УДК 346
DOI https://doi.org/10.32782/pyuv.v4.2023.6

І. С. Студенець
orcid.org/0000-0002-8812-3341
аспірантка кафедри економічного права та економічного судочинства
Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка

КОНЦЕСІЯ У СФЕРІ КІБЕРБЕЗПЕКИ

Постановка проблеми. Безумовно актуальним є питання ефективної взаємодії між бізнесом та державою для відновлення економіки України під час воєнного стану та під час післявоєнного відновлення. Концесія як модель державно-приватного партнерства (далі – «ДПП») є потужним інструментом для залучення інвестицій та досвіду приватного сектора. Під час стрімкого розвитку діджиталізації першочергове значення набуває кібербезпека та питання застосовності концесії як моделі ДПП в цій сфері.

Аналіз останніх досліджень і публікацій. Правовим питанням концесій в Україні присвячено ряд наукових доробків (в тому числі у складі праць, що стосуються ДПП). Прикладами актуальних дисертаційних досліджень є роботи Л.М. Гончарука (договір концесії) [1] та О.І. Вікарчук (концесія як засіб залучення довгострокових інвестицій) [2]. До нещодавніх досліджень відносяться напрацювання І.П. Лопушинського, В.М. Ємельянова (концесія в портовій галузі України) [3], С.Б. Єгоричевої, М.І. Лахижи (становлення та сучасний стан ДПП та концесій) [4] та інші.

Однак, відсутні дослідження правового регулювання та функціонування концесій у сфері забезпечення національної безпеки і кібербезпеки зокрема. Водночас, такі праці наявні в більш широкому полі – ДПП. Актуальні наукові дослідження у цій сфері представили В.О. Бойко [5], Ю.В. Заскока [6], В.В. Круглов [7], Р.Ю. Прав [8], підготовано аналітичні доповіді [9]). Міжнародні науковці та практики також не використовують концесію як модель здійснення ДПП у сфері кібербезпеки.

Метою статті є визначення особливостей правового регулювання концесії для забезпечення кібербезпеки як складової національної безпеки. До завдань віднесено: розглянути стратегічне регулювання ДПП у сфері забезпечення національної безпеки та правового регулювання ДПП у сфері кібербезпеки; проаналізувати законодавство щодо концесій у сфері кібербезпеки та надати рекомендації для розвитку концесійної моделі ДПП у сфері кібербезпеки.

Виклад основного матеріалу. *ДПП у сфері забезпечення національної безпеки.* ДПП в галузі національної безпеки (зокрема, пов'язане з воєнним станом, надзвичайною ситуацією, кібербезпекою) передбачає передачу найбільш монополізованих повноважень держави приватному партнеру. Більшість програмних довгострокових документів в сфері національної безпеки згадує застосування ДПП без деталізації його моделей, в тому числі концесії (див. Таблицю 1).

ДПП у сфері кібербезпеки. Кібербезпека є складовою національної безпеки України та може стати зразком для законодавчого та практичного розвитку ДПП і концесій в інших сферах національної безпеки. Критична потреба в розвитку ДПП в кібербезпеці зумовлена низкою причин, серед яких: приватизація деяких секторів критичної інфраструктури; велика кількість електронних інформаційних ресурсів; залежність інфраструктури від інформаційно-телекомунікаційних систем; зростаюча конвергенція комп'ютерних мереж [16]; розвиток діджиталізації тощо.

Проект Плану відновлення України передбачає розвиток потенціалу національної екосистеми кібербезпеки, включаючи посилення ДПП в напрямку кібер та інформаційної безпеки (проект зміцнення кібербезпеки малих і середніх компаній, підвищення стійкості і підтримки цифровізації бізнес-сектора) [17, ст. 63]. Крім того, заплановано розроблення законопроекту, спрямованого на врегулювання питань ДПП у сфері кібербезпеки Кабінетом Міністрів у першому півріччі 2023 року [13], текст якого наразі відсутній у публічних джерелах.

Реалізація кібербезпеки шляхом використання ДПП передбачає напрацювання відносин, пов'язаних із розкриттям конфіденційної, комерційної та персональної інформації, досягнення співвідношення інтересів партнерів, розроблення контрольних та наглядових процедур. Завдання, які повинні вирішити ДПП у сфері кібербезпеки: забезпечити надійний доступ до інтернет-мережі; регулювати технічну безпеку та оброблення даних; проводити обмін інформацією щодо кіберзагроз; здійснювати допомогу щодо вирішення ситуацій, пов'язаних із кіберзагрозами або незаконним контентом в Інтернет-мережі [10, ст. 220-221]. Напрямки можливої реалізації ДПП в кібербезпеці висвітлено нижче в Таблиці 2, проте на практиці такі партнерства відсутні.

