УДК 336.2 +346.62
DOI https://doi.org/10.32850/LB2414-4207.2021.19.17

ПРАВОВЕ РЕГУЛЮВАННЯ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Шевчук Оксана Романівна,
кандидат юридичних наук,
доцент кафедри конституційного,
адміністративного та фінансового
права
юридичного факультету
(Західноукраїнський національний
університет, м. Тернопіль, Україна)

Чорний Євген Михайлович,
аспірант кафедри конституційного,
адміністративного та фінансового
права
юридичного факультету
(Західноукраїнський національний
університет, м. Тернопіль, Україна)

Стаття присвячена дослідженню існуючої нині в Україні проблеми неврегульованості операцій, що здійснюються в рамках угод про державно-приватне партнерство у сфері інформаційної безпеки. Співавтори дійшли до висновку про необхідність узгодження змісту категорії "державно-приватна взаємодія" та категорії "державно-приватне партнерство". Пропонується при визначенні державно - приватної взаємодії звернути увагу на більш чітку детермінацію процесу обміну даними про кібератаки та кіберінциденти, а також наявність деталізованих стандартів та вимог до сертифікації відповідного обладнання. Зазначено також, що в умовах відсутності закону у сфері інформаційної безпеки критичної інформаційної інфраструктури, питання державно-приватної взаємодії у сфері кібербезпеки не врегулювані належним чином.

Необхідно також запровадити ефективний діалог як суб'єктів державної системи кібербезпеки, так і представників ІТ-сфери з метою підвищення довіри між державними органами та приватними суб'єктами з використанням апробованих правових та договірних механізмів США, країн ЄС у сфері інформації про позиції та інтереси учасників, в тому числі й визначення можливості формування органів державної влади, а також системних підходів до навчання і підвищення кваліфікації кадрів як державних, так і недержавних владних суб'єктів тощо.

Співавтори дійшли до висновку, що необхідно запровадити ефективний діалог як суб'єктів державної системи кібербезпеки, так і представників ІТ-сфери з метою підвищення довіри між державними органами та приватними суб'єктами з використанням апробованих правових та договірних механізмів США, країн ЄС у сфері інформації про позиції та інтереси учасників, в тому числі й визначення можливості формування органів державної влади, а також системних підходів до навчання і підвищення кваліфікації кадрів як державних, так і недержавних владних суб'єктів тощо. Пропонується також організувати відповідну платформу з обговорення взаємодії між державними

органами та приватними структурами задля захисту електронних інформаційних ресурсів України на базі Ради національної безпеки та оборони України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Ключові слова: державно-приватне партнерство, концесії, інвестиції, оподаткування, інформація, інформаційна безпека.

LEGAL REGULATION OF PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF INFORMATION SECURITY

Shevchuk Oksana Romanivna,
Candidate of Law,
Associate Professor at the Constitutional,
Administrative and Financial
Law Department
of the Faculty of Law
(West Ukrainian National University,
Ternopil, Ukraine)

Chornyi Yevhen Mykhailovych,
Postgraduate Student at the
Constitutional, Administrative
and Financial Law Department
of the Faculty of Law
(West Ukrainian National University,
Ternopil, Ukraine)

The article is devoted to the study of the current problem in Ukraine of unregulated operations carried out within the framework of public-private partnership agreements in the field of information security. The co-authors come to the conclusion that it is necessary to harmonize the content of the category "public-private interaction" and the category "public-private partnership". It is proposed to pay attention to a clearer determination of the process of data exchange on cyberattacks and cyber incidents, as well as the availability of detailed standards and requirements for certification of relevant equipment when determining public - private interaction. It is also noted that in the absence of a law in the field of information security of critical information infrastructure, issues of public-private cooperation in the field of cybersecurity are not properly regulated.

It is also necessary to establish an effective dialogue between both the subjects of the state cybersecurity system and representatives of the IT sphere in order to increase trust between public authorities and private entities using proven legal and contractual mechanisms of the US, EU countries in the field of information on positions and interests , including the definition of the possibility of forming public authorities, as well as systemic approaches to training and retraining of personnel of both state and non-state authorities, etc.

