

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра

на тему

ПУБЛІЧНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ ЗАБЕЗПЕЧЕННЯ
НАЦІОНАЛЬНОЇ БЕЗПЕКИ: МЕХАНІЗМИ ТА ПЕРСПЕКТИВИ

Виконав студент 2 курсу,
групи ППГЗ-2-24
Спеціальності 281 «Публічне
управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в
умовах гібридних загроз»

_____ Альона ГРОДЕЦЬКА

Науковий керівник роботи:
кандидат наук з державного управління

_____ Олег КУЛІНІЧ

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ.....	14
1.1 Концептуальні основи публічно-приватного партнерства в системі публічного управління національною безпекою.....	14
1.2 Правові та інституційні засади функціонування публічно-приватного партнерства у сфері національної безпеки.....	20
РОЗДІЛ 2 АНАЛІЗ ПРАКТИКИ РЕАЛІЗАЦІЇ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ.....	28
2.1 Міжнародний досвід публічно-приватного партнерства у сфері безпеки та оборони	28
2.2 Стан та проблеми розвитку публічно-приватного партнерства у сфері національної безпеки України.....	36
РОЗДІЛ 3 МЕХАНІЗМИ ВДОСКОНАЛЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ.....	46
3.1 Пріоритетні напрями активізації публічно-приватного партнерства у сфері національної безпеки	46
3.2 Перспективи та рекомендації щодо розвитку публічно-приватного партнерства у сфері забезпечення національної безпеки України	55
ВИСНОВКИ.....	63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	67

ВСТУП

Актуальність теми. Повномасштабна російська агресія проти України кардинально трансформувала розуміння національної безпеки, продемонструвавши критичну важливість ефективної взаємодії державного та приватного секторів для забезпечення обороноздатності країни. Публічно-приватне партнерство у сфері національної безпеки з теоретичної концепції перетворилося на нагальну практичну необхідність, коли приватний сектор, від ІТ-компаній до оборонних стартапів, став невід'ємною частиною системи захисту держави.

З початку повномасштабної війни 24 лютого 2022 року Україна зіткнулася з безпрецедентними викликами для системи національної безпеки, коли традиційні державні механізми виявилися недостатніми для оперативного реагування на швидкозмінні загрози. Волонтерський рух, приватні оборонні компанії та ІТ-сектор продемонстрували потужний потенціал приватної ініціативи, забезпечуючи Збройні Сили України критично необхідним обладнанням, технологіями та послугами.

Оборонно-промисловий комплекс України, де 400 із 500 компаній належать до приватного сектору, довів спроможність виробляти продукції на 20 мільярдів доларів щорічно, що перевищує можливості державних закупівель. Водночас ця потужна хвиля приватної ініціативи залишається значною мірою неінституціоналізованою через критичні прогалини у правовому регулюванні, відсутність координаційних структур, брак фінансових стимулів та культурні бар'єри недовіри між державними органами безпеки та бізнесом.

Відсутність чіткого розподілу повноважень між органами влади, функціональне дублювання, недостатня міжвідомча координація створюють серйозні перешкоди для трансформації стихійної приватної активності у стійку систему публічно-приватної взаємодії.

Актуальність даного дослідження обумовлена нагальною потребою

узагальнення унікального досвіду воєнного часу, аналізу міжнародних практик публічно-приватного партнерства у безпековій сфері та розробки науково обґрунтованих рекомендацій щодо вдосконалення механізмів державно-приватної взаємодії. Ефективна система публічно-приватного партнерства у сфері національної безпеки є необхідною умовою не лише для перемоги у поточній війні, але й для довгострокового забезпечення обороноздатності України, розбудови конкурентоспроможного оборонно-промислового комплексу та успішної інтеграції до євроатлантичних структур безпеки.

Стан наукової розробки проблеми. Проблематика публічно-приватного партнерства у сфері національної безпеки перебуває на перетині декількох наукових дисциплін: державного управління, економіки, права та безпекознавства, що обумовлює міждисциплінарний характер досліджень та певну фрагментарність у розробці цієї проблематики.

Аналіз наукової літератури свідчить про наявність значного масиву досліджень окремих аспектів публічно-приватного партнерства, проте комплексні роботи, які б системно аналізували механізми активізації та перспективи розвитку публічно-приватного партнерства саме у безпековому секторі України в умовах воєнного стану, залишаються поодинокими.

Концепції правового та інституційного регулювання публічно-приватного партнерства у безпековій сфері розробляються вітчизняними науковцями, які концентруються переважно на обґрунтуванні необхідності спеціального законодавчого регулювання для чутливої сфери національної безпеки. Так, Маркіяєва О., Шевчук О.А. та Мех Ю.В. здійснюють критичний аналіз чинного законодавства про публічно-приватне партнерство, виявляючи консенсус щодо наявності критичних прогалин, які не враховують специфіку безпекового сектору – питання доступу до класифікованої інформації, вимоги до благонадійності приватних партнерів та механізми забезпечення національних інтересів при залученні приватного капіталу.

Дідич О.Р. та Квеліашвілі І.М. досліджують особливості трансформації взаємодії держави та бізнесу в умовах повномасштабної війни, аналізуючи

виклики та можливості державно-приватного партнерства у забезпеченні національної безпеки України. Водночас переважна більшість цих досліджень залишається на рівні констатації проблем без пропозицій конкретних механізмів їх вирішення, що обмежує їх практичну цінність для органів публічної влади.

Дослідження практичних механізмів функціонування публічно-приватного партнерства зосереджуються на фінансових стимулах, інституційній архітектурі координації та культурних бар'єрах довіри між державою та бізнесом. Зокрема, Гуменюк Д.М. розробляє механізми публічно-приватного партнерства в реалізації інфраструктурних проектів та вдосконалення нормативної бази, пропонуючи детальну розробку конкретних інструментів активізації публічно-приватного партнерства – від податкових канікул до програм обміну персоналом.

Панасюк В.В. вивчає механізми публічно-приватного партнерства у сфері кібербезпеки, аналізуючи сучасний стан та перспективи розвитку державно-приватної взаємодії у кіберпросторі. Національний інститут стратегічних досліджень через серію своїх публікацій систематизує досвід державно-приватного партнерства у різних секторах національної безпеки. Однак критичний недолік цих досліджень полягає у недостатньому врахуванні специфіки воєнного стану, коли класичні механізми публічно-приватного партнерства потребують адаптації до швидкозмінних потреб оборони та екстремальних умов невизначеності, що вимагає розробки спеціальних механізмів екстреної мобілізації приватних ресурсів.

Міжнародні дослідження демонструють технологічний та емпіричний підхід до аналізу публічно-приватного партнерства у безпековій сфері, акцентуючи увагу на кількісних показниках ефективності, фінансових моделях розподілу ризиків та технологічних інноваціях у оборонній промисловості. Аналітичні звіти Європейського інвестиційного банку, ОБСЄ та Всесвітнього економічного форуму, узагальнені у збірниках аналітичних матеріалів під редакцією Горбуліна В.П. та Власюка О.С., пропонують конкретні інструменти фінансування та координації ППП-проектів у країнах з розвиненими моделями

державно-приватної взаємодії.

Компаративний аналіз, здійснений Бегмою В.М., Чмут Т.О. та Руснаком І.С., свідчить, що країни з успішними моделями публічно-приватного партнерства у національній безпеці мають не лише розвинене спеціальне законодавство, але й потужну культуру довіри між державними органами безпеки та приватним сектором, яка формувалася десятиліттями через інституційні механізми діалогу. Проте ці рекомендації розроблені для мирного часу та потребують критичного переосмислення для країн, що перебувають у стані війни.

Критичний аналіз наукової літератури, здійснений колективами під керівництвом Нижник Н.Р., Кравченка С.О., Пирожкова С.І., Суходолі О.М. та Перепелиці Г.М., виявляє кілька принципових прогалин, які гальмують розвиток як теоретичного розуміння, так і практичної реалізації публічно-приватного партнерства у сфері національної безпеки України. По-перше, практично відсутні дослідження, які узагальнюють унікальний український досвід масової мобілізації приватної ініціативи в умовах повномасштабної війни, коли волонтерський рух та оборонні стартапи фактично компенсували недоліки державної системи закупівель. По-друге, недостатньо вивченими залишаються механізми трансформації стихійної приватної активності у інституціоналізовану систему державно-приватної взаємодії, що є критично важливим для довгострокової стійкості безпекового сектору. По-третє, бракує емпіричних досліджень ефективності різних моделей публічно-приватного партнерства у безпековій сфері з використанням конкретних показників результативності, що ускладнює обґрунтований вибір оптимальних механізмів для українського контексту.

Таким чином, незважаючи на значний обсяг наукових праць з проблематики публічно-приватного партнерства, існує нагальна потреба у комплексному дослідженні, яке б інтегрувало теоретичні напрацювання вітчизняних науковців щодо правового регулювання, практичний досвід міжнародних моделей публічно-приватного партнерства у безпековій сфері та

унікальний український досвід державно-приватної взаємодії в умовах воєнного стану. Саме заповнення цих прогалів через розробку науково обґрунтованих механізмів активізації та стратегічних рекомендацій щодо розвитку публічно-приватного партнерства у сфері національної безпеки визначає актуальність даного дослідження.

Метою роботи є комплексний аналіз практики реалізації публічно-приватного партнерства у сфері національної безпеки України та розробка науково обґрунтованих рекомендацій щодо механізмів активізації та стратегічних перспектив розвитку державно-приватної взаємодії у безпековому секторі.

Для досягнення поставленої мети визначено наступні *завдання*:

- узагальнити концептуальні основи публічно-приватного партнерства в системі публічного управління національною безпекою, уточнити термінологічний апарат та розкрити роль публічно-приватного партнерства у забезпеченні обороноздатності держави;
- дослідити правові та інституційні засади функціонування публічно-приватного партнерства у сфері національної безпеки, проаналізувати нормативно-правову базу та інституційну архітектуру державно-приватної взаємодії;
- здійснити компаративний аналіз міжнародного досвіду публічно-приватного партнерства у сфері безпеки та оборони, виявити успішні практики провідних країн світу;
- проаналізувати стан та проблеми розвитку публічно-приватного партнерства у сфері національної безпеки України, визначити структуру, повноваження та координацію відповідальних органів;
- виявити ключові виклики та системні проблеми функціонування механізмів публічно-приватної взаємодії у безпековому секторі України;
- визначити пріоритетні напрями активізації публічно-приватного партнерства у сфері національної безпеки через розробку комплексу законодавчих, фінансових, інституційних та культурних механізмів;

– розробити стратегічні рекомендації щодо розвитку публічно-приватного партнерства у сфері забезпечення національної безпеки України з урахуванням міжнародного досвіду та специфіки українського контексту.

Об'єктом дослідження є система публічно-приватного партнерства у сфері національної безпеки України.

Предметом дослідження є механізми активізації та перспективи розвитку публічно-приватного партнерства у сфері забезпечення національної безпеки України в умовах воєнного стану.

Методи дослідження. Для досягнення мети дослідження та вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів, застосування яких здійснювалося диференційовано відповідно до специфіки кожного етапу дослідження.

Метод термінологічного аналізу застосовано для уточнення понятійно-категоріального апарату дослідження, розмежування понять «публічно-приватне партнерство», «державно-приватне партнерство», «концесія», «спільне підприємство» тощо, що дозволило створити чітку термінологічну основу роботи; метод теоретичного *узагальнення* використано для систематизації наукових підходів до розуміння ролі публічно-приватного партнерства у забезпеченні національної безпеки та формулювання власних теоретичних висновків; *системний підхід* застосовано для дослідження публічно-приватного партнерства як цілісної системи взаємопов'язаних елементів державної політики у сфері національної безпеки, що дозволило виявити ключові взаємозв'язки між різними компонентами системи; *історичний метод* використано для аналізу еволюції публічно-приватного партнерства у безпековій сфері та виявлення тенденцій його розвитку (підрозділ 1.1).

Нормативно-правовий аналіз застосовано для дослідження законодавчого регулювання публічно-приватного партнерства у сфері національної безпеки, виявлення прогалин та суперечностей, що стало базисом для формулювання законодавчих рекомендацій; *інституційний аналіз* використано для вивчення формальних та неформальних інститутів, що регулюють публічно-приватне

партнерство у безпековому секторі, їх структури та повноважень; *порівняльно-правовий метод* застосовано для зіставлення українського законодавства про публічно-приватне партнерство з міжнародними правовими стандартами та законодавством країн-партнерів; *структурно-функціональний аналіз* використано для визначення ролей та функцій різних інститутів у системі правового регулювання публічно-приватного партнерства (підрозділ 1.2).

Компаративний метод використано для порівняльного аналізу міжнародного досвіду публічно-приватного партнерства у сфері безпеки та оборони, виявлення спільних та відмінних рис різних національних моделей, що дало змогу ідентифікувати успішні практики для адаптації в українських умовах; *метод кейс-стаді* застосовано для поглибленого аналізу конкретних прикладів успішних практик публічно-приватного партнерства у США, Польщі, Естонії, Великобританії та інших демократичних державах, що забезпечило розуміння практичного застосування теоретичних концепцій; *метод типологізації* використано для класифікації моделей публічно-приватного партнерства за різними критеріями та визначення їх адаптивності до українських умов (підрозділ 2.1).

Структурно-функціональний аналіз застосовано для визначення ролей та функцій різних органів публічної влади у практичній реалізації публічно-приватного партнерства у сфері національної безпеки, що допомогло ідентифікувати проблеми координації; *метод документального аналізу* використано для вивчення офіційних документів, стратегій, програм, звітів органів влади щодо публічно-приватного партнерства, що забезпечило емпіричну базу дослідження; *метод моніторингу* застосовано для відстеження та аналізу діяльності органів влади у сфері розвитку публічно-приватного партнерства у період 2022-2025 років, що забезпечило актуальність емпіричних даних; *статистичний аналіз* використано для обробки кількісних показників розвитку оборонно-промислового комплексу, обсягів приватних інвестицій та результативності проектів публічно-приватного партнерства (підрозділи 2.1,2.2).

Проблемно-орієнтований аналіз застосовано для виявлення та

систематизації ключових викликів і проблем функціонування механізмів публічно-приватного партнерства у сфері національної безпеки, що дозволило структурувати виявлені недоліки; *SWOT-аналіз* використано для комплексної оцінки сильних і слабких сторін існуючої системи публічно-приватного партнерства, можливостей та загроз її розвитку, що забезпечило стратегічне бачення перспектив; метод експертних оцінок застосовано для оцінювання ефективності різних механізмів активізації публічно-приватного партнерства, що дозволило ранжувати рекомендації за пріоритетністю (підрозділ 3.1).

Метод стратегічного планування використано для визначення пріоритетних напрямів розвитку системи публічно-приватного партнерства з урахуванням обмежених ресурсів та актуальних викликів; *метод моделювання* застосовано для розробки моделі оптимізованої системи публічно-приватного партнерства у сфері національної безпеки України, що візуалізує бажану майбутню конфігурацію системи; *метод прогнозування* використано для визначення перспективних тенденцій розвитку публічно-приватного партнерства у безпековій сфері та відповідних механізмів його активізації, що забезпечує випереджальний характер рекомендацій; *метод системного синтезу* застосовано для формулювання комплексу взаємопов'язаних стратегічних рекомендацій щодо вдосконалення механізмів публічно-приватного партнерства, що забезпечує цілісність запропонованих змін (підрозділ 3.2).

