

УДК 35-027.21:351.86](477)

Р. В. Студзінський,  
Військовослужбовець Збройних Сил України  
ORCID ID: <https://orcid.org/0009-0002-2989-1321>

DOI: 10.32702/2306-6814.2025.22.355

# РОЛЬ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ В УКРАЇНІ

R. Studzinskiy,  
Serviceman of the Armed Forces of Ukraine

THE ROLE OF PUBLIC-PRIVATE PARTNERSHIPS IN ENSURING CYBERSECURITY IN UKRAINE

Повномасштабне вторгнення російської федерації на територію нашої держави зробила кіберпростір справжньою платформою бойових дій. Потужність та масштаби кібератак суттєво збільшились, орієнтуючись не тільки на публічні органи влади, але й на об'єкти критичної інфраструктури, більшість якої належить бізнес сектору. В умовах воєнного стану, коли країна мобілізує весь свій потенціал, державно-приватне партнерство відіграє критично важливу роль для консолідації зусиль і підвищення національної стійкості. В цілому варто зауважити, що дослідження ролі державно-приватного партнерства у забезпеченні кібербезпеки в Україні є надзвичайно актуальним, адже дозволяє виявити проблеми, розкрити перспективи та опрацювати ефективні механізми співробітництва для посилення національної кіберстійкості в умовах воєнних дій, євроінтеграції та незмінних гібридних загроз.

В статті визначено, що сутність державно-приватного партнерства у сфері забезпечення кібербезпеки в Україні полягає в акумуляції ресурсів, практики, технологій та можливостей державного та приватного секторів з метою ефективної протидії кіберзагрозам. Дана співпраця вважається визначальним інструментом в процесі підвищення національної кібернетичної стійкості, особливо в умовах повномасштабного вторгнення російської федерації на територію нашої держави, коли кількість та складність кібератак суттєво зросли. Встановлено, що роль державно-приватного партнерства у забезпеченні кібербезпеки в Україні криється у захисті критичної інфраструктури, забезпеченні доступу до інновацій та технологій, обміні інформаційними та розвідувальними даними, оперативному реагуванні на кіберінциденти, забезпеченні розвитку кадрового потенціалу, а також у гармонізації законодавчої бази.

The full-scale invasion of the Russian Federation into the territory of our state has made cyberspace a real platform for combat operations. The power and scale of cyberattacks have increased significantly, targeting not only public authorities, but also critical infrastructure facilities, most of which belong to the business sector. In conditions of martial law, when the country mobilizes all its potential, public-private partnership plays a critically important role in consolidating efforts and increasing national resilience. In general, it is worth noting that the study of the role of public-private partnership in ensuring cybersecurity in Ukraine is extremely relevant, as it allows identifying problems, revealing prospects and developing effective cooperation mechanisms to strengthen national cyber resilience in conditions of military operations, European integration and constant hybrid threats.

The article determines that the essence of public-private partnership in the field of cybersecurity in Ukraine is the accumulation of resources, practices, technologies and capabilities of the public and private sectors in order to effectively counter cyber threats. This cooperation is considered a key tool in the process of increasing national cyber resilience, especially in the context of the full-scale invasion of the Russian Federation into the territory of our state, when the number and complexity of cyber attacks have increased significantly. It is established that the role of public-private partnership in ensuring cybersecurity in Ukraine lies in protecting critical infrastructure, ensuring access to innovations and technologies, exchanging information and intelligence data, responding promptly to cyber incidents, ensuring the development of human resources, as well as in harmonizing the legislative framework. It is noted that despite significant efforts and ad hoc cooperation, the PPP mechanism in this area still faces serious challenges related to legislative gaps, lack of consistency,

*problems with information exchange and insufficient trust between state institutions and business. The further development of public-private partnership requires solving the above problems, implementing progressive foreign experience and creating clear, institutionalized cooperation mechanisms.*

*Ключові слова: публічне управління, кібербезпека, забезпечення кібербезпеки, держава, бізнес, державно-приватне партнерство.*

*Key words: public administration, cybersecurity, cybersecurity, state, business, public-private partnership.*

### ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

В сучасних умовах російсько-української війни, дослідження питання забезпечення кібербезпеки в Україні набуло виняткової актуальності. На сьогоднішній день кібербезпека перестала бути суто державним завданням, обернувшись на складний, багатогранний виклик, що потребує консолідації зусиль та ресурсів не лише держави, але й бізнес сектору. Державно-приватне партнерство (ДПП) у сфері забезпечення кібербезпеки визнається у будь-якій країні як ефективний механізм в процесі формування стійкої національної системи захисту при безперервно зростаючих кіберзагрозах. В нашій державі, всупереч визнанню стратегічної важливості ДПП, наприклад в Стратегії кібербезпеки України, мають місце також і вагомі виклики для його повноцінного впровадження. Недостатній рівень інституціоналізації, прогалини у нормативно-правовому забезпеченні та проблеми з координацією між суб'єктами негативно позначаються на використанні системного підходу в процесі дослідження даної проблематики. Це все визначає актуальність дослідження ролі та механізмів державно-приватного партнерства у забезпеченні кібербезпеки в Україні.

### АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дану проблематику досліджували такі науковці як В. Григоренко, Ю. Дзюрах, Д. Дубова, В. Круглов, Г. Малахов, Т. Панасюк, С. Петренко, Р. Прав, І. Стеців, Б. Чепіль та інші. Науковці наголошують, що ДПП виступає головним елементом для посилення національної кіберстійкості. Однак, аналіз вказує, що, всупереч позитивним зрушенням, ДПП у забезпеченні кібербезпеки в Україні все ще знаходиться на етапі становлення та наражається на низку проблем, що обумовлює потребу у додаткових дослідженнях.

### ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою даної статті є визначення ролі державно-приватного партнерства у забезпеченні кібербезпеки в Україні.

### ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Дослідження розвитку усіх аспектів сучасної суспільної життєдіяльності демонструє, що жодні органи державної влади не можуть самостійно реагувати та ефек-

тивно протистояти загрозам національній безпеці. Через це будь-яка держава докладає чимало зусиль для ведення гнучкої та багатовекторної політики задля пошуку додаткових безпекових можливостей. Важливим напрямом, який дозволяє посилити можливості країни та ефективно протистояти загрозам національній безпеці, вважається використання державно-приватного партнерства.

Зарубіжна практика обґрунтовано засвідчує, що "без комплексної взаємодії держави та приватного сектору неможливо побудувати ефективний та надійний кіберзахист. Державно-приватне партнерство передбачає таку форму співпраці, за якої досягаються цілі та завдання, що сприятимуть забезпеченню національної безпеки, економічного розвитку та побудові безпечного кіберсередовища для усіх громадян" [1]. Тобто під моделлю державно-приватного партнерства можна розуміти динамічні співпрацю між державними інституціями та бізнес сектором, які колективно виконують функції задля забезпечення безпеки у кібернетичному просторі.

На даний час державно-приватне партнерство "визнається як державами, так і недержавними суб'єктами ключовим елементом побудови дійсно ефективної системи кібербезпеки держави. Майже кожна стратегія кібербезпеки (національного чи наднаціонального рівня) або ж відомчий візійний документ (який стосується кібербезпеки) містить згадки про бажання розвивати ДПП" [2]. Варто зазначити, що "активізація ДПП у сфері національної безпеки відбулася з початком гібридної війни РФ проти України, коли населення країни об'єдналося з метою допомоги силам оборони протидіяти загрозі. Причому ініціатором партнерства виступив саме приватний сектор, продуктивна діяльність якого (благодійних організацій, волонтерських, громадських об'єднань, окремих юридичних осіб) сприяла підвищенню зацікавленості держави в партнерстві" [3]. Тому ДПП є "одним із ключових інструментів розвитку критичної інфраструктури та забезпечення стратегічних державних потреб, спрямоване на мобілізацію приватних інвестицій, підвищення ефективності управління державними ресурсами та сприяння інноваційному розвитку. Водночас, у сфері національної безпеки та продовольчої зокрема, застосування механізмів ДПП супроводжується низкою ризиків, пов'язаних із прозорістю, підзвітністю та контролем за використанням державних ресурсів" [4].

Отже, на нашу думку, сутність ДПП у сфері забезпечення кібербезпеки в Україні полягає в акумуляції ресурсів, практики, технологій та можливостей державного та приватного секторів з метою ефективної протидії кіберзагрозам. Дана співпраця вважається визна-

чальним інструментом в процесі підвищення національної кібернетичної стійкості, особливо в умовах повномасштабного вторгнення російської федерації на територію нашої держави, коли кількість та складність кібератак суттєво зросли.

В. В. Кругло зазначає, 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 кібербезпеки базуються на основі економічної ефективності та інноваційності; забезпеченні цілісності та доступності; приватності та свободи; відповідальності та прозорості; справедливості" [5].

На сьогоднішній день в Україні на законодавчому рівні визначені такі основні шляхи державно-приватного партнерства у сфері в кібербезпеки: "створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій; підвищення цифрової грамотності громадян та культури безпекового поведіння в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки; обмін інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів; партнерство та координація команд реагування на комп'ютерні надзвичайні події; залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки; 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; запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки; періодичне проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки; створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки; тісна взаємодія з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі" [6].

