УДК 340:007

Єрменчук О.П. ©
кандидат юридичних наук
(Служба безпеки України)

DOI: 10.31733/2078-3566-2019-1-62-66

ПРИВАТНИЙ СЕКТОР ЯК ВАЖЛИВИЙ СУБ'ЄКТ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття присвячена вивченню правових засад функціонування приватного сектору та аналізу його взаємодії з державою у сфері захисту критичної інфраструктури на прикладі різних світових держав. За результатами запропоновано форму взаємодії, необхідні повноваження та прогнозується можлива вигода від спільних заходів приватного сектору як суб'єкта захисту критичної інфраструктури.

***Ключові слова**: приватний сектор, партнерство, правове регулювання, захист, критична інфраструктура.*

Постановка проблеми. Позиція держав – лідерів ЄС за розвитком економіки та за можливістю впливати на геополітичну ситуацію у світі свідчить про усвідомлення ними прямої залежності національного благополуччя від безпечної та стійкої критичної інфраструктури (КІ) за умов досить глибокої інтегрованої взаємодії державного та приватного сектору. Їх стосунки у єдиному державно-приватному механізмі засновані на двосторонній вигоді та характеризуються наданням досить широких повноважень із захисту критичної інфраструктури представникам приватного сектору [1-2].

Директивою ЄС від 08.12.2008 № 114 "Про визначення та зміст європейської критичної інфраструктури та про оцінку необхідності підвищення рівня її захисту" закладено основи для реалізації політики щодо заохочення повноцінної участі приватного сектору у захисті критичної інфраструктури. У цьому документі визнано важливу роль приватного сектору у захисті критичної інфраструктури на рівні з державною системою [3].

Побудова в Україні відповідної системи вимагає врахування позитивного досвіду світових держав-лідерів та актуалізує наукові дослідження проблеми участі приватного сектору спільно з державними органами у захисті об'єктів критичної інфраструктури.

Аналіз публікацій стосовно різних аспектів захисту критичної інфраструктури висвітлено в роботах Д.С. Бірюкова, І.Д. Бондаренка, С.І. Кондратова, С.П. Іванюти, О.О. Климчука, І.В. Манжул, О.І. Насвіт, В.М. Панченко, В.В. Петрова, П.П. Скурського, О.М. Суходолі, В.Н. Цигичка та інших. Дослідженню окремих аспектів державно-приватного партнерства приділяли увагу такі науковці як О.М. Вінник , Р.Н. Джабраілов, М.Ю. Маісурадзе, П.П. Надолішній, В.М. Устименко та інші. Водночас, проблеми функціонування приватного сектору, як суб'єкта захисту критичної інфраструктури та його взаємозобов’язання з державними партнерами до сьогодні не були окремим об’єктом наукового дослідження та потребують додаткового вивчення, що і становить **мету** наукового дослідження автора.

Виклад основного матеріалу. Діяльність суб'єктів захисту КІ побудована на прямих вигодах, пов'язаних з чітким та спільним інтересом у забезпеченні безпеки та стійкості критичної інфраструктури нації.

У контексті цього, "партнерство" визначається як тісна співпраця між сторонами, які мають спільні інтереси у досягненні єдиної мети. З огляду на різні завдання, ролі та відповідальність партнерів у сфері функціонування критичної інфраструктури необхідними є гнучкі, активні та всеохоплюючі партнерські стосунки, спрямовані на підвищення надійності та стійкості критичної інфраструктури.

Згідно із вищезазначеною директивою ЄС на національних рівнях у різних країнах відповідні норми закріплюються переважно у стратегіях національної безпеки, стратегіях захисту різних сфер та інших базових розпорядчих актах, що стосуються функціонування критичної інфраструктури, зокрема і в планах її захисту.