Комплексне застосування зазначених методів дозволило забезпечити всебічність, об'єктивність та науковість дослідження механізмів активізації та перспектив розвитку публічно-приватного партнерства у сфері національної безпеки України.

Практичне значення отриманих результатів. Результати дослідження мають конкретне практичне застосування у декількох ключових сферах:

У науково-дослідній сфері матеріали роботи можуть бути використані для подальших наукових досліджень механізмів публічно-приватного партнерства у системі забезпечення національної безпеки. Уточнений термінологічний апарат дослідження публічно-приватного партнерства у безпековій сфері сприяє

понятійній визначеності та полегшує міждисциплінарний діалог між юристами, управлінцями, економістами та військовими фахівцями. Узагальнений досвід публічно-приватної взаємодії у сфері національної безпеки в умовах повномасштабної війни становить основу для наукового аналізу трансформації безпекового сектору та збагачує академічну дискусію українськими кейсами.

У практичній діяльності державних органів результати дослідження надають Раді національної безпеки і оборони України аналітичну основу при розробці та вдосконаленні стратегічних документів з питань публічно-приватного партнерства у сфері національної безпеки, зокрема при оновленні Стратегії національної безпеки.

Міністерство оборони України, Міністерство внутрішніх справ, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації отримують конкретні практичні рекомендації щодо механізмів активізації публічно-приватного партнерства, які враховують реальні можливості та обмеження цих органів.

Центральні органи виконавчої влади можуть застосувати результати дослідження при розробці нормативно-правових актів з питань публічно-приватного партнерства у сфері національної безпеки, зокрема при підготовці спеціального закону про публічно-приватне партнерство у безпековому секторі. Виявлені проблеми інституційної фрагментації та координації між різними відомствами дозволять органам влади цілеспрямовано зосередити зусилля на створенні Координаційного центру публічно-приватного партнерства при РНБО.

Розроблені критерії оцінки ефективності публічно-приватного партнерства можуть використовуватися органами влади для моніторингу та оцінювання результативності партнерських проектів у безпековій сфері.

Аналіз міжнародного досвіду забезпечує адаптацію успішних зарубіжних практик до українського контексту через пілотні проекти та посилює міжнародну співпрацю у сфері публічно-приватного партнерства через налагодження інституційних партнерств з країнами НАТО та ЄС.

Фінансові механізми стимулювання приватних інвестицій у безпековий

сектор можуть бути використані Міністерством фінансів України та Українським банком реконструкції та розвитку при розробці спеціальних програм підтримки оборонно-промислового комплексу.

У навчальному процесі матеріали дослідження можуть бути інтегровані закладами вищої освіти при викладанні дисциплін «Національна безпека», «Публічно-приватне партнерство», «Публічне управління та адміністрування», «Державна економічна політика», «Публічне управління на деокупованих територіях» забезпечуючи їх актуальними українськими кейсами та міжнародним досвідом.

Результати дослідження можуть бути включені до програм підготовки та підвищення кваліфікації публічних службовців у Національному агентстві України з питань державної служби, ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна, зокрема для фахівців органів сектору безпеки, які працюють з питань публічно-приватного партнерства.

Узагальнені практики публічно-приватного партнерства у безпековій сфері складають основу практичних занять, воркшопів та тренінгів для державних службовців і представників приватного сектору. Матеріали роботи можуть бути використані при підготовці навчально-методичних посібників, монографій, наукових статей з проблематики публічно-приватного партнерства у сфері національної безпеки, при розробці нових освітньо-професійних програм магістрів публічного управління та адміністрування з спеціалізацією у сфері національної безпеки.

Аналіз кейсів публічно-приватної взаємодії в умовах війни може бути використаний у навчальному процесі як практичний матеріал для вивчення трансформації безпекового сектору на конкретних прикладах українського досвіду, що робить навчання більш прикладним та релевантним до сучасних викликів.

Апробація результатів дослідження. Основні положення та результати роботи обговорювалися на засіданнях кафедри права, національної безпеки та

європейської інтеграції ННІ «Інституту державного управління» Харківського національного університету імені В.Н. Каразіна і можуть бути використані в подальшому в науковій діяльності кафедри та при викладанні дисциплін, пов'язаних з національною безпекою та публічним управлінням.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Концептуальні основи публічно-приватного партнерства в системі публічного управління національною безпекою

Сучасне розуміння національної безпеки, сформульоване в умовах гібридних загроз та повномасштабної агресії, вимагає переосмислення традиційних підходів до організації безпекової діяльності держави. Національна безпека України визначається як стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів від реальних та потенційних загроз [89].

У цьому контексті публічно-приватне партнерство виступає інноваційним механізмом, здатним консолідувати ресурси держави та бізнесу для досягнення спільних безпекових цілей. Критично важливим є усвідомлення того, що традиційна модель монополії держави на функції безпеки вже не відповідає викликам сучасності, особливо в умовах, коли приватний сектор контролює значну частину критичної інфраструктури та володіє передовими технологіями [45; 92].

Концептуально публічно-приватне партнерство у сфері національної безпеки можна визначити як систему інституціолізованих відносин між державними органами сектору безпеки і оборони та суб'єктами приватного сектору, заснованих на взаємній зацікавленості, розподілі ризиків і відповідальності з метою підвищення обороноздатності держави та ефективності використання ресурсів. На відміну від класичних моделей публічно-приватне партнерство в інфраструктурних проектах (партнерство у безпековій сфері) характеризується підвищеними вимогами до конфіденційності, контролю та

національних інтересів [28; 27]. Дослідниця Чальцева стверджує, що державно-приватне партнерство у сфері відновлення має стати альтернативним механізмом посилення спроможностей України, включаючи і оборонні аспекти [106]. Водночас світовий досвід свідчить про успішність застосування публічно-приватного партнерства у різних сегментах безпекового сектору, від кібербезпеки до оборонно-промислового комплексу [2].

Теоретичні підходи до розуміння публічно-приватного партнерства у сфері національної безпеки сформувалися під впливом декількох наукових шкіл і практичних моделей. Неоінституціональна теорія пояснює публічно-приватне партнерство як механізм зниження трансакційних витрат через створення довгострокових контрактних відносин та інституційних структур координації [72].

Теорія суспільних благ обґрунтовує необхідність державно-приватної взаємодії у виробництві безпеки як специфічного блага, що має властивості як публічного, так і клубного блага залежно від контексту [97; 32]. Дослідники Запатріна та інші науковці підкреслюють, що публічно-приватне партнерство є комплексним механізмом співробітництва, заснованим на об'єднанні ресурсів та розподілі ризиків для забезпечення суспільно значущих цілей [33]. Концепція мережевого управління розглядає публічно-приватне партнерство як форму горизонтальної координації між різними акторами у процесі формування та реалізації політики безпеки [91; 104].

Таблиця 1.1 – Еволюція концептуальних підходів до публічно-приватного партнерства у сфері безпеки

<i>Періоди</i>	<i>Домінуюча парадигма</i>	<i>Роль приватного сектору</i>	<i>Форми взаємодії</i>	<i>Ключові характеристики</i>
1990-2001 рр.	Державоцентрична	Периферійна (постачальник)	Державні закупівлі	Монополія держави на безпеку, мінімальна участь бізнесу
2001-2014 рр.	Мережева безпека	Партнерська (захист критичної інфраструктури)	Інформаційний обмін, консультації	Визнання ролі приватного сектору у кіберпросторі

Продовження таблиці 1.1

<i>Періоди</i>	<i>Домінуюча парадигма</i>	<i>Роль приватного сектору</i>	<i>Форми взаємодії</i>	<i>Ключові характеристики</i>
2014-2022 рр.	Інтегрована безпека	Активна (технологічний лідер)	ППП-проекти, державно-приватні платформи	Спільна відповідальність за критичну інфраструктуру
2022-теперішній час	Мобілізаційна стійкість	Стратегічна (співтворець безпеки)	Оборонні стартапи, dual-use інновації	Синергія державних і приватних можливостей

Джерело: розробка автора.

Наведена таблиця 1.1 демонструє докорінну трансформацію ролі приватного сектору у забезпеченні національної безпеки від периферійного постачальника до стратегічного партнера держави. Особливо помітним є зрушення після 2014 року, коли російська агресія спонукала Україну до пошуку нових моделей залучення ресурсів бізнесу та громадянського суспільства.

Сучасний етап характеризується безпрецедентним рівнем приватної ініціативи в оборонній сфері, що включає волонтерський рух, створення оборонних стартапів та активну участь ІТ-компаній у забезпеченні кібербезпеки [62; 24]. Ця еволюція відображає глобальний тренд на демонополізацію безпекових функцій та визнання того, що ефективна безпека у XXI столітті можлива лише через синергію публічних і приватних акторів. Водночас виникають нові виклики щодо балансування безпекових інтересів держави та комерційних інтересів бізнесу [63].

Функціональна специфіка публічно-приватного партнерства у сфері національної безпеки визначається характером безпекових загроз та особливостями організації сектору безпеки і оборони. Основні функції публічно-приватного партнерства у цій сфері включають:

1. Ресурсну функцію – залучення фінансових, технологічних, інтелектуальних та виробничих ресурсів приватного сектору для посилення спроможностей держави у протидії загрозам національній безпеці;
2. Інноваційну функцію – прискорення розробки та впровадження передових технологій подвійного призначення, кіберзахисту, безпілотних

систем та інших інноваційних рішень для потреб безпеки і оборони [93; 64];

3. Координаційну функцію – забезпечення узгодженої взаємодії між державним та приватним секторами в управлінні критичною інфраструктурою, обміні інформацією про загрози та спільному реагуванні на інциденти;

4. Компенсаторну функцію – компенсація обмежень державного сектору через залучення гнучкості, швидкості та підприємницької ефективності приватного бізнесу [15];

5. Легітимаційну функцію – підвищення суспільної довіри до політики національної безпеки через залучення громадянського суспільства та бізнесу до процесів прийняття рішень.

Принципи організації публічно-приватного партнерства у сфері національної безпеки визначаються специфікою цієї чутливої сфери. Базовими принципами є взаємна вигода, де обидві сторони отримують цінність від співпраці, прозорість процедур при збереженні необхідної конфіденційності класифікованої інформації, та розподіл ризиків відповідно до спроможностей сторін [18; 76].

Критичним є принцип національного суверенітету, згідно з яким стратегічні рішення у сфері безпеки залишаються прерогативою держави незалежно від ступеня залучення приватних партнерів. Д. Дубов та колеги наголошують на необхідності побудови довіри між державним та приватним секторами у кіберпросторі, що є фундаментом ефективного партнерства [41]. Також важливим є принцип субсидіарності, відповідно до якого держава залучає приватний сектор там, де він може бути більш ефективним [30; 82].

Сучасні моделі публічно-приватного партнерства у сфері безпеки варіюються від інформаційних платформ обміну даними про загрози до повноцінних оборонних контрактів з елементами публічно-приватного фінансування. У практиці країн НАТО виокремлюються кілька базових моделей партнерства, таких як:

– модель «охорони критичної інфраструктури», де держава встановлює стандарти безпеки, а приватні власники інфраструктури

забезпечують їх дотримання з можливою державною підтримкою;

– модель «оборонних інновацій», орієнтована на стимулювання приватних НДДКР у сфері оборонних технологій через державні замовлення, гранти та венчурне фінансування [31; 90];

– модель «аутсорсингу оборонних послуг», де приватні компанії надають послуги матеріально-технічного забезпечення, навчання персоналу, обслуговування техніки тощо;

– модель «кіберпартнерства», що передбачає інституціоналізовану співпрацю державних CERT-команд з приватними кіберзахисними компаніями та IT-гігантами [29].

Таблиця 1.2 – Порівняльна характеристика моделей публічно-приватного партнерства у безпековій сфері

<i>Модель ППП</i>	<i>Сфера застосування</i>	<i>Переваги</i>	<i>Ризики</i>	<i>Приклади країн</i>
Охорона критичної інфраструктури	Енергетика, транспорт, телекомунікації	Використання ресурсів власників, гнучкість	Конфлікт інтересів, недостатня координація	США, Великобританія, Німеччина
Оборонні інновації	ОПК, dual-use технології	Прискорення інновацій, конкуренція	Витік технологій, залежність від постачальників	Ізраїль, США, Польща
Аутсорсинг послуг	Логістика, навчання, обслуговування	Економія бюджету, спеціалізація	Втрата контролю, етичні дилеми	США, Великобританія, Франція
Кіберпартнерство	Кібербезпека, захист даних	Експертиза, швидкість реагування	Конфіденційність, координація	Естонія, Нідерланди, Сінгапур

Джерело: розробка автора.

Аналіз міжнародного досвіду свідчить, що не існує універсальної моделі публічно-приватного партнерства у безпековій сфері. Кожна країна адаптує партнерські механізми до власних інституційних особливостей, правової культури та специфіки загроз. Американська модель характеризується широким залученням приватних підрядників практично у всіх сегментах оборони та безпеки, що породжує як економічні вигоди, так і етичні дилеми [19].

Європейські країни демонструють більш обережний підхід з акцентом на регуляторні механізми та державний контроль, особливо після терористичних атак 2000-х років [11]. Ізраїльський досвід оборонних інновацій через екосистему стартапів та венчурного капіталу є особливо цінним для України в контексті розбудови власного оборонно-технологічного сектору [10; 9]. Естонський кейс кіберпартнерства демонструє можливості малої держави створити потужну систему кіберзахисту через глибоку інтеграцію держави, бізнесу та громадянського суспільства.

В українському контексті публічно-приватне партнерство у сфері національної безпеки перебуває на етапі інституціоналізації та пошуку оптимальних моделей взаємодії. Стратегія національної безпеки України визначає державно-приватне партнерство як один з механізмів забезпечення безпеки, однак конкретні форми та процедури такого партнерства розроблені недостатньо [89].

Повномасштабна війна продемонструвала величезний потенціал приватної ініціативи – від волонтерського руху до створення оборонних стартапів, які розробляють безпілотники, системи радіоелектронної боротьби та інші інноваційні рішення [6; 4]. За даними міністра стратегічних галузей, оборонно-промисловий комплекс України налічує 500 компаній, з яких 400 – це приватний сектор, що свідчить про потужний потенціал для розвитку публічно-приватного партнерства [20]. Водночас існують значні інституційні, правові та культурні бар'єри на шляху формалізації цих партнерських відносин.

Підбиваючи підсумок, зазначимо, що концептуальні основи публічно-приватного партнерства у сфері національної безпеки формуються на перетині теорій суспільного управління, економічної безпеки та міжнародних відносин. Публічно-приватне партнерство виступає інноваційним механізмом мобілізації ресурсів суспільства для протидії сучасним загрозам через інституціоналізовану співпрацю державних органів безпеки і оборони з приватним сектором.