The co-authors conclude that it is necessary to establish an effective dialogue between both the subjects of the state cybersecurity system and representatives of the IT sphere in order to increase trust between public authorities and private entities using proven legal and contractual mechanisms of the US, EU countries in the field of information. on the positions and interests of the participants, including the definition of the possibility of forming public authorities, as well as systematic approaches to training and retraining of personnel of both state and non-state authorities, etc. It is also proposed to organize an appropriate

platform to discuss cooperation between government agencies and private entities for the protection of electronic information resources of Ukraine on the basis of the National Security and Defense Council of Ukraine, involving a wide range of government officials, IT business, academia.

Key words: public-private partnership, concessions, investments, taxation, information, information security.

Постановка проблеми. Основною метою бюджетно-податкової політики України нині є досягнення макроекономічної рівноваги та створення стабільних фінансово-правових умов задля підтримки темпів зростання економіки країни. Очікуване збереження несприятливих зовнішньоекономічних умов, а також наявність низки невирішених внутрішніх структурних проблем економіки, що обмежують можливості для зростання, зумовлюють необхідність зосередження зусиль на розширенні потенціалу вітчизняної економіки. Досягненню цієї мети може сприяти створення стимулів для здійснення інвестицій, а також упровадження різних форм співпраці публічного й приватного партнерів.

Розроблення і використання моделей реалізації довгострокових інвестиційних проектів держави у взаємодії із бізнесом є загальносвітовою тенденцією. Потенційне різноманіття організаційно-правових форм державно-приватного партнерства (далі - ДПП) перетворює його в універсальний інструмент реалізації інвестиційної політики держави в широкому діапазоні сфер і галузей: від реалізації соціальних та інфраструктурних проектів до створення і виведення на ринок інноваційних продуктів.

Узагальнення кращих світових практик використання інструментів державно-приватного партнерства свідчить про їхню високу ефективність. Уряди багатьох країн світу підтримують проекти ДПП, що реалізуються за виконання частини функцій державою. Новою світовою тенденцією у сфері ДПП є розширення участі приватного капіталу в наданні державних послуг, наприклад, у сфері цифровізації процесів управління в освіті, охороні здоров'я, житловому будівництві, сільському господарстві, розвитку міських і сільських районів, розвитку людського капіталу, торгівлі, транспорту та інших [1]. Широке поширення інформаційних технологій у поєднанні з модернізацією концепцій нового державного управління збільшили участь приватного сектора в традиційно державних сферах. Приватним партнерам відводиться значна роль навіть у реалізації одного з найважливіших завдань, що виконуються державою організації процесу збору податків і контролю за повнотою їх надходження, зокрема, у створенні й підтримці процесу так званого електронного оподаткування [2; с. 283].

Аналіз останніх досліджень і публікацій. Проблематика правового регулювання операцій у сфері державно-приватного партнерства на сучасному етапі є предметом дослідження науковців та експертів, таких як: Oleksandr O. Bryhinets, Ivo Svoboda, Oksana R. Shevchuk, Yevgen V. Kotukh, Valentyna Yu. Radich, О. Шевчук, Ю. Панова, Stefan Verweij, Tim Busscher, Margo van den Brink та інших.

Проте проблемні питання правового регулювання державно-приватного партнерства у сфері інформаційної безпеки залишаються відкритими та потребують подальшого дослідження.

Метою статті є критичний огляд нових підходів до правового регулювання державно-приватного партнерства у сфері інформаційної безпеки й окреслення проблемних питань гармонійного розвитку взаємовідносин учасників інформаційного контролю.

Виклад основного матеріалу дослідження Особливу роль механізми ДПП відіграють у країнах з економікою, що розвивається (EMDE - emerging markets and development economies). Так, державно-приватне партнерство є значущим при здійсненні міської житлової політики в Індії, у розвитку портової інфраструктури в Азіатсько-Тихоокеанському регіоні, в наданні медичних та інших послуг соціального характеру в багатьох країнах. За даними Світового банку, завдяки ДПП протягом останніх 30 років понад 7000 інфраструктурних проектів на загальну суму 1,7 трлн. дол. США були реалізовані в 139 країнах [3; с.88].