В цілому варто зауважити, що Україна може отримати певні переваги від використання ДПП, які полягають у підвищенні національної стійкості (об'єднання зусиль суттєво зміцнює здатність держави протидіяти масованим кібератакам), вільному доступі до прогресивних технологій (держава може оперативно впроваджувати новітні рішення, що безперервно оновлюються приватним сектором), забезпеченні ефективного реагування (спільна координація дає можливість оперативно виявляти та реагувати на кіберінциденти), а також зменшенні ризиків (спільний аналіз ризиків та планування реагування на надзвичайні ситуації дає можливість мінімізувати наслідки кібератак).

В сучасних умовах впровадження ДПП в Україні здійснюється повільними темпами, попри те, що влада вважає ДПП головним механізмом реалізації політики оновлення економіки та розв'язання актуальних соціально-економічних проблем. Серед ключових причин можна визначити: "слабку політичну координацію, корупцію, недоліки у нормативно-правовому регулюванні, економічну нестабільність, застарілість об'єктів інфраструктури, низький рівень інвестицій, відсутність досвіду взаємодії держави та бізнесу у сфері кібербезпеки" [7]. Водночас ДПП визнається як "ключовий елемент кібербезпекової системи держави, який вимагає максимального ресурсного забезпечення. Хоча більшість розвинених країн мають тією чи іншою мірою працюючі форми ДПП, однак майже в кожному випадку вони формуються у режимі ad-hoc і під значним впливом історичного досвіду кожної конкретної країни. Зокрема, позитивним вбачається законодавчий досвід США у площині взаємного обміну інформацією про кіберзагрози між урядом та приватним сектором. У ЄС у межах пошуку ефективних форм ДПП проводяться програми консультацій з великим, малим та середнім бізнесом, асоціаціями, дослідницькими інституціями, громадським сектором, органами державної влади та органами регіонального рівня, що може стати основою відповідного процесу, якого потребує Україна" [8].

Отже, аналіз наукових джерел засвідчує, що ДПП виступає визначальним фактором в процесі забезпечення кібербезпеки в Україні, особливо в умовах воєнного стану. Незважаючи на те, що суттєві зусилля та ситуативне співробітництво, механізм ДПП у даній сфері досі наражається на серйозні виклики, пов'язані із законодавчими прогалинами, браком системності, проблемами з обміном інформаційними даними та недостатньою довірою між державними інституціями та бізнесом. Наступний розвиток ДПП вимагає розв'язання вище наведених проблем, імплементації прогресивного зарубіжного досвіду та створення чітких, інституціоналізованих механізмів співробітництва.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Таким чином, в умовах повномасштабного вторгнення російської федерації на територію нашої держави та постійних кібератак зі сторони країни-агресора роль державно-приватного партнерства в процесі забезпечення кібербезпеки в Україні є критично важливою. Дане співробітництво виступає визначальним інструментом для об'єднання ресурсів державного та приватного секторів, що сприяє створенню стійкої та ефективної системи кіберзахисту на загальнодержавному рівні.

Визначальна роль ДПП у забезпеченні кібербезпеки в Україні криється у:

1. Захисті критичної інфраструктури. Більшість об'єктів критичної інфраструктури в нашій державі перебуває у приватній власності. ДПП дозволяє забезпечити координацію зусиль та обмін інформаційними даними між державними органами та приватними операторами з метою колективного захисту від кібератак.

2. Забезпеченні доступу до інновацій та технологій. Так, бізнес сектор має усі передові інструменти, технології та експертизи в кіберзахисті. ДПП дає можливість державі одержати доступ до цих ресурсів з метою посилення своєї кіберстійкості та протистояння новітнім загрозам.

3. Обміні інформаційними та розвідувальними даними. Ефективна взаємодія між державними інституціями та приватними компаніями набуває ключового значення для обміну інформацією щодо кіберзагроз, інцидентів та методів реагування. Це дозволяє оперативно виявляти та нейтралізувати кібератаки, а також сприяє розробці ефективніших стратегій захисту.

4. Оперативному реагуванні на кіберінциденти. ДПП сприяє створенню спільних механізмів реагування на кіберінциденти, де бізнес надає технічну підтримку та експертизу, а державні інституції координують дії та забезпечують правове регулювання.

5. Забезпеченні розвитку кадрового потенціалу. Співробітництво з бізнес сектором, освітніми установами та дослідницькими центрами дає можливість державі залучати та готувати висококваліфікованих спеціалістів у сфері кібербезпеки. Це набуває виняткової актуальності, враховуючи кадровий дефіцит у цій галузі.

6. Гармонізації законодавчої бази. ДПП дозволяє удосконалити нормативно-правову базу у сфері забезпечення кібербезпеки, враховуючи досвід приватного сектору та міжнародні стандарти. Водночас бізнес бере участь у розробці та обговоренні законодавчих ініціатив, що сприяє створенню більш збалансованого та ефективного регулювання.