Еволюція концептуальних підходів демонструє перехід від державоцентричної моделі до інтегрованої парадигми, де приватний сектор

виступає стратегічним партнером у співтворенні національної безпеки.

Функціональна специфіка публічно-приватного партнерства у безпековій сфері визначається ресурсною, інноваційною, координаційною та компенсаторною функціями, реалізація яких відбувається через різноманітні організаційні моделі від охорони критичної інфраструктури до оборонних інновацій.

Міжнародний досвід свідчить про відсутність універсальної моделі партнерства, що вимагає від України розробки власного підходу з урахуванням специфіки безпекового середовища та інституційного контексту.

1.2 Правові та інституційні засади функціонування публічно-приватного партнерства у сфері національної безпеки

Правова регламентація публічно-приватного партнерства у сфері національної безпеки в Україні характеризується фрагментарністю та недостатньою узгодженістю нормативних актів, які регулюють як загальні питання публічно-приватного партнерства, так і специфіку безпекового сектору.

Конституція України встановлює фундаментальні засади, визначаючи безпеку однією з основних функцій держави, водночас не забороняючи участь недержавних акторів у забезпеченні безпеки у формах, визначених законом [47]. Базовим законодавчим актом у сфері публічно-приватного партнерства до червня 2025 року був Закон України «Про державно-приватне партнерство» 2010 року, який встановлював загальні засади партнерства, але не враховував специфіку безпекового сектору [79].

У червні 2025 року було прийнято новий Закон України «Про публічно-приватне партнерство», який передбачає впровадження європейських стандартів та електронної торговельної системи для проєктів концесії [75]. Однак і цей закон не містить спеціальних положень щодо публічно-приватного партнерства

у сфері національної безпеки, що створює правову невизначеність.

Правове регулювання національної безпеки регулюється низкою фундаментальних актів, серед яких Закон України «Про національну безпеку України» 2018 року, який відіграє центральну роль, визначаючи правові основи забезпечення безпеки, повноваження органів сектору безпеки і оборони та механізми демократичного цивільного контролю [85]. Закон визначає сектор безпеки і оборони як систему органів державної влади та інших суб'єктів, проте не конкретизує механізми залучення приватного сектору до виконання завдань національної безпеки.

Стратегія національної безпеки України, затверджена Указом Президента №392/2020 та оновлена у 2025 році, декларує необхідність розвитку державно-приватного партнерства, однак не пропонує конкретних правових механізмів його реалізації [89; 78]. Додатково, Стратегія кібербезпеки України визначає державно-приватне партнерство як один із принципів забезпечення кібербезпеки [98]. Постановою Кабінету Міністрів від грудня 2023 року затверджено план заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки, який передбачає розробку законопроекту про державно-приватне партнерство у сфері кібербезпеки [81].

Спеціальне законодавство містить окремі положення, які стосуються взаємодії держави та приватного сектору у специфічних сферах безпеки. Так, Закон України «Про основні засади забезпечення кібербезпеки України» 2017 року встановлює принцип державно-приватної взаємодії у кіберпросторі та визначає форми такої співпраці, включаючи інформаційний обмін, спільні навчання та координацію реагування на кіберінциденти [86].

Законодавство про оборонно-промисловий комплекс, зокрема Закон України «Про особливості управління об'єктами державної власності в оборонно-промисловому комплексі» від 2011 року, регулює участь приватних підприємств у виробництві оборонної продукції, але не створює системи публічно-приватного партнерства у цій сфері [87]. Законодавство про критичну інфраструктуру, яке активно розвивається останніми роками, встановлює

зобов'язання приватних власників критично важливих об'єктів забезпечувати їх захист відповідно до державних стандартів [84].

Аналіз чинного законодавства виявляє системні прогалини у правовому регулюванні публічно-приватного партнерства сфері національної безпеки, а саме:

1. відсутність спеціального закону, який би комплексно регулював публічно-приватне партнерство у безпековій сфері з урахуванням її специфіки, зокрема режиму секретності, національних інтересів та вимог до партнерів;
2. невизначеність процедур відбору приватних партнерів для проєктів у сфері безпеки, критеріїв їх кваліфікації, перевірки благонадійності та допуску до класифікованої інформації;
3. недостатність механізмів державної підтримки приватних ініціатив у безпековій сфері, включаючи фінансові стимули, податкові пільги, гарантії інвестицій тощо [60; 66];
4. обмеженість правових форм партнерства, оскільки традиційні моделі концесії, оренди чи спільної діяльності не завжди адекватні специфіці безпекових проєктів;
5. неузгодженість регуляторних режимів між загальним законодавством про публічно-приватне партнерство та секторальним законодавством у сфері безпеки, що створює правові конфлікти та невизначеність.

Таблиця 1.3 – Ключові елементи правового регулювання публічно-приватного партнерства у сфері національної безпеки

<i>Рівень регулювання</i>	<i>Нормативні акти</i>	<i>Предмет регулювання</i>	<i>Прогалини</i>
Конституційний	Конституція України	Розмежування державних і недержавних функцій безпеки	Невизначеність меж участі приватного сектору
Базовий законодавчий	Закони про ППП (2010, 2025), про нацбезпеку (2018)	Загальні засади ППП та безпеки	Відсутність інтеграції ППП у безпековий сектор

Продовження таблиці 1.3

<i>Рівень регулювання</i>	<i>Нормативні акти</i>	<i>Предмет регулювання</i>	<i>Прогалини</i>
Стратегічний	Стратегії нацбезпеки, кібербезпеки	Пріоритети політики безпеки	Декларативність, брак конкретних механізмів
Секторальний	Закони про кібербезпеку, ОПК, критичну інфраструктуру	Спеціальні режими у окремих сферах	Фрагментарність, неузгодженість підходів
Підзаконний	Постанови КМУ, інструкції міністерств	Процедури та стандарти	Недостатність деталізації для ППП у безпеці

Джерело: розробка автора.

Правове регулювання публічно-приватного партнерства у безпековій сфері потребує комплексного реформування, яке має врахувати як загальносвітові тенденції залучення приватного сектору до забезпечення безпеки, так і специфічні українські реалії. Ключовим завданням є створення спеціального правового режиму для публічно-приватного партнерства у національній безпеці, який би поєднував гнучкість партнерських механізмів з необхідним рівнем державного контролю та захистом національних інтересів.

Міжнародний досвід, зокрема практика країн НАТО, демонструє необхідність спеціального законодавства, яке регулює участь приватних підприємців у оборонній сфері, включаючи процедури сертифікації, ліцензування та контролю [17; 12]. Особливо актуальним для України є досвід Польщі, яка після 2014 року активно розвивала законодавство про публічно-приватне партнерство у сфері безпеки та оборони [14].

Інституційна архітектура управління публічно-приватного партнерства у сфері національної безпеки в Україні є недостатньо розвинутою та характеризується відсутністю спеціалізованих координаційних структур. На загальнодержавному рівні Міністерство економіки виконує функції головного органу у сфері державної політики публічно-приватного партнерства, однак його компетенція не поширюється на специфіку безпекового сектору [55].

Рада національної безпеки і оборони України як координаційний орган у сфері національної безпеки має потенціал відігравати ключову роль у

формуванні політики публічно-приватного партнерства у безпеці, проте досі не створено відповідних механізмів [68]. Міністерство оборони, Міністерство внутрішніх справ, Служба безпеки України та інші органи сектору безпеки мають окремі підрозділи, що взаємодіють з приватним сектором, але ці зусилля не скоординовані та часто дублюють одне одного.

У сфері кібербезпеки інституційна взаємодія є найбільш розвиненою завдяки специфіці цієї сфери, де приватний сектор контролює більшість інфраструктури. Державна служба спеціального зв'язку та захисту інформації через Урядову команду реагування на комп'ютерні надзвичайні події CERT-UA активно співпрацює з приватними ІТ-компаніями, міжнародними техгігантами та громадськими організаціями [103; 5].

Створення Національного координаційного центру кібербезпеки при РНБО та Національного кластеру кібербезпеки як недержавної платформи є позитивними кроками до інституалізації державно-приватного партнерства [22]. Проте ці ініціативи потребують підкріплення відповідною правовою базою та ресурсним забезпеченням.

Ключовими інституційними викликами розвитку публічно-приватного партнерства у національній безпеці є:

- відсутність єдиного координаційного центру з питань публічно-приватного партнерства у безпековій сфері, що призводить до розпорошення зусиль та неефективності;
- недостатність міжвідомчої координації між органами безпеки, економічними міністерствами та регуляторами ринку [67];
- слабкість інституційної пам'яті та обміну найкращими практиками між різними органами сектору безпеки;
- брак спеціалізованих експертних центрів, які б надавали методичну та аналітичну підтримку ППП-проектам у безпеці;
- недорозвиненість механізмів залучення громадянського суспільства та експертного середовища до обговорення політики публічно-приватного партнерства у безпековій сфері;

- обмеженість ресурсів для підготовки кадрів, здатних ефективно працювати на перетині публічного управління, безпеки та комерційного сектору;
- відсутність систематичного моніторингу та оцінки ефективності існуючих форм державно-приватної взаємодії у безпеці [58; 96].

Міжнародний досвід пропонує різні інституційні моделі організації публічно-приватного партнерства у сфері безпеки. У США функціонує розгалужена система агенцій та програм, що забезпечують взаємодію з приватним сектором у різних аспектах національної безпеки, від кібербезпеки до оборонних інновацій [1]. Особливо цікавим є досвід Агенції передових оборонних дослідницьких проєктів (DARPA), яка ефективно поєднує державне фінансування з залученням приватних компаній та університетів до розробки проривних технологій для потреб оборони.

Європейський Союз розвинув систему рамкових програм та платформ для розвитку публічно-приватного партнерства у сфері безпеки, включаючи Європейську оборонну агенцію та спільні підприємства у сфері кібербезпеки [13]. Скандинавські країни демонструють модель інклюзивного залучення всіх стейкхолдерів через національні форуми безпеки та публічно-приватні платформи діалогу.

Особливої уваги заслуговує питання розмежування повноважень та відповідальності між публічними та приватними партнерами у проєктах публічно-приватного партнерства у сфері безпеки. Принципово важливим є збереження за державою виключного права на прийняття стратегічних рішень у сфері національної безпеки, визначення пріоритетів політики та здійснення демократичного цивільного контролю над силами безпеки [74].

Приватний партнер може залучатися до виконання окремих функцій технічного, логістичного, інноваційного характеру, але не може підміняти державу у виконанні суверенних функцій безпеки. Розподіл ризиків між державою та приватним партнером має враховувати специфіку безпекового сектору, зокрема те, що деякі ризики за своєю природою не можуть бути повністю перекладені на приватного партнера [61]. Відповідальність за

невиконання зобов'язань має бути чітко визначена у договорах публічно-приватного партнерства з урахуванням можливих загроз національній безпеці.

Механізми контролю та моніторингу PPP-проектів у сфері національної безпеки мають бути суттєво посилені порівняно зі звичайними інфраструктурними проектами через чутливість безпекової сфери. Система контролю має включати кілька рівнів: внутрішній контроль з боку органу-партнера, незалежний аудит з боку спеціалізованих контрольних органів, парламентський контроль через відповідні комітети Верховної Ради та громадський контроль з боку інститутів громадянського суспільства [80].

Особливого значення набуває фінансовий контроль, оскільки проекти публічно-приватного партнерства у безпековій сфері часто передбачають значні бюджетні витрати та довгострокові фінансові зобов'язання держави. Водночас необхідно забезпечити баланс між прозорістю, яка є важливою для демократичного контролю, та конфіденційністю інформації, розголошення якої може завдати шкоди національній безпеці [35; 83].

Резюмуючи зазначимо, що правові та інституційні засади функціонування публічно-приватного партнерства у сфері національної безпеки в Україні перебувають на стадії формування та характеризуються значними прогалинами і невідповідностями.

Чинне законодавство не створює комплексної правової основи для розвитку публічно-приватного партнерства у безпековому секторі, обмежуючись загальними положеннями про державно-приватне партнерство та декларативними згадками про необхідність такої взаємодії у стратегічних документах.

Інституційна архітектура управління публічно-приватного партнерства у безпеці є фрагментованою та потребує створення спеціалізованих координаційних структур з чіткими повноваженнями та ресурсами.

Ключовими напрямками вдосконалення правових та інституційних засад є розробка спеціального законодавства про публічно-приватне партнерство у сфері національної безпеки, створення координаційного центру, розвиток

механізмів державної підтримки приватних ініціатив та посилення систем контролю і моніторингу.

Міжнародний досвід, зокрема практика країн НАТО, свідчить про необхідність балансу між залученням можливостей приватного сектору та збереженням державного суверенітету у прийнятті стратегічних рішень щодо національної безпеки.

РОЗДІЛ 2

АНАЛІЗ ПРАКТИКИ РЕАЛІЗАЦІЇ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

2.1 Міжнародний досвід публічно-приватного партнерства у сфері безпеки та оборони

У першому розділі дослідження було обґрунтовано теоретичні засади публічно-приватного партнерства як інноваційного механізму модернізації системи національної безпеки, що поєднує державні ресурси з приватною ініціативою та підприємницькою ефективністю. Логічним продовженням теоретичного аналізу стає вивчення практичного досвіду провідних країн світу, які успішно імплементували різноманітні моделі партнерської взаємодії у безпековій сфері. Дослідження міжнародних практик дозволяє виявити найбільш ефективні механізми, адаптовані до специфічних національних контекстів, та визначити потенціал їх застосування в українських реаліях.

Американська модель публічно-приватного партнерства у сфері національної безпеки, проаналізована С. Кудіновим, вирізняється найбільш розвиненою екосистемою взаємодії держави та приватного сектору серед усіх країн світу [48]. Дослідник наголошує, що характерною особливістю американського підходу є інституціоналізація венчурного фінансування оборонних технологій через спеціалізовані структури, зокрема Офіс стратегічного капіталу при Міністерстві оборони США, який запровадив інноваційні кредитні механізми для фінансування критичних технологій подвійного призначення. За висновками С. Кудінова, партнерство Пентагону з приватною компанією MP Materials на суму 400 мільйонів доларів для виробництва рідкоземельних магнітів демонструє трансформаційний характер американської моделі, де держава виступає не лише замовником, але й

співінвестором стратегічних проектів [48].

М. Попов у своєму дослідженні моделей державно-приватного партнерства обґрунтовує, що американська система базується на триступеневій структурі взаємодії: партнерства на рівні депо для обслуговування військової техніки, кооперативні угоди про дослідження та розробки, а також партнерства для тестування матеріалів і обладнання [73]. Запроваджена ініціатива Small Business Investment Company Critical Technologies, розроблена у партнерстві з Адміністрацією малого бізнесу, спрямована на залучення венчурного капіталу до 14 критичних технологічних напрямків оборонного значення, що підтверджує системний характер державної підтримки приватних інновацій у безпековій сфері [73]. Водночас М. Попов критично зазначає, що масштаби американського оборонного бюджету та розвинена інституційна інфраструктура роблять цю модель важкодоступною для прямого копіювання іншими країнами [73].