У 2020 році інвестиції у проекти ДПП у країнах з економікою, що розвивається, склали 93,3 млрд. доларів США за 304 проєктами, що на 37% перевищує рівень 2016 року. Значне зростання ринку ДПП-проєктів у 2017 році був викликаний, головним чином, реалізацією кількох мегапроєктів у Китаї та Індонезії. Однак загальний обсяг інвестицій в цих країнах за 2017 рік на 15% нижче середнього рівня за попередні п'ять років (109,8 млрд. дол. США), при цьому кількість проєктів збільшилася на 9% - з 280 (в 2016 році) до 304 (в 2017 році). Збільшення переважно було пов'язано з Єгиптом, де кількість ініційованих проєктів зросла з 2 до 25. Крім того, реалізація проектів ДПП здійснювалася 2017 року в 52 країнах, тоді як в 2016 році подібні проєкти реалізовувалися в 37 країнах [4; с.30]

Нині розвиток державно-приватного партнерства знаходиться також у сфері стратегічних інтересів України. В умовах скорочення й очевидного дефіциту бюджетного фінансування громадської інфраструктури в Україні кількість проєктів, реалізація яких здійснюється з використанням механізмів державно-приватного партнерства, збільшується. На нашу думку, однією з причин недостатнього поширення в Україні угод про ДПП в порівнянні з концесійними угодами та іншими формами державно-приватної співпраці можна назвати поточний стан нормативно-правового регулювання в цій сфері, та наявність положень, які можуть неоднозначно трактуватися учасниками угод.

В умовах підвищеного інтересу до механізму ДПП як з боку держави, так і з боку господарюючих суб'єктів, особливої актуальності набуває створення законодавчої бази, яка регламентує особливості правового регулювання низки питань, що виникають у рамках угод про державно-приватне партнерство у сфері інформаційної безпеки. Експертне дослідження проблем і перспектив розвитку ринку державно-приватного партнерства у сфері інформаційної безпеки в Україні свідчить, що до числа проблем, які відзначають учасники ДПП-проєктів, відноситься й відсутність нормативно-правової бази, що регулює порядок забезпечення інформаційної безпеки проектів ДПП. Акцент на співпрацю органів державної влади з приватним сектором як метод боротьби з онлайн-злочинністю здійснюють і К. Мін і М. Хан (*K. S. Min, S.W. Chai, M. Han, 2015),* які є дослідниками механізмів приватно-публічного партнерства в ЄС [5; с. 13].

Дійсно, починаючи з 2013 року, Стратегія кібербезпеки ЄС установлює роль взаємодії органів державної влади й приватного сектора в боротьбі з кіберзлочинністю та кібератаками *(New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient Brussels, (16 December, 2020)* [6]. Стратегія спільного цифрового ринку 2015 року та Директива ЄС щодо мережевої інформаційної і мережевої безпеки, яка набула чинності в серпні 2016 року, поглибили зазначену взаємодію.

Розглянемо вітчизняне законодавство щодо державно-приватного партнерства у сфері інформаційної безпеки. У Законі України "Про основні засади забезпечення кібербезпеки України" [7] регламентовано питання державно-приватної взаємодії у сфері інформаційної безпеки. Проте зміст терміну "державно-приватна взаємодія"

не повністю дублює поняття "державно-приватне партнерство", зазначене в Законі України "Про державно-приватне партнерство". Відповідно, як вірно зазначають О Шевчук та Н. Ментух *(O. Shevchuk, N. Mentuh, 2020)* "не до кінця зрозуміло, чи є зазначена взаємодія формою державно-приватного партнерства… і чи потрапляє вона під його критерії" [8]. Крім того, механізми такої взаємодії та їхня специфіка для сфери інформаційної безпеки чітко не встановлені.

Якщо державно-приватна взаємодія в галузі кібербезпеки є формою державно-приватного партнерства, то повинні простежуватися базові постулати відповідного державного механізму, наприклад, надання права управління, користування, використання майна, що є об'єктом партнерства або придбання, створення (реконструкція, будівництво, модернізація) об'єкта партнерства з подальшим управлінням, експлуатацією, користуванням за умови виконання та прийняття приватним партнером базових інвестиційних зобов'язань відповідно до положень договору, який укладено в рамках державно-приватного партнерства; встановлення в договірних відносинах "державного інтересу"; строковість відносин (тривалість від 5 до 50 років); покладення на приватного партнера частини ризиків, пов'язаних із здійсненням державно-приватного партнерства.