Основою злагоджених дій між учасниками від держави й приватного сектору, а

також міждержавного характеру стала "Попереджувальна інформаційна мережа критичної інфраструктури" (CIWIN). Це захищена, інформаційна, комунікаційна і попереджувальна система для обміну інформацією між членами ЄС про спільні загрози, ризики, уразливість та відповідні заходи зі зменшення ризиків. Для цього в державах – членах ЄС створено конкретні контактні місця. За їх допомогою існує можливість на форумі обмінюватись інформацією щодо захисту критичної інфраструктури. Також наявною є функція своєчасного попередження учасників про загрози. Окрім уповноважених державних службовців доступ до системи мають оператори критичної інфраструктури [4].

У Німеччині основні положення щодо повноважень приватного сектора у захисті КІ закріплені у Стратегії кібербезпеки від 2011 р. та Концепції основних заходів захисту критичної інфраструктури від 2006 р. Між операторами критичної інфраструктури (KRITIS), їх асоціаціями та відповідними державними установами, такими як Федеральне відомство інформаційної безпеки (BSI), у більшості секторів критичної інфраструктури запроваджено взаємодію UP KRITIS (державно-приватне партнерство). Таким чином досить вагомі завдання пов'язані з захистом КІ покладено на приватний сектор. Іншим прикладом участі приватного сектору у захисті КІ є CERT-Verbund – групи безпеки і команди реагування на комп'ютерні інциденти (CERT) сприяють обміну інформацією (наприклад, про уразливість або інциденти) та співпраці щодо усунення загроз. Співпраця з ними базується на угодах про нерозголошення інформації та на кодексі поведінки.

Для власників та керівників підприємств з числа об'єктів КІ передбачено економічне обґрунтування щодо забезпечення безпеки. В обґрунтуванні серед стимулів для операторів критичної інфраструктури зазначено: збільшення доходів; спрощення обмежень; захист сегмента ринку; ризик-менеджмент; захист технологій та товарних знаків.

У Об'єднаному Королівстві основи взаємодії державного та приватного секторів закладені Стратегією національної безпеки, Антитерористичною стратегією, (CONTEST – Counter terrorism strategy), Стратегією захисту кіберпростору (Cyber Security Strategy), а також в урядовому Плані розвитку національної інфраструктури.

Скоординованим діям суб'єктів захисту КІ активно сприяє Національний центр кібербезпеки (NCSC) як організація Великобританії, яка надає консультативну допомогу і підтримку державному і приватному секторам з питань протидії загрозам комп'ютерної безпеки. В центр включені експерти в галузі безпеки команди з реагування на комп'ютерні надзвичайні ситуації CERT-UK та MI-5, що діють з метою покращення кіберзахисту об'єктів КІ, мереж державного та приватного секторів, надання консультацій операторам та громадянам для функціонування і ведення бізнесу з використанням інформаційних мереж та Інтернету [5].

В Іспанії при Національному центрі розвідки (CNI) діють орган сертифікації безпеки інформаційних систем та національна комп'ютерна команда криптологічного центру реагування на комп'ютерні інциденти (CCN-CERT) [6]. Центр реагування на комп'ютерні інциденти (INCE) займається аналізом ризиків та загроз у кіберпросторі, їх прогнозом та організацією протидії.

Загалом, виникнення структури CERT тісно пов'язано з боротьбою проти комп'ютерних вірусів – так званих "мережевих черв'яків". Для протидії першому виявленому комп'ютерному вірусу у 1988 році на замовлення уряду США в університеті Карнегі-Меллон була сформована "комп'ютерна команда екстреної готовності – computer emergency response team", або "CERT". Після цього створення подібних організацій розпочалось в усьому світі [7]. На відміну від США, на території Європейського союзу більшість груп CERT створювалися університетами і великими IT-компаніями. Загальноєвропейська організація носить назву "TF-CSIRT" (англ. Task force – collaboration security incident response teams).

Досить активно співпраця в рамках державно-приватного партнерства розвивається і у сфері захисту критичної інфраструктури від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха тощо). Саме для цієї сфери характерною є можливість зростання негативних наслідків від порушення цілісності КІ у геометричній прогресії ("каскадні ефекти").