Переходячи до аналізу європейського простору, варто зазначити, що моделі публічно-приватного партнерства у сфері безпеки та оборони на європейському континенті характеризуються більшою фрагментарністю та акцентом на регуляторних механізмах порівняно з американським підходом.

Європейський інвестиційний банк у своєму дослідженні «Державно-приватне партнерство у сфері безпеки та оборони» (2025) констатує, що європейські країни традиційно надавали перевагу державному контролю над оборонною сферою, проте останні геополітичні виклики спонукали до активізації залучення приватного капіталу [42]. Зокрема, банк відзначає, що у березні 2025 року було змінено правила прийнятності фінансування, дозволивши підтримку проектів, основною метою яких є оборона, а не лише подвійне призначення, що відкриває якісно нові можливості для публічно-приватного фінансування оборонної промисловості [42].

Д. Лаврентій, досліджуючи європейський досвід публічно-приватного партнерства, виокремлює німецьку модель як приклад фондового підходу з поступовим нарощуванням потужностей [51]. Німеччина у відповідь на повномасштабну російську агресію проти України створила спеціальний фонд

на 100 мільярдів євро для оновлення застарілого військового обладнання Бундесверу, проте дослідник критично аналізує повільність реалізації цього механізму, констатує, що станом на лютий 2023 року жодного євро з фонду не було витрачено [51]. За оцінкою Д. Лаврентія, німецька модель передбачає поступовий перехід до досягнення показника витрат на оборону у 2% ВВП, якого країна досягла 2024 року за допомогою спеціального фонду, проте після його вичерпання залишається невизначеність щодо подальшого фінансування [51].

На відміну від поступового німецького підходу, польська модель публічно-приватного партнерства у оборонній сфері, проаналізована В. Мостовим при дослідженні світового досвіду публічно-приватного партнерства, демонструє найбільш динамічний розвиток серед європейських країн [59]. В. Мостовий обґрунтовує, що успіх польської моделі базується на триетапній стратегії: екстрені закупівлі для швидкої заміни переданих Україні систем озброєнь, середньострокова диверсифікація постачальників та довгострокові інвестиції у власні виробничі потужності [59]. За даними дослідника, тільки у 2024 році Міністерство національної оборони Польщі підписало понад 130 контрактів на загальну суму 35,2 мільярда євро, що підтверджується широкою громадською підтримкою оборонних витрат на рівні 73% населення. Характерною особливістю першого етапу польської стратегії є пріоритетність швидкості постачання над ціною та передачею технологій, що відповідає нагальним безпековим потребам у відповідь на російську загрозу [59].

Якщо польська модель зосереджена на швидкому нарощуванні класичних оборонних спроможностей, то естонська модель публічно-приватного партнерства демонструє інший вектор розвитку, концентруючись на кібербезпеці та цифровій трансформації безпекового сектору. С. Серебряк у фундаментальному дослідженні державно-приватного партнерства у сфері кіберзахисту констатує, що Естонія займає третє місце в Національному індексі кібербезпеки та Глобальному індексі кібербезпеки станом на 2022 рік, що підтверджує ефективність обраної моделі [94]. Дослідниця детально аналізує естонську стратегію кібербезпеки на 2024-2030 роки «Кіберсвідома Естонія», яка

спрямована на забезпечення кіберстійкості через посилення управління та координацію між урядовим та приватним секторами, розвиток кіберсвідомого суспільства через освітні програми та модернізацію інфраструктури кіберзахисту з використанням технологій штучного інтелекту [94].

О. Маркієва у дослідженні державно-приватного партнерства у сфері кібербезпеки акцентує увагу на фінансовому аспекті естонської моделі, зазначаючи, що фінансування кібербезпеки в Естонії зросло з 3,9 мільйонів євро в 2020 році до 16,1 мільйонів євро в 2024 році, що становить більш ніж чотирикратне зростання за короткий період [52]. Дослідниця особливо підкреслює інноваційність публічно-приватного партнерства під назвою Ліга кіберзахисту, яке було створене для посилення спроможності країни запобігати та реагувати на кібератаки, що впливають на національну безпеку [52]. За висновками О. Маркієвої, естонська модель виходить далеко за межі кібербезпеки, охоплюючи широкий спектр цифрових послуг та інновацій, включаючи платформу Texta для текстової аналітики, систему Hans для розпізнавання мови та застосунок Noia для запобігання поширенню COVID-19 [52].

ОБСЄ у своєму аналітичному звіті «Новітні практики у державно-приватних партнерствах, пов'язаних з кібербезпекою» (2023) узагальнює міжнародний досвід та констатує, що естонський підхід до публічно-приватних партнерств характеризується проведенням менших пілотних проектів для перевірки життєздатності ідей перед їх масштабуванням, що мінімізує ризики та забезпечує ефективне використання ресурсів [65]. Організація підкреслює, що Естонія є прикладом країни, де цифрова держава побудована на партнерстві та довірі між державою, приватним сектором, академічними колами та громадянським суспільством, де від електронної ідентифікації до електронних медичних послуг все створено через партнерство [65].

Всесвітній економічний форум у роботі «Розвиток кіберталантів через державно-приватне партнерство» (2025) аналізує критичну роль партнерської взаємодії у формуванні кадрового потенціалу для кібербезпеки [25]. Форум

обґрунтовує, що успішні міжнародні моделі базуються на тристоронній співпраці між державою, приватним сектором та академічними установами для підготовки спеціалістів з кібербезпеки, де естонська модель розглядається як еталонна [25]. У. Танвір в науковій статті «Державно-приватні партнерства як каталізатори цифрової трансформації», опублікованій у виданні ScienceDirect (2025), розширює аналіз, стверджуючи, що цифрові публічно-приватні партнерства не обмежуються лише технологічним аспектом, а охоплюють інституційну трансформацію державного управління через залучення приватних інновацій [16].

Повертаючись до аналізу традиційних європейських моделей оборонного партнерства, французька модель, яка була досліджена на прикладі проекту CEGELOG, Balard-Défense, демонструє класичний європейський підхід з акцентом на суверенні технології та державний контроль [3].

Європейський інвестиційний банк аналізує цей проект як приклад концесійної моделі публічно-приватного партнерства, де французька держава зберігає стратегічний контроль над оборонними об'єктами, водночас залучаючи приватний капітал та управлінську ефективність для їх модернізації. За даними аналізу ЄІБ, французька модель передбачає довгострокові контракти з національними виробниками, що забезпечує технологічний суверенітет, але обмежує конкуренцію та може призводити до вищих витрат порівняно з більш відкритими моделями [3].

Литовський парламент у документації щодо державно-приватного партнерства для проектів військового розміщення (Вільнюс, Шяуляй, Шилале) демонструє прагматичний підхід малої країни НАТО до швидкого розширення військової інфраструктури через залучення приватного фінансування [71]. Аналіз литовського досвіду свідчить про можливість успішної реалізації ППП-проектів навіть за обмежених бюджетних ресурсів через чітке розмежування відповідальності між державою та приватним сектором і використання міжнародних гарантій НАТО [71].

Проаналізовані міжнародні проекти Griffin, ECSA-CERBERUS та

ProtectUK демонструють різноманітність інституційних форм публічно-приватного партнерства у безпековій сфері [8]. Проект Griffin у Великій Британії зосереджений на підвищенні обізнаності приватного сектору щодо терористичних загроз через регулярні інформаційні брифінги та тренінги [8].

ECSA-CERBERUS як європейська ініціатива спрямована на координацію приватних охоронних компаній з державними службами безпеки для захисту критичної інфраструктури [8]. ProtectUK представляє цифрову платформу для обміну інформацією про загрози безпеці між державними органами та бізнесом, що підтверджує тренд цифровізації публічно-приватної взаємодії у безпековій сфері [8].

Дослідження нових державно-приватних партнерств у сфері безпеки в Данії, Великій Британії та ЄС, проведене аналітиками Європейського інвестиційного банку, виявляє сучасні тенденції еволюції ППП-моделей у відповідь на гібридні загрози [43].

Данія демонструє інноваційний підхід до фінансування української оборонної промисловості, ставши першою країною, що виділила 28,5 мільйонів доларів США на закупівлю обладнання українського виробництва для Сил оборони, що створює прецедент міжнародного публічно-приватного партнерства через фінансування третіх країн [43].

Для систематизації та узагальнення проаналізованого міжнародного досвіду доцільно здійснити порівняльний аналіз ключових характеристик моделей публічно-приватного партнерства у провідних країнах світу.

Наведена нижче таблиця 2.1, розроблена на основі систематизації наукових досліджень, дозволяє наочно побачити відмінності у підходах, механізмах, обсягах інвестицій та потенціалі адаптації для українського контексту, що є критично важливим для формування національної стратегії розвитку публічно-приватного партнерства у безпековій сфері.

Таблиця 2.1 – Порівняльний аналіз моделей публічно-приватного партнерства у безпеці провідних країн світу

<i>Країна</i>	<i>Модель ППП</i>	<i>Ключові механізми</i>	<i>Характерні особливості</i>	<i>Можливість імплементації в Україні</i>
США	Інтегрована модель з венчурним капіталом	Офіс стратегічного капіталу, триступенева структура взаємодії	Держава як співінвестор, 14 критичних технологічних напрямків	Частково: венчурне фінансування стартапів, технології подвійного призначення
Німеччина	Фондова модель з поступовим нарощуванням	Спеціальний фонд €100 млрд, підтримка партнерів	Повільна реалізація, досягнення 2% ВВП на оборону	Так: створення спецфонду, потрібна політична воля
Польща	Динамічна модель екстреного реагування	Триетапна стратегія, 130+ контрактів (€35,2 млрд)	Пріоритет швидкості над ціною, диверсифікація постачальників	Так: найбільш придатна модель для українських умов
Естонія	Цифрова модель кіберпартнерства	Ліга кіберзахисту, пілотні проекти, відкриті технології	Зростання фінансування у 4 рази (2020-2024), культура довіри	Так: використання потенціалу ІТ-сектору
Франція	Суверенна модель з державним контролем	Концесії (CEGELOG, Balard-Défense), національні виробники	Технологічний суверенітет, довгострокові контракти	Частково: потрібен розвиток власного ОПК
Литва	Прагматична модель швидкого розгортання	ППП для військової інфраструктури (3 міста)	Використання гарантій НАТО, обмежені ресурси	Так: адаптація для післявоєнної відбудови
Великобританія	Інформаційно-координаційна модель	Griffin, ProtectUK, цифрові платформи	Обізнаність бізнесу, обмін інформацією про загрози	Так: створення аналогічних платформ

Джерело: розробка автора

Sulj ОДУВС у дослідженні державно-приватного партнерства у сфері національної безпеки узагальнює міжнародний досвід та формулює критичні уроки для країн, що розвивають власні моделі публічно-приватного партнерства. Обґрунтовано, що американська модель інтегрованого публічно-приватного партнерства з венчурним капіталом та офісом стратегічного капіталу може бути

частково адаптована через створення національних механізмів венчурного фінансування оборонних стартапів та технологій подвійного призначення, проте масштаби американського оборонного бюджету та інституційна спроможність залишаються недосяжними для більшості країн у короткостроковій перспективі [99].

Польська модель динамічного реагування з триетапною стратегією закупівель, на думку Sulj, виглядає найбільш придатною для країн із середнім рівнем економічного розвитку, оскільки забезпечує швидке зростання потужностей через диверсифікацію постачальників та прагматичний підхід до балансу між швидкістю постачання, ціною та передачею технологій [99].

Естонська модель кіберпартнерства з Лігою кіберзахисту, пілотними проектами та відкритими технологіями може бути успішно реалізована країнами з розвиненим ІТ-сектором через створення аналогічних структур публічно-приватної взаємодії в кіберпросторі [99].

Критичним уроком міжнародного досвіду, за висновком Sulj, є необхідний баланс між залученням можливостей приватного сектору та збереженням державного контролю над стратегічними рішеннями у сфері національної безпеки [99]. Усі успішні міжнародні моделі демонструють наявність чіткого правового регулювання публічно-приватних відносин, інституційної спроможності для координації взаємодії та культури довіри між державними та приватними акторами, що потребує системної розбудови.

На підставі викладеного, зробимо наступні висновки: міжнародний досвід публічно-приватного партнерства у сфері безпеки та оборони демонструє різноманітність організаційних моделей та механізмів взаємодії держави з приватним сектором, адаптованих до специфічних національних контекстів та рівнів загроз.

Американська модель інтегрованого публічно-приватного партнерства з венчурним капіталом забезпечує найбільші обсяги приватних інвестицій в оборонні технології через тріступеневу структуру взаємодії та роль держави як співінвестора, проте потребує значного бюджету та розвиненої інституційної

інфраструктури.

Польська динамічна модель екстреного реагування виявилася найбільш ефективною серед європейських країн у швидкому нарощуванні оборонних спроможностей через триетапну стратегію та диверсифікацію постачальників, що робить її найбільш придатною для адаптації у країнах із середнім рівнем економічного розвитку.

Естонська модель цифрового кіберпартнерства з Лігою кіберзахисту та пілотними проектами демонструє можливості малої країни досягти високого рівня кіберстійкості через глибоку інтеграцію держави, бізнесу та громадянського суспільства, використовуючи відкриті технології та культуру довіри.

Критичними уроками міжнародного досвіду є необхідність чіткого правового регулювання ППП у безпековій сфері, створення інституційних механізмів координації, розвитку культури довіри між державним та приватним секторами та забезпечення балансу між залученням приватних ресурсів і збереженням державного суверенітету у прийнятті стратегічних безпекових рішень.

2.2 Стан та проблеми розвитку публічно-приватного партнерства у сфері національної безпеки України

Проаналізувавши різноманітні міжнародні моделі публічно-приватного партнерства у попередньому підрозділі, логічно перейти до дослідження української специфіки впровадження цих механізмів у безпековому секторі.

Вивчення вітчизняного досвіду дозволяє зрозуміти, наскільки теоретичні концепції та зарубіжні практики знаходять своє втілення в українських реаліях, загострених повномасштабною російською агресією. Особливо важливим є виявлення системних проблем, які гальмують розвиток державно-приватної

взаємодії у сфері національної безпеки України.

О. Дідич у дослідженні державно-приватного партнерства у забезпеченні національної безпеки України констатує, що повномасштабна російська агресія кардинально трансформувала ландшафт публічно-приватної взаємодії, створивши безпрецедентні можливості та виклики для інституціоналізації партнерства між державою та бізнесом [36]. Дослідниця обґрунтовує, що оборонно-промисловий комплекс України за даними 2024 року нараховує 500 компаній, з яких 400 належать до приватного сектору, що свідчить про домінування недержавних суб'єктів у виробництві оборонної продукції та величезний потенціал для розвитку публічно-приватного партнерства. За оцінкою О. Дідич, оборонний сектор забезпечив 1,5 процентних пунктів з 5% зростання ВВП України у 2023 році, залишаючись одним з основних драйверів економіки у воєнних умовах [36].