Таблиця 1

ДПП у стратегіях національної безпеки. Розроблено автором.

Стратегії	*Положення про ДПП*
Національної безпеки [11]	*Держава створить ефективну систему безпеки та стійкості критичної інфраструктури, засновану на (…) ДПП. Модернізація транспортної інфраструктури (…), у тому числі через механізми ДПП. Оборонно-промисловий комплекс (…) реалізуватиме потенціал ДПП.*
Забезпечення державної безпеки [12]	*Розвиток ДПП з урахуванням пріоритетності інтересів держави в системі забезпечення державної безпеки.*
Кібербезпеки [13]	*Врегулювання на законодавчому рівні питання ДПП у сфері кібербезпеки, визначивши форми і методи здійснення такого партнерства, зміцнивши взаємну довіру та передбачивши можливість запровадження експериментальних проектів у цій сфері.*
Воєнної безпеки [14]	*Використання можливостей ДПП (…) для вітчизняного і спільного з партнерами розроблення, виробництва й оснащення сил оборони сучасним озброєнням, військовою та спеціальною технікою, забезпечення засобами ураження, у тому числі безпілотними і роботизованими, вкладення довгострокових інвестицій у розвиток військової інфраструктури.*
Розвитку оборонно-промислового комплексу [15]	*Впровадження механізмів ДПП в оборонно-промисловому комплексі з метою спільного розроблення та реалізації інвестиційних та інноваційних проектів, налагодження трансферу технологій, залучення компетенцій, кадрів, інновацій, технологій, капіталу і досвіду управління приватних підприємств і організацій для спільного вирішення задач забезпечення національної безпеки.*

Таблиця 2

Основні законодавчо визначені напрямки застосування ДПП у сфері кібербезпеки. Розроблено автором.

Закон України «Про основні засади забезпечення кібербезпеки України»	*ЗУ «Про критичну інфраструктуру»*
– партнерство та координація команд реагування на комп'ютерні надзвичайні події; *– надання консультативної та практичної допомоги з питань реагування на кібератаки;* *– формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;* *– тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, IT-компаніями з метою виконання заходів кіберборони в кіберпросторі.*	*– забезпечення резервування основних ресурсів для функціонування критичної інфраструктури у різних режимах;* *– організації системи оповіщення населення та суб'єктів господарювання про інциденти та кризові ситуації на об'єктах критичної інфраструктури;* *– створення механізмів для саморегулювання, обміну інформацією між операторами об'єктів критичної інфраструктури у певному секторі;* *– створення та підтримка розвитку систем сертифікації та оцінки відповідності.*
ДПП здійснюється з урахуванням установлених законодавством особливостей правового режиму щодо окремих об'єктів та окремих видів діяльності.	

Міжнародна практика демонструє досить схожі напрямки взаємодії. Наприклад, ключові елементи Національної стратегії кібербезпеки Німеччини в частині ДПП включають: захист критичної інфраструктури та IT-систем; зміцнення інформаційної безпеки державного управління шляхом прийняття єдиної «федеральної мережі»; розвиток інновації в IT індустрії тощо [5].

Концесія у сфері кібербезпеки. Концесія – це договірна модель ДПП, сторонами якої є публічна сторона, концесієдавець, та приватна сторона, концесіонер, та яка передбачає строкове платне створення/удосконалення об'єкту концесії та (або) управління ним з розподілом ризиків між сторонами концесійного договору. Концесія в сфері кібербезпеки не набула свого поширення ні в законодавстві, ні на практиці як в Україні, так і в інших країнах.

Потенційним ключовим напрямом для застосування концесії в кібербезпеці є технічний захист інформації (діяльність, спрямована на забезпечення інженерно-технічними засобами конфіденційності, цілісності та доступності інформації) на об'єктах критичної інфраструктури. Прикладами можуть слугувати: проектування та будівництво приміщень, захищених від технічних витоків інформації; забезпечення інформаційних систем джерелами резервного живлення, в тому числі шляхом створення резервних трансформаторних

підстанцій та/або ліній електропередач; створення та використання інформаційно-аналітичних систем підтримки та ухвалення управлінських рішень тощо. Враховуючи «чутливість» даної сфери, вважаємо за доцільне врегулювати особливості концесії та ДПП в сфері кібербезпеки на рівні окремих положень у відповідних законах.