Тому у деяких країнах, наприклад у Данії, одним з основних координаторів роботи у сфері захисту критичної інфраструктури є Агентство з управління надзвичайними ситуаціями (DEMA). Саме цей орган і очолює контактну групу із захисту критичної інфраструктури, в межах якої організовано міжгалузеву співпрацю, включаючи приватний

сектор. Законодавчою основою організації партнерства в Данії є Акт керування діями (Інструкція) у випадку надзвичайної ситуації (англ., the Emergency Management Act). Він визначається як план функціонування суспільства за незвичайних умов. Його основною метою є забезпечення впорядкованого та скоординованого використання ресурсів громадянського суспільства.

Захист від кіберзагроз та загроз від надзвичайних ситуацій також передбачає і захист від загроз у сфері державної безпеки.

Девізом Федерального відомства Німеччини з охорони Конституції (BfV) у сфері захисту економіки є "запобігання загрозам через діалог та обмін інформацією" [8]. Хоча захист КІ та нових розробок є обов'язком операторів, однак BfV надає рекомендації щодо захисту. Вони в першу чергу включають протидію розвіддіяльності, організованої спецслужбами іноземних держав, протидію іншим загрозам у цій сфері.

Обмін інформацією між BfV та бізнесом розпочато з 2008 року, цим займається підрозділ із захисту економіки (нім., Arbeitsgemeinschaft für Sicherheit der Wirtschaft). Крім того, у Німеччині діє цікавий механізм залучення до співпраці зі спецслужбою, і цей процес активно заохочує держава. Так, особам, які сприяють діяльності BfV, надається право платити знижену на 10 відсотків податкову ставку за своїми доходами.

Поряд з UP KRITIS в Німеччині існує спільна інтернет-платформа BSI та BBK (Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих) щодо захисту критичної інфраструктури [9].

У США, згідно з положеннями національного плану (англ., National Infrastructure Protection Plan, NIPP) в частині «Партнерство для забезпечення безпеки та стійкості критично важливої інфраструктури» передбачено необхідність учасників-партнерів колективно визначати національні пріоритети та формулювати чіткі заходи задля пом'якшення ризиків, прогнозувати та аналізувати прогрес і вигоду та відслідковувати зворотній зв'язок [10]. У свою чергу, національний план є формою організації національних зусиль, він сприяє прогресу на основі залучення широкого кола учасників-партнерів з різних рівнів урядової гілки влади, приватних та некомерційних секторів, у тому числі й громадянського суспільства, до розуміння важливості забезпечення безпеки і стійкості критично важливої інфраструктури [11]. Крім того, він слугує консолідуючим фактором, оскільки використовує спільні структури та механізми, що полегшують обмін інформацією та вирішення спільних проблем.

В Україні одним з основних нормативно-правових актів, яким унормовано правові та організаційні засади взаємодії приватного сектору з партнерами є Закон України "Про державно-приватне партнерство України" (від 01.07.2010 № 2404-VI, далі – Закон). Законом сформовано поняття та ознаки державно-приватного партнерства, закріплено його основні принципи та форми, визначено основні сфери застосування державно-приватного партнерства та особливості договірно-правових відносин. Відповідно до статті 1 вказаного Закону державно-приватне партнерство – це співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів 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, та відповідає ознакам державно-приватного партнерства, визначеним цим Законом.

Закон України не встановлює вичерпного переліку форм державно-приватного партнерства, а лише визначає, що основною формою ДПП є цивільно-правовий договір, зокрема про концесію; управління майном (виключно за умови передбачення у договорі, укладеному в рамках державно-приватного партнерства, інвестиційних зобов'язань приватного партнера); спільну діяльність та інші договори.

Водночас деякі повноваження приватного сектора у сфері захисту КІ регулюються законами України "Про концесії" та "Про угоди про розподіл продукції", а також окремими підзаконними актами, серед яких слід згадати Постанову Кабінету Міністрів України "Про затвердження Порядку надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства" [12-14].