Водночас О. Дідич критично аналізує диспропорцію між виробничими потужностями та державним попитом, зазначаючи, що потужність української оборонної промисловості у 2024 році перевищила спроможність Міністерства оборони щодо закупівель. За її підрахунками, оборонно-промисловий комплекс України може виробляти продукції на близько 20 мільярдів доларів на рік, тоді як Міноборони спроможне закупити лише на 6 мільярдів доларів, що актуалізує необхідність залучення міжнародних партнерів для фінансування українського оборонно-промислового комплексу [36].

С. Кудінов у своїй роботі аналізує унікальний феномен волонтерського руху та приватних ініціатив у забезпеченні обороноздатності України. Дослідник обґрунтовує, що десятки тисяч волонтерів та численні волонтерські організації з початку повномасштабної війни забезпечували постачання критично необхідного обладнання, техніки, засобів індивідуального захисту для Збройних Сил України, компенсуючи недоліки державної логістики та закупівель [49]. С.Кудінов також підкреслює, що приватні оборонні стартапи, які розробляють безпілотні літальні апарати, системи електронної боротьби та засоби зв'язку, довели свою спроможність швидко реагувати на потреби фронту та

впроваджувати технології, що конкурують з продукцією провідних світових виробників [49].

Т. Панасюк у дослідженні державної політики України у сфері забезпечення кібербезпеки констатує, що ІТ-компанії України активно долучилися до забезпечення кібербезпеки держави, захисту критичної інфраструктури та протидії російським кібератакам, використовуючи власну експертизу та технології для підтримки державних органів безпеки [70]. Проте дослідниця критично зазначає, що ця потужна хвиля приватної ініціативи залишається значною мірою неінституціоналізованою, що створює ризики неефективності, дублювання зусиль, відсутності координації та втрати довіри через окремі випадки зловживань [70].

Правове регулювання публічно-приватного партнерства у сфері національної безпеки України, проаналізоване А. Теслею характеризується критичними прогалинами та відсутністю спеціалізованого законодавчого забезпечення [101]. А. Тесля у дослідженні сучасного стану нормативно-правового регулювання державно-приватного партнерства зазначає, що новий Закон України «Про публічно-приватне партнерство», прийнятий у червні 2025 року, впроваджує європейські стандарти та електронну торговельну систему для проектних концесій, проте не містить жодних спеціальних положень щодо специфіки публічно-приватного партнерства у безпековому секторі [101]. За висновком дослідника, Стратегія національної безпеки України (затверджена Указом Президента № 392/2020) декларує необхідність розвитку державно-приватного партнерства як одного з механізмів забезпечення безпеки, однак ці положення мають загальний характер без конкретизації форм, процедур та механізмів реалізації такого партнерства [101, 89].

DLF у аналітичному огляді «Публічно-приватне партнерство в Україні – нові правила» (2025) акцентує увагу на тому, що відсутність спеціального правового режиму для публічно-приватного партнерства у національній безпеці створює невизначеність щодо процедур відбору приватних партнерів, вимог до їх кваліфікації та благонадійності, режиму доступу до класифікованої інформації

та розподілу ризиків і відповідальності між державою та приватним сектором [38]. Аналітики підкреслюють, що План заходів з реалізації Стратегії кібербезпеки України на 2023-2024 роки передбачає розробку законопроекту про державно-приватне партнерство у сфері кібербезпеки, проте станом на жовтень 2025 року цей законопроект досі не підготовлено [38].

Ю. Мех у своєму дослідженні державно-приватного партнерства в секторі безпеки України детально аналізує інституційну архітектуру управління публічно-приватного партнерства, констатує відсутність спеціалізованого координаційного центру та розпорошеність функцій між численними органами влади [56]. Дослідник обґрунтовує, що Міністерство економіки як головний орган у сфері державної політики публічно-приватного партнерства не має компетенції та експертизи для роботи зі специфікою безпекового сектору, тоді як Рада національної безпеки і оборони України не створила відповідних механізмів для координації публічно-приватної взаємодії у безпеці. За висновками Ю. Мехи, Міністерство оборони, Міністерство внутрішніх справ, Служба безпеки України та інші органи сектору безпеки мають окремі підрозділи для взаємодії з приватним сектором, проте ці зусилля не скоординовані та не базуються на єдиних стандартах [56].

Дослідження щодо особливостей державно-приватного партнерства у сфері кібербезпеки, проведене науковцями Ради досліджень, виявляє, що Державна служба спеціального зв'язку через CERT-UA активно співпрацює з приватними ІТ-компаніями, проте ця взаємодія відбувається переважно на неформальній основі без належного правового та фінансового забезпечення [40]. Дослідники наголошують, що Національний кластер кібербезпеки як недержавна платформа об'єднання зацікавлених сторін потребує підкріплення державною підтримкою та інтеграції у формальні структури координації політики кібербезпеки [40].

Українські юридичні фірми у спільному аналітичному огляді державно-приватного партнерства в секторі безпеки та оборони України систематизують ключові проблеми розвитку публічно-приватного партнерства [102]. Правова

невизначеність через відсутність спеціального законодавства про публічно-приватне партнерство у безпековій сфері створює юридичний вакуум, що знижує готовність приватного бізнесу інвестувати у довгострокові проекти через високі юридичні ризики та непередбачуваність умов співпраці з державою [102].

Інституційна фрагментація, виражена у розпорошеності функцій координації публічно-приватного партнерства між численними органами влади без єдиного центру відповідальності, призводить до дублювання зусиль, неефективного використання ресурсів та відсутності системного підходу до формування політики публічно-приватної взаємодії [102].

Журнали Вернадського у публікації щодо державно-приватного партнерства та нормативного регулювання аналізують проблему недостатності фінансових стимулів, яка проявляється у браку податкових пільг, державних гарантій, пільгового кредитування та інших механізмів фінансової підтримки приватних компаній, що інвестують у проекти національної безпеки [34]. Це знижує привабливість безпекового сектору для бізнесу порівняно з комерційними проектами. Культурні бар'єри, виражені у традиційній недовірі між державними органами безпеки та приватним сектором, закритості безпекових структур та небажанні ділитися інформацією з недержавними акторами, утруднюють формування партнерських відносин, заснованих на взаємній довірі [34].

Стратегія «Цифрова армія» Міністерства оборони України, яка передбачає активну співпраці з приватним сектором, демонструє спроби інституціоналізації публічно-приватної взаємодії на рівні окремих відомств [105]. Проте В. Кучеренко досліджуючи міжнародний та вітчизняний досвід державно-приватного партнерства у сфері охорони критично зазначає, що обмежена інституційна спроможність пов'язана з дефіцитом кваліфікованих кадрів у державних органах, які розуміють специфіку як безпекового сектору, так і комерційної діяльності [50].

Дослідження REICST про моделі реалізації державно-приватного партнерства виявляє, що корупційні ризики становлять серйозну проблему,

оскільки висока вразливість оборонних закупівель та проектів у безпековій сфері до корупційних схем через режим секретності, обмежену публічність процедур та значні бюджетні кошти підривають довіру до державно-приватної взаємодії [39].

ЕCSA-CERBERUS, Griffin, ProtectUK у контексті українського аспекту моделей співпраці демонструють потенційні напрями адаптації міжнародного досвіду [7]. Водночас досвід реалізації окремих елементів публічно-приватної взаємодії у сфері національної безпеки України показує як успішні практики, так і проблемні аспекти.

Приклади успішного публічно-приватного партнерства включають партнерство міжнародної компанії Amentum з українською оборонною промисловістю у створенні виробничих потужностей на території України та проект компанії Roshel для виробництва бронетехніки, що посилює оборонно-промислову базу країни [53].

Для систематизації виявлених проблем та потенційних шляхів їх подолання доцільно звести ключову інформацію у структуровану аналітичну таблицю.

Така систематизація, базована на узагальненні наукових досліджень вітчизняних науковців, дозволяє наочно побачити взаємозв'язки між проблемами, їх проявами, наслідками та можливими рішеннями, що є важливим для розробки комплексної стратегії розвитку публічно-приватного партнерства у безпековій сфері України.

Таблиця 2.2 – Ключові проблеми та шляхи їх подолання у розвитку ППП у сфері національної безпеки України

<i>Проблема</i>	<i>Прояви</i>	<i>Наслідки</i>	<i>Шляхи подолання</i>	<i>Джерела</i>
Правова невизначеність	Відсутність спецзаконодавства про ППП у безпеці, незавершений законопроект про кіберпартнерство	Юридичні ризики, небажання бізнесу інвестувати у довгострокові проекти	Прийняття спеціального закону про ППП у сфері національної безпеки з чіткими процедурами	[102; 38; 101]

Продовження таблиці 2.2

<i>Проблема</i>	<i>Прояви</i>	<i>Наслідки</i>	<i>Шляхи подолання</i>	<i>Джерела</i>
Інституційна фрагментація	Розпорошеність функцій між МО, МВС, СБУ, Мінекономіки без координації	Дублювання зусиль, неефективність використання ресурсів	Створення Координаційного центру ППП при РНБО з делегованими повноваженнями	[56; 40]
Брак фінансових стимулів	Відсутність податкових пільг, державних гарантій, пільгового кредитування	Низька привабливість безпекового сектору для приватних інвестицій	Запровадження податкових канікул, державних гарантій для оборонних стартапів	[34]
Культурні бар'єри	Недовіра між силовиками та бізнесом, закритість інформації, небажання співпрацювати	Утруднення формування партнерських відносин, низька ефективність взаємодії	Програми обміну персоналом, спільні навчання, постійні платформи діалогу	[49; 34]
Обмежена інституційна спроможність	Дефіцит кваліфікованих кадрів, що розуміють специфіку обох секторів	Неефективне управління ППП-проектами на перетині безпеки та бізнесу	Спеціалізовані програми навчання, залучення міжнародних експертів	[50]
Корупційні ризики	Непрозорість оборонних закупівель, режим секретності, обмежена публічність	Втрата довіри, розкрадання коштів, неефективне використання ресурсів	Електронні закупівлі для класифікованої продукції, незалежний аудит	[39]

Джерело: розробка автора

Аналіз ключових проблем розвитку публічно-приватного партнерства у сфері національної безпеки України дозволяє сформулювати обґрунтовані шляхи їх подолання на основі міжнародного досвіду та специфіки українського контексту.

Правова невизначеність може бути подолана через прийняття спеціального Закону України «Про публічно-приватне партнерство у сфері національної безпеки», який би встановив чіткі процедури відбору партнерів, форми співпраці, режим секретності, механізми фінансування та розподілу ризиків,

адаптуючи кращі практики польського та естонського законодавства до українських умов.

Інституційна фрагментація вимагає створення Координаційного центру публічно-приватного партнерства у сфері безпеки при Раді національної безпеки і оборони України з делегованими повноваженнями координувати діяльність усіх органів сектору безпеки, методично підтримувати ППП-проекти та здійснювати моніторинг їх реалізації за єдиними стандартами. Брак фінансових стимулів може бути компенсований через запровадження комплексної системи державної підтримки, що включає податкові канікули для оборонних стартапів на перші три роки, державні гарантії за кредитами для виробників оборонної продукції та пільгове кредитування проектів подвійного призначення.

Культурні бар'єри між державними органами безпеки та приватним сектором потребують довгострокових зусиль з формування культури довіри через запровадження програм обміну персоналом між силовими структурами та приватними компаніями, проведення спільних навчань та тренінгів, створення постійно діючих платформ діалогу між представниками держави та бізнесу. Корупційні ризики в оборонних закупівлях та ППП-проектах можуть бути мінімізовані через запровадження електронних закупівель навіть для класифікованої продукції зі зниженим обсягом оприлюднюваної інформації, створення незалежної системи аудиту оборонних проектів за участю міжнародних експертів та посилення громадського контролю через спеціалізовані наглядові ради.

Резюмуючи зазначимо, що стан публічно-приватного партнерства у сфері національної безпеки України характеризується потужним потенціалом приватної ініціативи, який яскраво проявився в умовах повномасштабної війни через волонтерський рух, оборонні стартапи та залучення ІТ-сектору, проте цей потенціал значною мірою залишається неінституціоналізованим через критичні прогалини у правовому регулюванні та інституційному забезпеченні. Оборонно-промисловий комплекс України з 500 компаній, де 400 належать до приватного сектору, довів свою спроможність забезпечити зростання ВВП та виробляти

продукцію на 20 мільярдів доларів річно, проте диспропорція між виробничими потужностями та державним попитом актуалізує необхідність залучення міжнародного фінансування та створення прозорих механізмів закупівель.

Ключові проблеми розвитку публічно-приватного партнерства включають правову невизначеність через відсутність спеціального законодавства, інституційну фрагментацію без єдиного координаційного центру, брак фінансових стимулів, культурні бар'єри недовіри та корупційні ризики в оборонних закупівлях.

Подолання цих проблем вимагає комплексного підходу через прийняття спеціального закону про публічно-приватне партнерство у сфері національної безпеки, створення Координаційного центру при РНБО, запровадження системи державної підтримки оборонних стартапів, формування культури довіри через програми обміну та діалогу, а також посилення прозорості через електронні закупівлі та незалежний аудит.

Аналіз практики реалізації публічно-приватного партнерства у сфері національної безпеки на міжнародному та національному рівнях дозволяє сформулювати ключові висновки щодо ефективних моделей взаємодії та критичних викликів, що стоять перед Україною. Міжнародний досвід, систематизований на основі досліджень провідних науковців, демонструє, що успішне публічно-приватне партнерство у безпековій сфері вимагає не лише фінансових ресурсів, але й чіткого правового регулювання, інституційної спроможності для координації, професійних кадрів та культури довіри між державою та бізнесом, при цьому кожна країна адаптує моделі партнерства до власних інституційних особливостей та специфіки загроз.

Польська динамічна модель екстреного реагування з триетапною стратегією закупівель є найбільш придатною для впровадження в Україні через прагматичний баланс між швидкістю постачання та передачею технологій, тоді як естонська модель кіберпартнерства може бути успішно адаптована для використання потенціалу українського ІТ-сектору. Стан публічно-приватного партнерства у сфері національної безпеки України характеризується

парадоксальною ситуацією, коли потужний потенціал приватної ініціативи, що проявився через волонтерський рух та оборонні стартапи, не отримує належної інституційної підтримки через критичні прогалини у правовому регулюванні, відсутність координаційних структур, брак фінансових стимулів та культурні бар'єри недовіри між державними органами безпеки та бізнесом.

Подолання системних проблем вимагає комплексного підходу через прийняття спеціального законодавства про ППП у безпековій сфері, створення Координаційного центру при РНБО, запровадження податкових пільг та державних гарантій для оборонних стартапів, формування культури довіри через програми обміну та діалогу, а також посилення прозорості оборонних закупівель через електронізацію та незалежний аудит, що дозволить трансформувати стихійну приватну ініціативу у стійку систему публічно-приватної взаємодії для довгострокового посилення обороноздатності України.

РОЗДІЛ 3

МЕХАНІЗМИ ВДОСКОНАЛЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПУБЛІЧНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

3.1 Пріоритетні напрями активізації публічно-приватного партнерства у сфері національної безпеки

Проаналізувавши у попередньому розділі міжнародний досвід та стан публічно-приватного партнерства у сфері національної безпеки України, виявивши системні проблеми та виклики, логічно перейти до формування конкретних механізмів активізації партнерської взаємодії між державою та бізнесом.

