інформаційної системи MISP-UA з метою обміну ідентифікаторами компрометації, що використовувались у кібератаках.

Крім того, за ініціативи СБ України започатковано проект CyberCrime@EAPIII спільно з Радою Європи, який серед іншого спрямований на покращення співробітництва правоохоронних і спеціальних органів країн-членів Східного партнерства з приватним ІТ-сектором у сфері використання електронних доказів у досудових розслідуваннях і протидії кіберзагрозам загалом.

Подібну активність у сфері взаємодії державних органів та приватних суб'єктів демонструють і МВС України, яке у 2015 році підписало Меморандум про взаєморозуміння з корпорацією "Майкрософт" щодо захисту даних, інформаційної та кібербезпеки.

Особливо високу динаміку розвитку КДПП демонструє Департамент кіберполіції Національної поліції України, який залучає експертів для обміну даними, проведення тренінгів для співробітників, взаємодіє з академічною спільнотою, наприклад, Харківським національним університетом радіоелектроніки, Національним аерокосмічним університетом ім. М.Є. Жуковського "ХАІ".

Інший суб'єкт Національної системи кібербезпеки – Національний банк України створив Центр кіберзахисту (CSIRT-NBU), на базі якого долучає представників банківської спільноти до питань формування критеріїв та методології віднесення об'єктів критичної інфраструктури банківської системи України до критичної інфраструктури та вирішення питань організації кіберзахисту в банківській системі України.

Підсумовуючи проведений аналіз, відзначимо, що розвиток правових основ взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів у загальному питанні кібербезпеки потребує, насамперед, запровадження змістовного діалогу як суб'єктів Національної системи кібербезпеки, так і представників ІТ-бізнесу. Такий діалог має бути спрямований на підвищення довіри між приватними суб'єктами та державними органами. У процесі такого діалогу мають використовуватися вже апробовані договірні і правові механізми США, країн ЄС щодо обміну інформацією про позиції та інтереси учасників, зокрема і визначення можливості формування недержавних регуляторних органів, формування системних підходів до підготовки і підвищення кваліфікації кадрів як державних, так і недержавних суб'єктів тощо.

Виконання приватними компаніями державних контрактів щодо підтримки рішень з електронного урядування, документообігу тощо зумовлюють необхідність розподілу обов'язків щодо захисту державних електронних інформаційних ресурсів. Крім того, під час кібератак об'єктами є як державні, так і недержавні ресурси, що зумовлює спільність інтересів при розслідуванні атак. Безумовно, приватні суб'єкти мають сумніви стосовно відкриття доступу до власної інформації з обмеженим доступом, намагаючись проводити внутрішні розслідування інцидентів і кібератак. Актуальними для приватного сектору є й репутаційні ризики, пов'язані з витоком інформації про ненадійність систем захисту на підприємстві. Саме ці питання мають стати предметом попереднього обговорення з наступним їх відображенням у нормах права.

Пропонуємо організувати відповідну платформу для обговорення питань взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України на базі Апарату РНБО України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Висновки.

Аналіз підходів в іноземних країнах до питань взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки загалом і захисту електронних інформаційних ресурсів зокрема, а також вітчизняного законодавства щодо досліджуваного питання дав підстави для наступних висновків.

Вважаємо за необхідність узгодження змісту поняття "державно-приватна взаємодія" з поняттям "державно-приватне партнерство". Пропонується при визначенні державно-приватної взаємодії звертати увагу на більш чітку термінологію щодо обміну даними про кіберінциденти та кібератаки, а також наявність більш детальних стандартів у державно/приватних вимогах до сертифікації відповідного обладнання.

Вважаємо, що за відсутності закону про кіберзахист критичної інформаційної інфраструктури, питання державно-приватної взаємодії у сфері кібербезпеки не можуть бути урегульовані належним чином.

Також вважаємо за необхідність запровадити змістовний діалог як суб'єктів Національної системи кібербезпеки, так і представників ІТ-бізнесу з метою підвищення довіри між приватними суб'єктами та державними органами з використанням апробованих договірних і правових механізмів США, країн ЄС щодо обміну інформації про позиції та інтереси учасників, зокрема і визначення можливості формування недержавних регуляторних органів, формування системних підходів до підготовки і підвищення кваліфікації кадрів як державних, так і недержавних суб'єктів тощо.

Відповідну платформу для обговорення пропонується організувати на базі Апарату РНБО України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Перспективами подальших наукових пошуків визначаємо питання напрацювання правових механізмів взаємодії державних і недержавних суб'єктів у сфері кібербезпеки.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.

2. Марущак А.І., Панченко В.М. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. *Інформаційна безпека людини, суспільства, держави*. 2014. № 3 (16). С. 63-79.

3. Жиляєв І.Б., Семенченко А.І. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. *Стратегічні пріоритети*. 2017. № 4. С. 55-63. URL: http://nbuv.gov.ua/UJRN/spa_2017_4_8

4. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Державне управління*. 2018. Т. 29(68). № 3. С. 57-61. URL: http://nbuv.gov.ua/UJRN/sntvupa_2018_29_3_13

5. Русецький А.А. Місце судових експертиз у системі протидії кіберзагрозам у сфері інформаційної безпеки України. *Теорія та практика судової експертизи і криміналістики*. 2018. Вип. 18. С. 263-271. URL: http://nbuv.gov.ua/UJRN/Tpsek_2018_18_32

6. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. № 9. С. 100-108.

7. Про Рекомендації парламентських слухань "Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України": Постанова Верховної Ради України. *Відомості Верховної Ради*. 2016. № 17. Ст. 191.

8. National Strategy to Secure Cyberspace. February 2003. URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

9. Cyber Resilience. Playbook for PublicPrivate Collaboration. URL: http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf

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

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

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

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

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

15. Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN#document1

16. NIS Directive on security of network and information systems. URL: https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

17. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

18. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

19. Сайт Міністерства розвитку економіки, торгівлі та сільського господарства. URL: http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=196d3373-eb07-4834-a61e-b3608f28eb22&title=SutnistDerzhavnoprivatnogoPartnerstva

20. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. *Офіційний вісник України*. 2019. № 50. ст. 1697.

21. ІнАУ пропонує кроки до ефективного державно-приватного партнерства в сфері кібербезпеки. https://inau.ua/news/inau-proponuye-kroky-do-efektyvnogo-derzhavno-pryvatnogo-partnerstva-v-sferi-kiberbezpeky.

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