Якщо державно-приватна взаємодія - це інша концепція, то ці відносини повинні регулюватися іншими законами та нормативними актами. З огляду на особливості такої співпраці в галузі кібербезпеки, особливо захисту національних електронних інформаційних ресурсів, необхідно не лише визначити відповідні терміни, а й визначити обмін даними про кіберінциденти та кібератаки, стандарти кібербезпеки, сертифікацію відповідного обладнання, вирішення державних та приватних вимог.

Вважаємо, що за відсутності закону про кібербезпеку критичної інформаційної інфраструктури питання державно-приватної взаємодії у сфері інформаційної безпеки не можуть бути урегульовані належним чином. Звичайно, прийняття "Загальних вимог до захисту мереж критичної інфраструктури" є позитивним кроком на шляху закладання основи державно-приватної співпраці в галузі кібербезпеки, але видається необхідним вирішити відповідні питання на юридичному рівні та заздалегідь узгодити з приватними структурами, надати їм певні повноваження та можливі преференції.

За наявності колізій у правовому регулюванні механізму державно-приватної взаємодії існують численні приклади формування відповідних відносин. Так, Служба безпеки України розробила та застосувала платформу для збору, обробки та обміну інформацією про інциденти в кібербезпеці в реальному часі, а також технічні дані про ідентифікатор пошкодження інформаційної системи критичної інфраструктури. Активність у галузі взаємодії приватних суб'єктів та державних органів демонструє і МВС України, яке в 2015 році укладає Меморандум про співпрацю з корпорацією Microsoft щодо захисту особистих даних, інформаційної та кібербезпеки.

Інший суб'єкт державної системи кібербезпеки - це Національний банк України, який створив Центр інформаційного захисту (CSIRT-NBU), на базі якого залучає представників банківської спільноти до визначення критеріїв та встановлення методології віднесення об'єктів критичної інформаційної інфраструктури фінансової системи України до об'єктів критичної інфраструктури, а також до вирішення питань забезпечення кіберзахисту фінансової системи України.

Тому ми дійшли до висновку, що до загальних питань кібербезпеки для формування правової бази співпраці державних органів і приватних структур задля захисту електронних інформаційних ресурсів потрібен діалог між національними відділами кібербезпеки та ІТ-відділами бізнесу. Цей діалог має бути спрямований на формування

довіри між приватними суб'єктами та державними органами влади. У такому процесі діалогу повинні використовуватися контрактні та правові механізми, перевірені Сполученими Штатами й країнами ЄС, задля обміну інформацією про позиції та інтереси учасників, включаючи визначення можливості створення недержавних регулюючих органів та формування системного підходу, підготовку та перепідготовку державних і недержавних структур тощо.

Реалізація приватними компаніями державних контрактів у сфері підтримки електронного врядування, документообігу тощо зумовлює необхідність розподілу обов'язків у сфері захисту державних електронних інформаційних ресурсів. Окрім того, під час кібератак об'єктами є як державні, так і приватні ресурси, що зумовлює спільність інтересів під час розслідування атак. Безумовно, приватні суб'єкти мають заперечення стосовно відкриття доступу до власної інформації з обмеженим доступом, намагаючись проводити внутрішні розслідування інцидентів і кібератак. Репутаційні ризики, пов'язані з розкриттям недостовірної інформації про системи корпоративної безпеки, також пов'язані з приватним сектором. Ці питання повинні бути предметом первинного обговорення та згодом відображені в законі.

Ми пропонуємо організувати відповідну платформу для обговорення взаємодії між державними органами та приватними структурами задля захисту електронних інформаційних ресурсів України на базі Ради національної безпеки та оборони України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Висновки з дослідження і перспективи подальших досліджень у цьому напрямі. Аналіз міжнародного досвіду правового регулювання взаємодії державних органів та приватних суб'єктів із метою забезпечення інформаційної безпеки загалом та захисту інформаційних ресурсів зокрема, а також вітчизняного законодавства у сфері досліджуваного питання дає підстави для наступних висновків.