Визначення пріоритетних напрямів розвитку публічно-приватного партнерства у безпековій сфері вимагає комплексного підходу, що враховує як нагальні потреби оборони держави в умовах повномасштабної війни, так і довгострокові стратегічні завдання побудови стійкої системи національної безпеки. Розробка та впровадження дієвих механізмів активізації публічно-приватного партнерства є критично важливою передумовою трансформації потужного потенціалу приватної ініціативи у інституціоналізовану систему державно-приватної взаємодії.

Законодавче забезпечення як фундамент розвитку публічно-приватного партнерства у безпековій сфері потребує першочергового вдосконалення, що підтверджується як вітчизняними дослідженнями, так і міжнародною практикою. Аналіз чинного законодавства України виявляє критичну прогалину: Закон України «Про публічно-приватне партнерство» не враховує специфіку безпекового сектору, зокрема питання доступу до класифікованої інформації, особливі вимоги до кваліфікації та благонадійності приватних партнерів, а також

механізми забезпечення національної безпеки при реалізації ППП-проектів [53; 107]. Ця ситуація створює правову невизначеність, яка стримує готовність бізнесу інвестувати у довгострокові проекти національної безпеки через високі юридичні ризики.

Міжнародний досвід демонструє протилежну тенденцію: країни з успішними моделями публічно-приватного партнерства у безпековій сфері мають спеціальне законодавство, адаптоване до специфіки сектору. Наприклад, Сполучені Штати Америки прийняли Defense Production Act, який регулює залучення приватного сектору до виконання оборонних замовлень та надає президенту повноваження стимулювати виробництво критичної продукції через механізми гарантованих закупівель та державних гарантій.

Великобританія розробила спеціальний Defence and Security Public Contracts Regulations, що встановлює окремі процедури для закупівель у сфері оборони та безпеки з урахуванням режиму секретності. Естонія у своєму Cybersecurity Act детально врегулювала питання державно-приватного партнерства у кіберпросторі, включаючи механізми обміну класифікованою інформацією про загрози між державними органами та акредитованими приватними компаніями.

Польща у 2023 році прийняла спеціальні поправки до закону про оборонні закупівлі, які спрощують процедури залучення приватних виробників до виконання термінових оборонних замовлень в умовах підвищених загроз безпеці. Литва запровадила окремий правовий режим для публічно-приватних проектів військової інфраструктури, що дозволяє прискорити процедури відбору партнерів при збереженні вимог безпеки.

Франція через Defence Code регулює концесійні угоди у оборонній сфері з чітким розмежуванням між публічними та приватними інтересами. Данія створила спеціальний правовий механізм для міжнародного співфінансування оборонних проектів третіх країн, що дозволило профінансувати закупівлю української оборонної продукції.

Воєнний стан вимагає адаптації класичних механізмів публічно-

приватного партнерства до швидкозмінних потреб оборони, де критичною стає оперативність прийняття рішень [37]. Необхідність створення спрощених процедур залучення приватного сектору до виконання оборонних замовлень при збереженні контролю та підзвітності стала очевидною у перші місяці повномасштабної війни, коли волонтерські організації та приватні компанії оперативніше забезпечували фронт, ніж державна система закупівель.

Конкретним прикладом є ситуація з закупівлею безпілотних літальних апаратів: державні процедури вимагали 3-6 місяців від оголошення тендеру до постачання, тоді як приватні виробники через волонтерські платформи забезпечували постачання за 2-4 тижні.

Фінансові механізми стимулювання приватних інвестицій у безпековий сектор мають стати потужним інструментом активізації партнерства. Система податкових стимулів, що включає звільнення від сплати податку на прибуток для компаній, які інвестують у проекти національної безпеки, зниження ставки податку на додану вартість на імпорту обладнання подвійного призначення та надання інвестиційних податкових кредитів для оборонних стартапів, може суттєво підвищити привабливість безпекового сектору для приватного капіталу [26]. Державні гарантії за кредитами приватних компаній, що реалізують проекти у сфері національної безпеки, здатні знизити фінансові ризики інвесторів, роблячи довгострокові інвестиції економічно виправданими навіть в умовах воєнної невизначеності.

Критичним елементом успішної активізації публічно-приватного партнерства є створення ефективної інституційної архітектури координації взаємодії між державою та бізнесом. Розпорошеність функцій між Міністерством оборони, Службою безпеки України, Міністерством внутрішніх справ, Державною службою спеціального зв'язку та іншими органами без єдиного координаційного центру призводить до дублювання зусиль та втрати синергії [57]. Створення спеціалізованого Координаційного центру публічно-приватного партнерства у сфері національної безпеки при Раді національної безпеки і оборони України з делегованими повноваженнями може забезпечити

методичний супровід PPP-проектів, проведення експертизи пропозицій від приватного сектору та моніторинг реалізації партнерських угод за єдиними стандартами.

Особлива увага має бути приділена механізмам кібербезпеки як найбільш перспективному напрямку публічно-приватного партнерства, що підтверджується як високим потенціалом українського ІТ-сектору, так і зростаючою інтенсивністю кібератак [69]. Створення національної платформи обміну інформацією про кіберзагрози між державними органами та приватними ІТ-компаніями на принципах конфіденційності, оперативності та взаємної довіри може суттєво підвищити рівень кіберзахисту критичної інфраструктури. Механізм спільних кіберучень за участю представників державного та приватного секторів дозволить відпрацювати координацію дій під час масштабних кібератак, що є особливо актуальним враховуючи досвід російських кібератак на українську енергетичну інфраструктуру у 2022-2024 роках.

Культурна трансформація відносин між державними органами безпеки та приватним сектором потребує системних довгострокових зусиль, оскільки традиційна недовіра та закритість безпекових структур гальмують розвиток ефективного партнерства [95]. Програми обміну персоналом, коли державні службовці безпекового сектору проходять стажування у провідних приватних компаніях, а представники бізнесу тимчасово залучаються до роботи у державних органах, можуть суттєво змінити сприйняття можливостей і обмежень кожного сектору. Конкретним прикладом успішності такого підходу є досвід співпраці Державної служби спеціального зв'язку з українськими ІТ-компаніями під час відбиття масованих російських кібератак у лютому-березні 2022 року, коли саме неформальна довіра між окремими фахівцями дозволила оперативно координувати захист критичної інфраструктури.

Міжнародна підтримка розвитку публічно-приватного партнерства у безпековій сфері може стати потужним каталізатором прискорення впровадження ефективних механізмів [23]. Створення міжнародного фонду підтримки публічно-приватного партнерства за участю країн-партнерів, який

надаватиме гранти та пільгові кредити для реалізації спільних проєктів, дозволить частково компенсувати обмеженість бюджетних ресурсів України в умовах війни. Данія вже створила прецедент, виділивши 28,5 мільйонів доларів на закупівлю українського озброєння, що фактично є формою міжнародного публічно-приватного партнерства через фінансування приватного оборонно-промислового комплексу третьої країни.

Інноваційний розвиток через створення спеціалізованих інвестиційних фондів для підтримки оборонних стартапів має стати важливим напрямком активізації публічно-приватного партнерства [44]. Досвід американського Defense Innovation Unit демонструє ефективність моделі, коли держава не лише замовляє готову продукцію, а й інвестує у ранні стадії розробки технологій подвійного призначення, отримуючи як інноваційні рішення для потреб безпеки, так і комерційно успішні продукти.

В українських умовах створення Національного фонду оборонних інновацій з паритетним фінансуванням від держави та приватних інвесторів могло б стимулювати розвиток власних технологій замість залежності від імпорту. Конкретним прикладом потреби у такому механізмі є ситуація з розробкою українських безпілотників: приватні стартапи створили конкурентоспроможні моделі FPV-дронів, які за ефективністю перевершують закордонні аналоги, однак відсутність системної державної підтримки на ранніх стадіях розробки уповільнила масове впровадження цих технологій.

Адаптивне управління PPP-проєктами в умовах невизначеності вимагає гнучкості умов партнерських угод з можливістю оперативного перегляду зобов'язань сторін у відповідь на зміни безпекової ситуації [100]. Досвід реалізації оборонних проєктів у 2022-2024 роках показав критичну важливість можливості коригувати терміни, обсяги та специфікації замовлень без розірвання контрактів. Приклад – компанії «Укроборонпром», яка змогла швидко переорієнтувати виробництво з планових ремонтів техніки на екстрену модернізацію бронетранспортерів для потреб фронту завдяки гнучким умовам державного замовлення, підтверджує ефективність адаптивного підходу.

Пілотні проекти як механізм апробації нових форм державно-приватної взаємодії дозволяють вивчити ефективність механізмів партнерства перед їх масштабуванням на всю безпекову сферу [21]. Рекомендується розпочати з невеликих пілотних ППП-проектів у кібербезпеці, логістиці для потреб оборони та розробці технологій подвійного призначення. Конкретним прикладом успішного пілотного проекту може бути створення регіонального центру кібербезпеки для західного регіону України на базі Львівської політехніки у партнерстві з провідними ІТ-компаніями, що дозволить відпрацювати модель галузевого центру перед його тиражуванням в інших регіонах.

Для систематизації проаналізованих механізмів активізації публічно-приватного партнерства у сфері національної безпеки та визначення пріоритетності їх впровадження доцільно структурувати ключову інформацію у вигляді комплексної таблиці. Така систематизація дозволяє наочно побачити взаємозв'язки між типами механізмів, конкретними інструментами їх реалізації, очікуваними результатами та рівнем пріоритетності впровадження, що є критично важливим для формування поетапної стратегії розвитку публічно-приватного партнерства у безпековій сфері України.

Таблиця 3.1 – Механізми активізації публічно-приватного партнерства у сфері національної безпеки України

<i>Тип механізму</i>	<i>Конкретні інструменти</i>	<i>Очікувані результати</i>	<i>Пріоритетність</i>	<i>Джерела</i>
Законодавчі механізми	Прийняття спеціального Закону про ППП у сфері нацбезпеки; нормативне врегулювання доступу до класифікованої інформації; процедури перевірки благонадійності	Правова визначеність для інвесторів; зниження юридичних ризиків; прозорість процедур	Критична (2025-2026)	[53; 107; 88]
Фінансові механізми	Податкові канікули для оборонних стартапів (3 роки); державні гарантії за кредитами; пільгове кредитування через УБРР; зниження ставки ПДВ на імпорт обладнання	Підвищення інвестиційної привабливості безпекового сектору; залучення приватного капіталу; зростання кількості проектів	Висока (2025-2027)	[26; 44]

Продовження таблиці 3.1

<i>Тип механізму</i>	<i>Конкретні інструменти</i>	<i>Очікувані результати</i>	<i>Пріоритетність</i>	<i>Джерела</i>
Інституційні механізми	Створення Координаційного центру ППП при РНБО; міжвідомча робоча група; електронна система управління проектами; регулярні консультації держава-бізнес	Координація зусиль різних відомств; усунення дублювання; підвищення ефективності взаємодії	Висока (2025-2026)	[57; 95]
Механізми кібербезпеки	Національна платформа обміну інформацією про кіберзагрози; спільні кіберучення; акредитація постачальників послуг кіберзахисту; галузеві центри кібербезпеки	Підвищення рівня кіберзахисту критичної інфраструктури; оперативне реагування на інциденти	Критична (2025-2026)	[69; 54]
Механізми екстреної мобілізації	Рамкові угоди з приватними компаніями; спрощені процедури залучення; резервний фонд для екстреного фінансування; прискорені процедури держзакупівель	Швидке залучення приватних потужностей в кризових ситуаціях; гнучкість реагування на загрози	Висока (2025-2026)	[37; 46]
Механізми культурної трансформації	Програми обміну персоналом держава-бізнес; спільні навчання та тренінги; публічні форуми для діалогу; інформаційні кампанії	Подолання недовіри між секторами; формування культури партнерства; взаємне розуміння специфіки	Середня (2026-2028)	[95; 100]
Механізми міжнародної підтримки	Міжнародний фонд підтримки ППП; співфінансування проектів країнами-партнерами; технічна допомога міжнародних організацій	Залучення додаткових фінансових ресурсів; трансфер технологій та досвіду; інтеграція в міжнародні мережі	Середня (2026-2027)	[23; 21]
Механізми інноваційного розвитку	Національний фонд оборонних інновацій; гранти на дослідження; пілотні проекти; інкубатори оборонних стартапів	Стимулювання інновацій у безпековій сфері; розвиток технологій подвійного призначення	Висока (2025-2027)	[44; 21; 77]

Джерело: розробка автора

Аналіз механізмів активізації публічно-приватного партнерства у сфері національної безпеки дозволяє сформулювати стратегію поетапного впровадження з урахуванням критичності, ресурсної забезпеченості та часових

рамках реалізації. Критична пріоритетність законодавчих механізмів обумовлена тим, що правова визначеність є базовою передумовою для всіх інших форм державно-приватної взаємодії – без чіткого законодавчого врегулювання процедур, прав та обов'язків сторін бізнес не готовий робити довгострокові інвестиції у високоризиковий безпековий сектор. Досвід показує, що навіть за наявності значного потенціалу для партнерства, як у випадку з українським ІТ-сектором у кібербезпеці, відсутність спеціального законодавства обмежує масштаби співпраці неформальними домовленостями, які не можуть замінити інституціоналізованих механізмів.

Паралельне впровадження інституційних та фінансових механізмів є логічним наступним кроком після створення законодавчої основи. Координаційний центр при РНБО не лише забезпечить організаційну основу для управління ППП-проектами, але й стане єдиною точкою входу для приватного сектору, усуваючи поточну проблему розпорошеності функцій між численними відомствами. Податкові стимули та державні гарантії мають працювати синхронно з інституційними змінами: створення найкращої організаційної структури не призведе до масового залучення приватного капіталу, якщо інвестиції у безпековий сектор залишатимуться економічно не вигідними порівняно з комерційними проектами.

Особлива увага до механізмів кібербезпеки та екстреної мобілізації обумовлена не лише їх критичною важливістю для національної безпеки, але й можливістю швидкої реалізації. Український ІТ-сектор вже демонструє високу готовність до партнерства з державою, що підтверджується численними прикладами ефективної співпраці під час відбиття кібератак. Механізми екстреної мобілізації, апробовані у перші місяці повномасштабної війни через волонтерські ініціативи, можуть бути формалізовані та інституціоналізовані відносно швидко, оскільки вже існує практичний досвід такої взаємодії.

Механізми культурної трансформації, хоча й мають середню пріоритетність за терміновістю, є критично важливими для довгострокового успіху всієї системи публічно-приватного партнерства. Без подолання взаємної

недовіри між державними органами безпеки та приватним сектором, без формування спільної культури партнерства навіть найкращі законодавчі та фінансові механізми працюватимуть неефективно. Досвід успішних моделей публічно-приватного партнерства у інших країнах, зокрема в Естонії, демонструє, що культура довіри між секторами є такою ж важливою передумовою ефективного партнерства, як і правове регулювання чи фінансові стимули.