Ще одним нормативно-правовим актом, що встановлює повноваження приватного сектору, є постанова Кабінету Міністрів України "Деякі питання організації здійснення державно-приватного партнерства", якою затверджено Порядок проведення конкурсу з

визначення приватного партнера для спільної взаємодії з державним механізмом [15].

Незважаючи на широке закріплення повноважень приватного сектору у сфері захисту КІ, стримуючим фактором у його розвитку як повноправного гравця залишається складність, багаторівневість і забюрократизованість нормативно-правової бази регулювання [16].

Водночас варто зазначити, що в Україні розпочалось створення низки документів стратегічного та доктринального характеру, що безпосередньо стосуються захисту критичної інфраструктури. У цих документах приділено увагу приватному сектору та партнерству у сфері захисту критичної інфраструктури. Серед основних з них доцільно згадати Стратегію національної безпеки України, де акцентовано увагу на налагодженню співробітництва між різними суб'єктами захисту критичної інфраструктури та значна роль приділяється приватному сектору [17]. У Стратегії кібербезпеки України передбачено розширення співпраці з громадянським суспільством, а також удосконалення співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, в тому числі і з приватним сектором, який розглядається як самостійний суб'єкт захисту КІ. Зокрема, наголошується на необхідності створення умов "для залучення 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 інфраструктури, до забезпечення кібербезпеки України" [18]. У іншому доктринальному документі - Концепції створення державної системи захисту критичної інфраструктури взагалі роль приватного сектору виноситься на надзвичайно високий рівень. Він вважається одним із основоположних елементів організації діяльності у сфері захисту критичної інфраструктури.

Враховуючи викладене, як **висновки** можемо констатувати, що приватний сектор є досить важливим суб'єктом захисту критичної інфраструктури та поряд з державними органами є незамінним гравцем у системі захисту критичної інфраструктури України.

Приватний сектор володіє інформацією щодо актуальних ризиків та загроз функціонуванню об'єктів критичної інфраструктури, що при налагодженому процесі обміну дозволить значно підвищити ефективність діяльності державних органів із захисту цих об'єктів. Повноваження приватного сектору доцільно передбачити окрім основних нормативно-правових актів у сфері, також в рамках національного плану захисту критичної інфраструктури, де мають бути зазначені спільні державно-приватні інтереси у забезпеченні безпеки та стійкості критичної інфраструктури. Серед взаємовигідних аспектів доцільно виділити наступні:

– держава може різними механізмами підтримки (інвестиції, асигнування, дотації, зниження податкового навантаження тощо) сприяти функціонуванню важливих об'єктів інфраструктури, від їх важливості та участі у захисті критичної інфраструктури залежатиме обсяг державної допомоги;

– державні органи можуть надавати доступ до наявної своєчасної, достовірної та найбільш повної інформації про загрози та ризики;

– державні органи можуть надавати дані операторам критичної інфраструктури щодо різних варіацій загроз та ризиків та тенденцій розвитку ситуації у певному сегменті внутрішнього чи зовнішнього ринку;

– державні органи можуть надавати детальну інформацію щодо ризиків, чим забезпечують свій вклад у захист об'єктів КІ, що позначиться на інвестиціях в безпеку та стійкість з боку операторів;

– оператори критичної інфраструктури можуть отримувати достовірну інформацію про наявні та потенційні загрози і ризики для вжиття відповідних заходів з підвищення безпеки та стійкості, а також розраховувати на необхідні заходи підтримки відповідних органів та місцевої чи державної влади;

– оператори критичної інфраструктури можуть отримувати достовірну інформацію, важливу для вжиття заходів з покращення інвестиційної діяльності;

– оператори критичної інфраструктури можуть впливати на дієвість та ефективність планів державних органів із забезпечення безпеки та стійкості в їх сферах діяльності;

– оператори критичної інфраструктури, які займаються господарською діяльністю, за умов тісної взаємодії з державними органами у сфері захисту критичної інфраструктури можуть якісно організувати роботу та підвищити прибуток. У свою чергу, збільшення їх прибутку є прямо пропорційним вигоді держави зі сплати ними податку з прибутку.