Варто зазначити, що не зважаючи на всі існуючі виклики, активне залучення бізнесу є незамінним в процесі побудови ефективної, стійкої та адаптивної системи кібербезпеки нашої держави. Особливо це актуально в умовах воєнного стану, коли об'єднання зусиль є ключовим для захисту національних інтересів у кіберпросторі.

## Література:

1. Григоренко В. А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки. Інформація і право. 2021. № 2 (37). С. 155—161. DOI: [https://doi.org/10.37750/2616-6798.2021.2\(37\).238405](https://doi.org/10.37750/2616-6798.2021.2(37).238405).

2. Дубова Д. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. К.: НІСД, 2018. 84 с.

3. Панасюк Т. І., Петренко С. В. Сучасний стан державно-приватного партнерства у сфері кібербезпеки: досвід України. Інформаційна безпека людини, суспільства, держави. 2025. № 1 (38). С. 42—51. DOI: [https://doi.org/10.511369/2707-7276-2025-1\(38\)-4](https://doi.org/10.511369/2707-7276-2025-1(38)-4).

4. Стеців І. С., Стеців І. І., Дзюрах Ю. М., Чепіль Б. А. Проблеми державно-приватного партнерства в умовах цифровізації управлінських рішень у сфері національ-

ної безпеки України. Держава та регіони. 2024. № 4. С. 207—215. DOI: <https://doi.org/10.32782/1813-3401.2024.4.31>.

5. Круглов В. В. Державно-приватне партнерство у сфері кібербезпеки. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Державне управління. 2018. № 3. С. 57—61.

6. 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#top>

7. Прав Р. Ю. Роль механізму державно-приватного партнерства у розвитку кібербезпеки України на сучасному етапі. Інвестиції: практика та досвід. 2019. № 21. С. 143—150. DOI: <https://doi.org/10.32702/2306-6814.2019.21.143/>

8. Малахов Г. Б. Шляхи удосконалення державно-приватного партнерства у сфері кібербезпеки України. Інформація і право. 2023. № 4 (47). С. 197—206. DOI: [https://doi.org/10.37750/2616-6798.2023.-4\(47\).291666/](https://doi.org/10.37750/2616-6798.2023.-4(47).291666/)

## References:

1. Hryhorenko, V. A. (2021), "Best foreign practices in developing mechanisms for public-private partnership in the field of cybersecurity", *Informatsiia i pravo*, vol. 2 (37), pp. 155—161. DOI: [https://doi.org/10.37750/2616-6798.2021.2\(37\).238405](https://doi.org/10.37750/2616-6798.2021.2(37).238405).

2. Dubova, D. (2018), *Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyy dosvid ta mozhlyvosti dlia Ukrainy* [Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine], NISD, Kyiv, Ukraine.

3. Panasiuk, T. I. and Petrenko, S. V. (2025), "Current state of public-private partnership in the field of cybersecurity: experience of Ukraine", *Informatsiina bezpeka liudyny, suspilstva, derzhavy*, vol. 1 (38), pp. 42—51. DOI: [https://doi.org/10.511369/2707-7276-2025-1\(38\)-4](https://doi.org/10.511369/2707-7276-2025-1(38)-4).

4. Stetsiv, I. S., Stetsiv, I. I., Dziurakh, Yu. M. and Chepil, B. A. (2024), "Problems of public-private partnership in the context of digitalization of management decisions in the sphere of national security of Ukraine", *Derzhava ta rehiony*, vol. 4, pp. 207—215. DOI: <https://doi.org/10.32782/1813-3401.2024.4.31>.

5. Kruhlov, V. V. (2018), "Public-private partnership in the sphere of cybersecurity", *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho*. Seriya: Derzhavne upravlinnia, vol. 3, pp. 57—61.

6. The Verkhovna Rada of Ukraine (2017), *The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity in Ukraine"*, available at: <https://zakon.rada.gov.ua/laws/show/2163-19#top> (Accessed 24 October 2025).

7. Prav, R. Yu. (2019), "The Role of the Public-Private Partnership Mechanism in the Development of Cybersecurity in Ukraine at the Present Stage", *Investytsii: praktyka ta dosvid*, vol. 21, pp. 143—150. DOI: <https://doi.org/10.32702/2306-6814.2019.21.143>.

8. Malakhov, H. B. (2023), "Ways to Improve Public-Private Partnership in the Sphere of Cybersecurity in Ukraine", *Informatsiia i pravo*, vol. 4 (47), pp. 197—206. DOI: [https://doi.org/10.37750/2616-6798.2023.-4\(47\).291666](https://doi.org/10.37750/2616-6798.2023.-4(47).291666).

*Стаття надійшла до редакції 10.11.2025 р.*