Міжнародна підтримка та інноваційні механізми мають середню пріоритетність, оскільки їх реалізація вимагає додаткового часу на переговори з міжнародними партнерами та створення складніших інституційних структур. Однак ці напрямки є критично важливими для довгострокової стійкості системи публічно-приватного партнерства, оскільки дозволяють залучити додаткові фінансові ресурси та технологічну експертизу, компенсуючи обмеженість бюджетних можливостей України в умовах війни. Створення Національного фонду оборонних інновацій за участю міжнародних інвесторів може стати механізмом не лише фінансування розробки технологій, але й інтеграції українського оборонно-промислового комплексу до міжнародних мереж кооперації.

Таким чином, пріоритетні напрями активізації публічно-приватного партнерства у сфері національної безпеки України охоплюють комплекс законодавчих, фінансових, інституційних та культурних механізмів, впровадження яких має здійснюватися поетапно з урахуванням критичності та терміновості кожного напрямку.

Законодавчі механізми через прийняття спеціального Закону про публічно-приватне партнерство у сфері національної безпеки та нормативне врегулювання специфічних питань доступу до класифікованої інформації мають критичну пріоритетність як базова передумова всіх інших форм партнерства. Інституційні механізми через створення

Координаційного центру публічно-приватного партнерства при РНБО та міжвідомчої робочої групи забезпечують організаційну основу для ефективної

координації взаємодії між державними органами безпеки та приватним сектором.

Механізми кібербезпеки через національну платформу обміну інформацією про кіберзагрози та галузеві центри кібербезпеки віднесено до критичної пріоритетності через зростаючу інтенсивність кібератак та високий потенціал українського ІТ-сектору для швидкої реалізації цих ініціатив.

Фінансові механізми стимулювання через податкові канікули, державні гарантії та пільгове кредитування мають високу пріоритетність для підвищення інвестиційної привабливості безпекового сектору, тоді як механізми культурної трансформації через програми обміну персоналом та спільні навчання вимагають довгострокових систематичних зусиль для формування культури довіри між державою та бізнесом.

3.2 Перспективи та рекомендації щодо розвитку публічно-приватного партнерства у сфері забезпечення національної безпеки України

Визначивши у попередньому підрозділі пріоритетні напрями активізації публічно-приватного партнерства, доцільно буде перейти до формування конкретних перспектив та обґрунтованих рекомендацій щодо розвитку державно-приватної взаємодії у безпековій сфері.

Україна перебуває на критичному етапі трансформації системи національної безпеки, коли повномасштабна війна одночасно створює безпрецедентний попит на швидке залучення приватних ресурсів і загрожує хаотизацією цього процесу через відсутність належної інституційної інфраструктури.

Аналіз сучасних тенденцій розвитку публічно-приватного партнерства у сфері національної безпеки дозволяє стверджувати, що успіх трансформації залежить від комплексного підходу, який охоплює законодавчі, фінансові,

інституційні та культурні виміри [53; 107; 37]. Першочерговою рекомендацією має стати прийняття спеціального Закону України «Про публічно-приватне партнерство у сфері національної безпеки» протягом 2025-2026 років, оскільки саме цей нормативний акт створить правову визначеність для інвесторів та встановить прозорі процедури реалізації партнерських проектів.

Критично важливим є включення до законодавства спеціальних норм щодо режиму доступу приватних партнерів до класифікованої інформації, механізмів перевірки благонадійності учасників та процедур захисту інвестицій у стратегічно важливі об'єкти. Конкретним прикладом необхідності такого регулювання є ситуація з приватними виробниками безпілотників, які потребують доступу до тактичної інформації для розробки ефективних рішень, однак чинне законодавство не передбачає оперативних механізмів надання такого доступу без тривалих процедур отримання державних допусків.

Фінансові механізми стимулювання приватних інвестицій потребують радикального переосмислення підходів до оподаткування та державної підтримки проектів національної безпеки [26; 44]. Запровадження нульової ставки податку на прибуток для компаній, що реалізують ППП-проекти у безпековій сфері протягом перших трьох років, може суттєво підвищити привабливість цього сектору для бізнесу.

Зниження ставки ПДВ до 7% на імпорт обладнання та технологій подвійного призначення для оборонних підприємств, що працюють у рамках партнерства, дозволить знизити вхідні бар'єри для інвестицій. Створення при Українському банку реконструкції та розвитку спеціалізованої кредитної лінії для фінансування ППП-проектів з пільговою процентною ставкою 5% річних та можливістю відстрочення погашення основної суми боргу має стати потужним інструментом підтримки довгострокових інвестицій в умовах високих ризиків.

Система державних гарантій, що покривають до 50% кредитних зобов'язань приватних компаній, які реалізують стратегічно важливі проекти у оборонно-промисловому комплексі, може стати ключовим механізмом зниження фінансових ризиків інвесторів. Досвід показує, що навіть найбільш технологічно

спроможні українські компанії стикаються з труднощами у залученні комерційного фінансування для оборонних проектів через високу невизначеність воєнного часу та тривалі терміни окупності інвестицій.

Інституційна архітектура координації публічно-приватного партнерства потребує створення спеціалізованих структур з чітко визначеними повноваженнями та відповідальністю [57; 46]. Утворення Координаційного центру публічно-приватного партнерства у сфері національної безпеки як постійно діючого структурного підрозділу апарату РНБО з чисельністю не менше 15 штатних працівників має забезпечити централізоване управління процесами державно-приватної взаємодії. Цей центр має здійснювати експертизу всіх пропозицій щодо ППП-проектів, координувати діяльність різних органів сектору безпеки, вести єдиний електронний реєстр проектів та щоквартально звітувати перед РНБО про стан реалізації партнерських ініціатив.

Створення міжвідомчої робочої групи з питань публічно-приватного партнерства під головуванням Секретаря РНБО з обов'язковою участю заступників керівників ключових органів сектору безпеки, представників Міністерства економіки, Міністерства фінансів та трьох найбільших приватних компаній оборонно-промислового комплексу і ІТ-сектору забезпечить регулярний діалог між державою та бізнесом. Засідання цієї робочої групи щонайменше раз на квартал дозволять оперативно виявляти проблеми, узгоджувати позиції та формувати спільні рішення щодо розвитку партнерства.

Розробка та затвердження Національної стратегії публічно-приватного партнерства у сфері національної безпеки на період до 2030 року має визначити довгострокові цілі та етапи розвитку державно-приватної взаємодії [46; 77]. Ця стратегія має передбачати три послідовні фази реалізації: невідкладний етап (2025-2026 роки) для створення правової та інституційної основи, середньостроковий етап (2027-2028 роки) для масштабування пілотних проектів та формування культури партнерства, довгостроковий етап (2029-2030 роки) для інтеграції українських моделей публічно-приватного партнерства у міжнародні стандарти НАТО та ЄС.

Особлива увага має бути приділена розвитку публічно-приватного партнерства у сфері кібербезпеки як найбільш перспективного напрямку державно-приватної взаємодії [69; 54]. Створення Національної платформи обміну інформацією про кіберзагрози на базі Державної служби спеціального зв'язку з обов'язковою участю представників провідних ІТ-компаній, операторів критичної інфраструктури та академічних установ дозволить підвищити рівень кіберзахисту держави. Система безпечного обміну індикаторами компрометації та інформацією про виявлені вразливості між державними органами та приватним сектором у режимі реального часу з використанням сучасних криптографічних протоколів має стати стандартом взаємодії.

Галузеві інформаційно-аналітичні центри кібербезпеки для критичних секторів економіки – енергетики, транспорту, фінансового сектору та телекомунікацій – мають функціонувати на засадах публічно-приватного партнерства з паритетним фінансуванням 50% від держави та 50% від приватних операторів галузі. Конкретним прикладом реалізації такого підходу може стати створення Центру кібербезпеки енергетичної інфраструктури за участю Міністерства енергетики, Державної служби спеціального зв'язку та провідних енергетичних компаній для координації захисту від кібератак на об'єкти генерації та розподілу електроенергії.

Запровадження обов'язкових щорічних спільних кібернавчань за участю представників державних органів та приватних компаній для відпрацювання координації дій під час масштабних кібератак на критичну інфраструктуру має стати регулярною практикою. Досвід показує, що саме під час таких навчань виявляються прогалини у взаємодії та формуються неформальні зв'язки між фахівцями, які потім забезпечують ефективну координацію в реальних кризових ситуаціях.

Культурна трансформація відносин між державою та бізнесом у безпековій сфері потребує системних довгострокових зусиль [95; 100]. Програма «Безпека через партнерство», у рамках якої щорічно 20 державних службовців органів сектору безпеки проходять тримісячне стажування у провідних приватних

компаніях, а 20 представників бізнесу тимчасово залучатимуться до роботи у державних органах, може суттєво змінити взаємне сприйняття можливостей і обмежень кожного сектору.

Проведення щорічного Національного форуму публічно-приватного партнерства у сфері національної безпеки за участю керівництва органів сектору безпеки, представників бізнесу, науковців та міжнародних експертів створить постійно діючу платформу для діалогу та обміну досвідом.

Міжнародна підтримка розвитку публічно-приватного партнерства може стати потужним каталізатором прискорення впровадження ефективних механізмів [23; 21]. Ініціювання створення Міжнародного фонду підтримки публічно-приватного партнерства у сфері національної безпеки України за участю США, Великобританії, Канади, Польщі та країн Балтії з можливістю надання грантів до 5 мільйонів доларів на реалізацію інноваційних проектів дозволить частково компенсувати обмеженість бюджетних ресурсів.

Конкретним прикладом може стати фінансування спільного українсько-польсько-балтійського проекту створення виробництва безпілотних літальних апаратів, де українська держава забезпечує регуляторну підтримку та гарантований обсяг закупівель, українські приватні компанії надають технологічну експертизу, польські партнери забезпечують доступ до ринків НАТО, а балтійські країни інвестують у виробничі потужності.

Створення Національного фонду оборонних інновацій як публічно-приватної інституції з початковим капіталом 100 мільйонів доларів, де 60% фінансування надходить від держави та 40% від приватних інвесторів, має стимулювати розвиток власних технологій подвійного призначення [44]. Цей фонд має інвестувати у стартапи на ранніх стадіях розробки, надавати гранти на дослідження розміром від 50 до 500 тисяч доларів та виступати співінвестором комерційних проектів з оборонним потенціалом.

Реалізація пілотних проектів у трьох ключових напрямках дозволить апробувати механізми партнерства перед їх масштабуванням [21]. По-перше, створення регіонального центру кібербезпеки для західного регіону України на

базі Львівської політехніки у партнерстві з провідними ІТ-компаніями для відпрацювання моделі галузевого центру. По-друге, реалізація пілотного проекту з логістичного забезпечення Збройних Сил у партнерстві з міжнародною логістичною компанією для впровадження сучасних технологій управління ланцюгами постачання. По-третє, створення інкубатора оборонних стартапів при одному з провідних технічних університетів для підтримки молодих підприємців, що розробляють інноваційні рішення для потреб безпеки.

Для оцінки перспектив розвитку публічно-приватного партнерства у сфері національної безпеки України доцільно використати комплексний набір критеріїв, що охоплюють різні виміри ефективності партнерської взаємодії.

Перший критерій: правова забезпеченість – передбачає оцінку наявності спеціалізованого законодавства, повноти нормативного регулювання та ступеня адаптації правових норм до специфіки безпекового сектору.

Другий критерій: інституційна спроможність – характеризується наявністю спеціалізованих координаційних структур, професіоналізмом кадрів та ефективністю механізмів міжвідомчої координації.

Третій критерій: фінансова привабливість – оцінюється через наявність податкових стимулів, державних гарантій, обсяги залучених приватних інвестицій та економічну ефективність реалізованих проектів.

Четвертий критерій: рівень довіри – характеризує якість культурної взаємодії між державою та бізнесом через показники співпраці, інтенсивність обміну інформацією та успішність спільних ініціатив.

П'ятий критерій: інноваційність – відображає здатність системи публічно-приватного партнерства генерувати технологічні прориви, кількість підтриманих стартапів та впровадження нових рішень у безпековій сфері.

Шостий критерій: міжнародна інтегрованість – оцінює ступінь відповідності українських практик публічно-приватного партнерства стандартам НАТО та ЄС, обсяги міжнародного фінансування та участь у міжнародних проектах.

На основі цих критеріїв можна окреслити реалістичні перспективи

розвитку публічно-приватного партнерства у трьох часових горизонтах [77]. У короткостроковій перспективі (2025-2027 роки) очікується створення правової та інституційної основи через прийняття спеціального закону, створення Координаційного центру, запровадження базових фінансових стимулів та реалізацію пілотних проектів. Критерії правової забезпеченості та інституційної спроможності мають досягти середнього рівня, тоді як фінансова привабливість та рівень довіри залишатимуться на стадії формування.

У середньостроковій перспективі (2028-2030 роки) прогнозується масштабування успішних моделей партнерства, суттєве зростання обсягів приватних інвестицій у безпековий сектор та інтеграція українських практик публічно-приватного партнерства у стандарти НАТО. Критерії фінансової привабливості та інноваційності мають досягти високого рівня, а рівень довіри між державою та бізнесом – переходити від формальної взаємодії до справжнього партнерства. Міжнародна інтегрованість має зрости через активну участь України у спільних оборонних проектах країн-партнерів та залучення значних обсягів міжнародного фінансування.

У довгостроковій перспективі (після 2030 року) публічно-приватне партнерство має трансформуватися у основну модель фінансування та реалізації проектів у сфері національної безпеки України, забезпечуючи стійкість оборонно-промислового комплексу та кіберстійкість держави.

Усі шість критеріїв мають досягти високого рівня розвитку, коли правова забезпеченість, інституційна спроможність, фінансова привабливість, рівень довіри, інноваційність та міжнародна інтегрованість формують зрілу екосистему публічно-приватного партнерства, здатну ефективно реагувати на нові виклики національній безпеці.

Критично важливою перспективою є повна інтеграція українських моделей публічно-приватного партнерства у безпековій сфері до стандартів НАТО та ЄС, що відкриє доступ до міжнародних програм фінансування, технічної допомоги та спільних проектів з країнами-членами Альянсу. Україна має активно позиціонувати публічно-приватне партнерство як ключовий

механізм міжнародної кооперації у безпековій сфері, демонструючи власні успіхи та готовність до співпраці.

Резюмуємо: Перспективи розвитку публічно-приватного партнерства у сфері національної безпеки України визначаються комплексним підходом до впровадження рекомендацій законодавчого, фінансового, інституційного та культурного характеру з використанням шести ключових критеріїв оцінки: правової забезпеченості, інституційної спроможності, фінансової привабливості, рівня довіри, інноваційності та міжнародної інтегрованості.

Першочерговими рекомендаціями є прийняття спеціального закону протягом 2025-2026 років, створення Координаційного центру при РНБО, запровадження нульової ставки податку на прибуток для ППП-проектів, створення спеціалізованої кредитної лінії при УБРР та формування системи державних гарантій.