Крім того, розвиток ДПП та концесій у сфері кібербезпеки дозволить здійснити поштовх до розвитку пов'язаних сфер, і в першу чергу кіберстрахування – виду страхування, що захищає від ризиків інформаційних технологій, IT-інфраструктури та діяльності у кіберпросторі та характеризується двома підходами щодо покриття кіберстрахування (страхування кібервідповідальності чи майнове страхування), а також відсутністю правового регулювання (питання ліцензування, спеціального органу тощо).

Висновки і пропозиції. Доцільність застосування державно-приватного партнерства у сфері кібербезпеки передбачено на рівні програмних довгострокових документів, а шляхи застосовування – на законодавчому рівні. Концесія як модель ДПП у сфері кібербезпеки не виокремлюється ні науковцями, ні законотворцями як в Україні, так і на міжнародній арені. Потенційним ключовим напрямом для застосування концесії в кібербезпеці є технічний захист інформації на об'єктах критичної інфраструктури. Вбачаємо за доцільне законодавчо врегулювати можливість запровадження концесій в сфері кібербезпеки, а саме: нові положення у законах про ДПП та про концесію, а також доповнення статей про шляхи запровадження ДПП у закон про критичну інфраструктуру та кібербезпеку (через затвердження невиключного переліку напрямків ДПП або поіменовану концесію) з метою ефективної реалізації ДПП для технічного захисту інформації. Пропонується в подальших дослідженнях систематизувати приклади міжнародного досвіду щодо концесій або інших форм ДПП у кібербезпеці та на основі аналізу виділити можливі бар'єри для України та шляхи їх подолання.

Література

1. Гончарук Л.М. Договір концесії : автореф. дис. … канд. юрид. наук : 12.00.03. Київ, 2012. 21 с. URL: https://mydisser.com/en/catalog/view/6/44/9286.html.
2. Вікарчук О.І. Концесія у трансформаційній економіці : дис. … канд. екон. наук : 08.01.01. Київ, 2006. 194 с.
3. Лопушинський І.П., Ємельянов В.М. Концесія в портовій галузі України як форма державно-приватного партнерства. Public Administration and Regional Development. 2021. № 11. С. 232-250. URL: https://pard.mk.ua/index.php/journal/article/download/241/200.
4. Єгоричева С.Б., Лахижа М.І. Публічно-приватне партнерство в посткомуністичних країнах : монографія. Київ: ІПК ДСЗУ, 2020. 304 с.
5. Бойко В.О. Державно-приватне партнерство у сфері кібербезпеки: кейс Німеччини. НІСД. URL: https://niss.gov.ua/sites/default/files/2018-01/Germany-7f497.pdf.
6. Заскока Ю.В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. Наукові перспективи. 2021. № 9(15). С. 85–98. DOI: https://doi.org/10.52058/2708-7530-2021-9(15)-85-98.
7. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління. 2018. С. 57–61. URL: https://www.researchgate.net/profile/Vitalij-Kruglov/publication/327791991_Derzavno-privatne_partnerstvo_u_sferi_kiberbezpeki/links/5ba4b29692851ca9ed1a7c4c/Derzavno-privatne-partnerstvo-u-sferi-kiberbezpeki.pdf.
8. Прав Р.Ю. Роль механізму державно-приватного партнерства у розвитку кібербезпеки України на сучасному етапі. Інвестиції: практика та досвід. 2019. №21. С. 143–150.
9. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. / за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с. Маркєєва О.Д., Розвадовський Б.Л. Держава та приватний сектор на захисті національної безпеки: від взаємодії до партнерства : аналіт. доп. Київ: НІСД, 2021. 70 с. URL: https://doi.org/10.53679/niss-analytrep.2021.23.
10. Круглов В.В. Механізми державного регулювання розвитку державно-приватного партнерства в Україні : дис. … д-ра наук з держ. упр. : 25.00.02. Харків, 2020. 479 с. URL: https://ipa.karazin.ua/wp-content/themes/kbuapa/filesforpages/science/kvv_dis_20202606.pdf.
11. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України" : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.
12. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки" : Указ Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text.
13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
14. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України" : Указ Президента України від 25.03.2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text.
15. Про рішення Ради національної безпеки і оборони України від 18 червня 2021 року «Про Стратегію розвитку оборонно-промислового комплексу України» : Указ Президента України від 20.08.2021 р. № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text.
16. Марушак А., Панченко В. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. Інформаційна безпека, людина суспільство держава. 2014. № 3(16). С. 56–63.