Вважаємо за необхідне узгодити зміст категорії "державно - приватна взаємодія" та категорії "державно-приватне партнерство". Пропонуємо при визначенні державно - приватної взаємодії звернути увагу на більш чітку детермінацію процесу обміну даними про кібератаки та кіберінциденти, а також на наявність деталізованих стандартів і вимог до сертифікації відповідного обладнання.

Вважаємо, що в умовах відсутності закону у сфері інформаційної безпеки критичної інформаційної інфраструктури, питання державно-приватної взаємодії у сфері кібербезпеки не врегульовані належним чином.

Також вважаємо за необхідне запровадити ефективний діалог як суб'єктів державної системи кібербезпеки, так і представників ІТ-сфери з метою підвищення довіри між державними органами та приватними суб'єктами з використанням апробованих правових та договірних механізмів США, країн ЄС у сфері інформації про позиції та інтереси учасників, в тому числі й визначення можливості формування органів державної влади, а також системних підходів щодо навчання і підвищення кваліфікації кадрів як державних, так і недержавних владних суб'єктів тощо.

Ми пропонуємо організувати відповідну платформу для обговорення взаємодії між державними органами та приватними структурами задля захисту електронних інформаційних ресурсів України на базі Ради національної безпеки та оборони України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Перспективами подальших наукових досліджень визначаємо питання розробки правових механізмів взаємодії органів державної влади та недержавних суб'єктів у сфері кібербезпеки.

Список використаних джерел:

1. Bryhinets O.O., Svoboda I., Shevchuk O.R., Kotukh Y.V., Radich V.Y. Public value management and new public governance as modern approaches to the development of public administration. Revista San Gregorio. Special edition. 2020.Núm. 42.

2. Шевчук О., Кузь Т. Правове забезпечення інформаційної безпеки процесу надання електронних адміністративних послуг. *Актуальні проблеми правознавства.* 2021. № 1. С. 59-66.

3. Kruhlov V. V. Public-private partnership in the field of cybersecurity. "Scientific Notes of Taurida V. I. Vernadsky University", series "Public Administration. 2018. No 29(68). P. 57–61.

4. 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.

5. 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.

6. New E.U. Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient Brussels, 16 December, 2020. URL: file:///C:/Users/User/Downloads/New_EU_Cybersecurity_Strategy_and_new_rules_to_make_physical_and_digital_critical_entities_more_resilient.pdf (Дата звернення 18.06.2021).

7. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року№ 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (Дата звернення 18.06.2021)

8. O Shevchuk N. Mentuh Korzyści podatkowe jako element wspierający podmioty ekonomiczne w okresie walki z COVID-19: aspekt porównawczy i prawny - Analizy i Studia CASP, 2020.

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

10. Bergmann A. Editorial: Digitalization starts affecting core processes. *Public Money & Management*. 2021. Vol. 41. No4. P. 279-280.

11. Medhekar A. Public-private Partnerships for Inclusive Development: Role of Private Corporate Sector in Provision of Healthcare Services, Procedia - Social and Behavioral Sciences. 2014. Vol.157. P. 33-44. ISSN 1877-0428, https://doi.org/10.1016/j.sbspro.2014.11.007.

12. Parker L.A., Zaragoza G.A., Hernández-Aguado I. Promoting population health with public-private partnerships: Where's the evidence?. *BMC Public Health.* 2019. No19. P. 1438. https://doi.org/10.1186/s12889-019-7765-2

13. Tshombe L., Molokwane T. An analysis of public private partnership in emerging economies. *Risk governance & control: financial markets & institutions.* 2016. No 6(4-2). P. 306-316. https://doi.org/10.22495/rgcv6i4c2art8

14. Rowe S., Alexander N., Kretser A. et al. Principles for building public-private partnerships to benefit food safety, nutrition, and health research. *Nutr Rev*. 2013. Vol. 71(10). P.682-691. doi:10.1111/nure.12072