Бібліографічні посилання

1. Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав. *Актуальні проблеми вдосконалення чинного законодавства України.* Івано-Франківськ, 2017. № XLIV. С. 224-235.
2. Єрменчук О.П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. *Науковий вісник ДДУВС.* 2017. № 3. С. 135-140.
3. Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (CD 2008/114/EC).
4. Марек Сметана. Защита критической инфраструктуры. Подходы государств Европейского Союза к определению элементов критической инфраструктуры. Острава: ВШБ – Технический университет Острава, 2014/2015. 60 с. (текст для курсов, подготавливаемых в рамках сотрудничества Чешская Республика – Молдавия).
5. https://www.ncsc.gov.uk/information/about-ncsc.
6. https://es.wikipedia.org/wiki/Centro_Nacional_de_Inteligencia.
7. https://www.incibe.es/que-es-incibe/como-trabajamos.
8. https://www.verfassungsschutz.de.
9. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. Bundesministerium des Innern, 2006. URL: www.bmi.bund.de.
10. NIPP 2013 Partnering for Critical Infrastructure. Security and Resilience. URL: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.
11. Єрменчук О. П. Інформаційно-комунікаційна складова державно-приватного партнерства у захисті критичної інфраструктури як важливий елемент забезпечення державної безпеки. *Актуальні проблеми управління інформаційною безпекою держави:* IX Всеукраїнська науково-практична конференція (Київ, 30 березня 2018 р.). Київ, 2018. С. 68–70.
12. Про концесії: Закон України від 16.07.1999 № 997-XIV // ВВР України. 1999. № 41. Ст. 372.
13. Про угоди про розподіл продукції: Закон України від 14.09.1999 р. № 1039-XIV // ВВР України. 1999. № 44. Ст. 391.
14. Про затвердження Порядку надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства: постанова Кабінету Міністрів України від 09.02.2011 № 81. *Офіційний вісник України*. 2011. № 10. Ст. 458.
15. Про деякі питання організації здійснення державно-приватного партнерства: постанова Кабінету Міністрів України від 11.04.2011 № 384. *Офіційний вісник України.* 2011. № 28. Ст. 1168.
16. Щодо розвитку державно-приватного партнерства як механізму активізації інвестиційної діяльності в Україні: аналітична записка. URL: http://www.niss.gov.ua/articles/816.
17. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. "Про Стратегію національної безпеки України": Указ Президента України від 26 травня 2015 р. № 287/2015.
18. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року № 96/2016. *Офіційний вісник України.* 2016. 29 березня. Ст. 899.

Надійшла до редакції 22.02.2019

SUMMARY

Yermenchuk O.P. Private sector as an important subject of critical infrastructure protection. The article deals with study of the legal principles of the functioning of the private sector and analysis of its interaction with the state in the field of critical infrastructure protection on the example of different world powers. The results of the proposed form of interaction, the necessary powers and projected possible benefits from joint activities of the private sector as a subject of protection of critical infrastructure. In Ukraine, the launch of a series of documents of strategic and doctrinal nature, which directly concern the protection of critical infrastructure. Among them are: Cybersecurity Strategy of Ukraine and the Concept for the creation of a state system for the protection of critical information structures. These documents focus on the private sector and partnerships in critical infrastructure protection.

The private sector is a very important subject of critical infrastructure protection and, along with state bodies, is an indispensable player in the critical infrastructure protection system in Ukraine. The private sector has information on the actual risks and threats to the functioning of critical infrastructure objects, which, with a well-established exchange process, will significantly increase the efficiency of state bodies' activities in protecting these objects. It is expedient to envisage the powers of the private sector in addition to the basic normative acts in the area, as well as within the framework of the national plan for the protection of critical infrastructure, which should indicate common public-private interests in ensuring the security and stability of critical infrastructure.

Keywords*: private sector, partnership, legal regulation, protection, critical infrastructure.*