17. Проект Плану відновлення України : Матеріали робочої групи «Діджиталізація». Національна рада з відновлення України від наслідків війни. 2022. 119 с. URL: https://www.kmu.gov.ua/storage/app/sites/1/recoveryrada/ua/digitization.pdf.

Анотація

Студенець І. С. **Концесія у сфері кібербезпеки.** – Стаття.

У статті представлено аналіз концесійної моделі у сфері кібербезпеки в Україні, що є однією зі складових національної безпеки. На сьогодні відомі дослідження, присвячені правовим питанням концесії в Україні, та дослідження, присвячені державно-приватному партнерству в кібербезпеці, проте в жодному з них не розглядається правове регулювання та функціонування концесії як моделі здійснення державно-приватного партнерства у сфері забезпечення кібербезпеки. Мета цієї статті – визначення особливостей правового регулювання концесії для забезпечення кібербезпеки в Україні.

Автором розглянуто програмне довгострокове регулювання державно-приватного партнерства у сфері забезпечення національної безпеки та визначено направленість правового регулювання державно-приватного партнерства у сфері кібербезпеки. Зазначено, що концесія як модель державно-приватного партнерства у сфері кібербезпеки не виокремлюється ні на рівні законодавства, ні у наукових працях в Україні та в інших країнах. Водночас саме кібербезпека може стати зразком для законодавчого та практичного розвитку державно-приватного партнерства і концесій в інших сферах національної безпеки.

У статті проаналізовано необхідність застосування концесій у сфері кібербезпеки та застосовне правове регулювання. Потенційним ключовим напрямом для застосування концесії в кібербезпеці можу бути технічний захист інформації на об'єктах критичної інфраструктури.

Запропоновано законодавчо врегулювати можливість запровадження концесій в сфері кібербезпеки через введення нових положень у законах про державно-приватне партнерство та про концесію, а також доповнення статей про шляхи запровадження державно-приватного партнерства у законах про критичну інфраструктуру та основні засади забезпечення кібербезпеки України (шляхом визначення концесії або невиключного переліку).

Для подальших досліджень пропонується провести аналіз міжнародного досвіду державно-приватного партнерства у сфері кібербезпеки у ряді країн та огляд бар'єрів і шляхів їх подолання для функціонування концесій у кібербезпеці.

Ключові слова: господарська діяльність, національна безпека, відновлення економіки, діджиталізація, кіберстрахування.

Summary

Studenets I. S. **Concession in Cybersecurity.** – Article.

The article provides the analysis of the concession model in the field of cyber security in Ukraine, which is one of the components of national security. Currently, there are known studies devoted to the legal issues of the concession in Ukraine, and studies devoted to public-private partnership in cyber security. However, none of them consider the legal regulation and operation of the concession as a model for the implementation of public-private partnership in the field of cyber security. The purpose of this article is to determine the specifics of the legal regulation of the concession to ensure cyber security in Ukraine.

The author considered the programmatic long-term policies of public-private partnership in the field of ensuring national security and determined the direction of legal regulation of public-private partnership in the cyber security. It is noted that the concession as a model of public-private partnership in the cyber security is not singled out either at the level of legislation or in research studies in Ukraine and other countries. At the same time, cyber security may become a model for the legislative and practical development of public-private partnerships and concessions in other areas of national security.

The article analyzes the necessity of applying concessions in the cyber security and the applicable legal regulation. A potential key direction for the application of the concession in cyber security may be the technical protection of information at critical infrastructure facilities.

It is proposed to legislatively regulate the possibility of introducing concessions in the cyber security sphere through the introduction of new provisions in the laws on public-private partnership and on concession, as well as the addition of provisions on the methods of usage of public-private partnership in the laws on critical infrastructure and on the basic principles of ensuring cyber security of Ukraine (by defining the concession or providing a non-exclusive list of PPP usage).

For further research, it is proposed to conduct an analysis of the international experience of public-private partnerships in the cyber security in certain countries and a overview of barriers and mitigation ways for the functioning of concessions in cyber security.

Key words: economic (business) activity, national security, economic recovery, digitalization, cyber insurance.