Специфічні рекомендації для кібербезпеки включають створення Національної платформи обміну інформацією про кіберзагрози, галузевих центрів кібербезпеки з паритетним фінансуванням та обов'язкові щорічні спільні кіберучення, що дозволить підвищити рівень захисту критичної інфраструктури.

Перспективи розвитку визначаються трифазовою моделлю з короткостроковою фазою (2025-2027) створення правової основи та пілотних проектів, середньостроковою фазою (2028-2030) масштабування успішних моделей та зростання приватних інвестицій, довгостроковою фазою (після 2030) трансформації публічно-приватного партнерства у основну модель фінансування проектів національної безпеки з повною інтеграцією до євроатлантичних структур безпеки.

ВИСНОВКИ

За результатами дослідження сформульовано нижченаведені основні висновки та пропозиції:

1. Теоретико-методологічні засади публічно-приватного партнерства у сфері національної безпеки формують концептуальний фундамент для розуміння ролі, функцій та механізмів взаємодії державного та приватного секторів у забезпеченні безпеки держави. Концептуальний аналіз засвідчує еволюцію підходів від державоцентричної парадигми до інтегрованої моделі, де приватний сектор виступає стратегічним партнером у співтворенні національної безпеки через ресурсні, інноваційні та координаційні функції.

Міжнародний досвід демонструє різноманітність організаційних моделей публічно-приватного партнерства у безпековій сфері – від охорони критичної інфраструктури до оборонних інновацій, що адаптуються до специфічних національних контекстів та інституційних традицій.

2. Правові та інституційні засади публічно-приватного партнерства у сфері національної безпеки України характеризуються недостатньою розвиненістю та фрагментарністю регулювання. Відсутність спеціального законодавства, неузгодженість нормативних актів, слабкість інституційної координації та обмеженість механізмів державної підтримки створюють бар'єри для ефективного розвитку партнерства між державою та бізнесом у безпековій сфері.

Водночас повномасштабна війна продемонструвала величезний потенціал приватної ініціативи та необхідність системної інституціоналізації державно-приватної взаємодії через створення відповідної правової бази, координаційних структур та механізмів стимулювання приватних інвестицій у національну безпеку. Вдосконалення теоретико-методологічних, правових та інституційних засад публічно-приватного партнерства у сфері національної безпеки є критично важливим для посилення обороноздатності України, ефективного використання

ресурсів суспільства та забезпечення довгострокової безпекової стійкості держави.

3. Аналіз практики реалізації публічно-приватного партнерства у сфері національної безпеки на міжнародному та національному рівнях дозволяє сформулювати ключові висновки щодо ефективних моделей взаємодії та критичних викликів, що стоять перед Україною. Міжнародний досвід, систематизований на основі досліджень провідних науковців, демонструє, що успішне публічно-приватного партнерства у безпековій сфері вимагає не лише фінансових ресурсів, але й чіткого правового регулювання, інституційної спроможності для координації, професійних кадрів та культури довіри між державою та бізнесом, при цьому кожна країна адаптує моделі партнерства до власних інституційних особливостей та специфіки загроз.

Польська динамічна модель екстреного реагування з триетапною стратегією закупівель є найбільш придатною для впровадження в Україні через прагматичний баланс між швидкістю постачання та передачею технологій, тоді як естонська модель кіберпартнерства може бути успішно адаптована для використання потенціалу українського ІТ-сектору.

4. Стан публічно-приватного партнерства у сфері національної безпеки України характеризується парадоксальною ситуацією, коли потужний потенціал приватної ініціативи, що проявився через волонтерський рух та оборонні стартапи, не отримує належної інституційної підтримки через критичні прогалини у правовому регулюванні, відсутність координаційних структур, брак фінансових стимулів та культурні бар'єри недовіри між державними органами безпеки та бізнесом.

Подолання системних проблем вимагає комплексного підходу через прийняття спеціального законодавства про публічно-приватне партнерство у безпековій сфері, створення Координаційного центру при РНБО, запровадження податкових пільг та державних гарантій для оборонних стартапів, формування культури довіри через програми обміну та діалогу, а також посилення прозорості оборонних закупівель через електронізацію та незалежний аудит, що дозволить

трансформувати стихійну приватну ініціативу у стійку систему публічно-приватної взаємодії для довгострокового посилення обороноздатності України.

5. Механізми вдосконалення та перспективи розвитку публічно-приватного партнерства у сфері національної безпеки України формують комплексну систему заходів, впровадження яких має здійснюватися поетапно з урахуванням критичності та терміновості кожного напрямку.

Пріоритетні напрями активізації публічно-приватного партнерства включають законодавчі механізми через прийняття спеціального Закону про публічно-приватне партнерство у сфері національної безпеки як базової передумови всіх інших форм партнерства, фінансові механізми через податкові канікули та державні гарантії для підвищення інвестиційної привабливості безпекового сектору, інституційні механізми через створення Координаційного центру при РНБО для ефективної координації взаємодії та механізми кібербезпеки через національну платформу обміну інформацією про кіберзагрози.

6. Конкретні рекомендації щодо розвитку публічно-приватного партнерства передбачають прийняття спеціального закону протягом 2025-2026 років, внесення змін до Податкового кодексу для запровадження нульової ставки податку на прибуток для ППП-проектів протягом трьох років, створення спеціалізованої кредитної лінії при УБРР з пільговою ставкою 5% річних, утворення Координаційного центру публічно-приватного партнерства з чисельністю не менше 15 штатних працівників та запровадження програм обміну персоналом між державою та бізнесом.

7. Для оцінки перспектив розвитку використано шість критеріїв: правова забезпеченість, інституційна спроможність, фінансова привабливість, рівень довіри, інноваційність та міжнародна інтегрованість, які дозволяють комплексно оцінити ефективність впровадження механізмів публічно-приватного партнерства.

Перспективи розвитку публічно-приватного партнерства визначаються трифазовою моделлю: короткострокова фаза (2025-2027 роки) створення

правової та інституційної основи через прийняття спеціального закону, створення Координаційного центру та реалізацію пілотних проектів у кібербезпеці, логістиці та інкубації оборонних стартапів; середньострокова фаза (2028-2030 роки) масштабування успішних моделей партнерства, суттєве зростання обсягів приватних інвестицій у безпековий сектор та інтеграція українських практик публічно-приватного партнерства у стандарти НАТО; довгострокова фаза (після 2030 року) трансформації публічно-приватного партнерства у основну модель фінансування та реалізації проектів у сфері національної безпеки України з повною інтеграцією до євроатлантичних структур безпеки та досягненням високого рівня за всіма шістьма критеріями оцінки ефективності партнерської взаємодії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Annual Report on Major Projects 2022-23. UK IPA, 2023. URL: <https://assets.publishing.service.gov.uk/media/64c91eaed8b1a71e86b05df3/IPA-Annual-report-2022-2023.pdf.pdf> (Last accessed: 28.10.2025).
2. Between Now and NATO: A Security Strategy for Ukraine. CEPA, January 2025. URL: <https://cepa.org/comprehensive-reports/between-now-and-nato-a-security-strategy-for-ukraine/> (Last accessed: 04.10.2025).
3. CEGELOG. Balard-Défense: оборонні проекти ДПП у Франції (приклад Європейського інвестиційного банку). Париж : CEGELOG, 2024. 67 с.
4. Comprehensive Assistance Package for Ukraine. NATO, 2024. URL: https://www.nato.int/cps/en/natohq/topics_231639.htm (Last accessed: 04.10.2025).
5. Cybersecurity 2023: trends and prospects. National Cybersecurity Cluster, 13 March 2023. URL: <https://cybersecuritycluster.org.ua/en/events/17th-cluster-session-cybersecurity-2023-trends-new-opportunities-and-prospects/> (Last accessed: 20.10.2025).
6. Defence ministers address strengthening NATO's deterrence. NATO, 15 February 2024. URL: https://www.nato.int/cps/en/natohq/news_222622.htm (Last accessed: 13.10.2025).
7. ECSA-CERBERUS, Griffin, ProtectUK : український аспект моделей співпраці у сфері безпеки : збірник матеріалів міжнародної конференції / упоряд. Т.В. Семенюк. Київ : НІСД, 2024. 234 с.
8. Griffin, ECSA-CERBERUS, ProtectUK: міжнародні проекти публічно-приватного партнерства у безпековій сфері : компаративний аналіз / за ред. Дж. Томпсона. Лондон : Security Studies Press, 2024. 198 с.
9. NATO and Ukraine start major defence procurement review. NATO, 18 March 2024. URL: https://www.nato.int/cps/en/natohq/news_223818.htm (Last accessed: 12.10.2025).
10. NATO Defence Ministers to advance work on deterrence and defence.

NATO, 16 October 2024. URL: https://www.nato.int/cps/en/natohq/news_229538.htm (Last accessed: 12.10.2025).

11. NATO Relations with Ukraine. NATO, 2025. URL: https://www.nato.int/cps/en/natohq/topics_37750.htm (Last accessed: 12.10.2025).

12. NATO's partnerships. NATO, 2024. URL: https://www.nato.int/cps/en/natohq/topics_84336.htm (Last accessed: 18.10.2025).

13. PPP & Concessions: French experience. France, 2022.

14. Review of the European PPP market 2023. European Investment Bank, 2024. URL: https://www.eib.org/attachments/lucalli/20240030_epec_market_update_2023_en.pdf (Last accessed: 18.10.2025).

15. Sychova V., Samofalova T. Private-Public Partnership in the Post-War Reconstruction of Ukraine. *State Formation*. 2023. No. 2. P. 125–141. DOI: <https://doi.org/10.26565/1992-2337-2023-2-10> (Last accessed: 18.10.2025).

16. Tanvir U. Public-Private Partnerships as Catalysts for Digital Transformation in Security Sector. *ScienceDirect*. 2025. Vol. 45. P. 234–247. DOI: [10.1016/j.giq.2025.101789](https://doi.org/10.1016/j.giq.2025.101789).

17. The Secretary General's Annual Report 2024. NATO, 2025. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2025/4/pdf/sgar24-en.pdf (Last accessed: 18.10.2025).

18. Tsiuman Y.S. Public-Private Partnership as a Mechanism Providing Sustainable Development for the Recovery of the Country. *Collection of scientific publications NUS*. 2023. Vol. 490, no. 1. P. 227–234. DOI: [https://doi.org/10.15589/znp2023.1\(490\).27](https://doi.org/10.15589/znp2023.1(490).27) (Last accessed: 18.10.2025).

19. UK defence spending. House of Commons Library, 2024. 24 p. URL: <https://researchbriefings.files.parliament.uk/documents/CBP-8175/CBP-8175.pdf> (Last accessed: 18.10.2025).

20. Ukraine-NATO relations. Wikipedia, October 2025. URL: https://en.wikipedia.org/wiki/Ukraine-NATO_relations (Last accessed: 18.10.2025).

21. Адаптація міжнародного досвіду публічно-приватного партнерства у сфері національної безпеки до українських реалій (2022-2024) : науково-

аналітична записка / Центр досліджень армії, конверсії та роззброєння ; авт.: В.М. Бегма, Т.О. Чмут, І.С. Руснак. Київ : ЦДАКР, 2024. 145 с.

22. Академія Публічно-Приватного Партнерства, 2025. URL: <https://appp.com.ua/en/> (дата звернення: 20.10.2025).

23. Аналітичні звіти міжнародних організацій щодо публічно-приватного партнерства у сфері безпеки: адаптація до України (2022-2025) : збірник матеріалів / упоряд. В.П. Горбулін, О.С. Власюк. Київ : НІСД, 2025. 289 с.

24. Військово-промисловий комплекс: державний чи приватний? CASE Україна, 21 вересня 2023. URL: <https://case-ukraine.com.ua/publications/vijskovo-promyslovyj-kompleks-derzhavnyj-chy-pryvatnyj/> (дата звернення: 07.10.2025).

25. Всесвітній економічний форум. Розвиток кіберталантів через державно-приватне партнерство: глобальні тренди. Женева : WEF, 2025. 124 с.

26. Гуменюк Д.М. Механізм публічно-приватного партнерства в реалізації інфраструктурних проектів: вдосконалення нормативної бази. Інвестиції: практика та досвід. 2024. № 5. С. 67–74. DOI: 10.32702/2306-6814.2024.5.67.

27. Державно-приватне партнерство в контексті попередження та реагування на надзвичайні ситуації: міжнародний досвід, проблеми та перспективи для України: аналітична записка / Національний інститут стратегічних досліджень, 2023. URL: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/derzhavno-privatne-partnerstvo-v-konteksti-poperedzhennya-ta> (дата звернення: 03.10.2025).

28. Державно-приватне партнерство в секторі безпеки України: основні принципи та форми. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2025. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/273697> (дата звернення: 02.10.2025).

29. Державно-приватне партнерство у сфері кібербезпеки в Україні. U.P.M.P., 26 квітня 2018. URL: https://upmp.news/post_blog/derzhavno-privatne-partnerstvo-u-sferi-kiberbezpeki-v-ukrayini/ (дата звернення: 11.10.2025).

30. Державно-приватне партнерство у сфері кібербезпеки. *National Institute for Strategic Studies*, 2018. URL: <https://niss.gov.ua/en/node/123> (дата звернення: 10.10.2025).

31. Державно-приватне партнерство у сфері кібербезпеки: що планується впровадити? / DTKT News, 19 вересня 2024. URL: <https://news.dtki.ua/state/other/93302> (дата звернення: 10.10.2025).

32. Державно-приватне партнерство як інструмент залучення ресурсів приватного сектору / Міністерство економіки України, 2024. URL: <https://me.gov.ua/Documents/Detail?lang=uk-UA&id=196d3373-eb07-4834-a61e-b3608f28eb22> (дата звернення: 05.10.2025).

33. Державно-приватне партнерство як механізм реалізації нової регіональної політики / U-LEAD, 2017. URL: http://rdpa.regionet.org.ua/images/129/PPP_report_U-LEAD_30_10_2017.pdf (дата звернення: 06.10.2025).

34. Державно-приватне партнерство: нормативне регулювання та фінансові механізми / О.М. Непомнящий та ін. Журнали Вернадського : Публічне управління та адміністрування. 2024. Вип. 23. С. 89–98.

35. Деякі питання організації ДПП : Постанова КМУ від 11.04.2011 № 384. URL: <https://zakon.rada.gov.ua/laws/show/384-2011-p> (дата звернення: 22.10.2025).

36. Дідич О.Р. Державно-приватне партнерство у забезпеченні національної безпеки України в умовах воєнного стану. *Публічне управління та митне адміністрування*. 2024. № 2(41). С. 67–76.

37. Дідич О.Р. Державно-приватне партнерство у забезпеченні національної безпеки України в умовах війни: виклики та можливості. *Вісник Національного університету цивільного захисту України*. Серія : Державне управління. 2023. Вип. 2(19). С. 89-98.

38. ДЛФ. Публічно-приватне партнерство в Україні – нові правила 2025: практичний коментар до законодавства. Київ : DLF Attorneys-at-law, 2025. 89 с.

39. Дослідження REICST про моделі реалізації державно-приватного

партнерства у безпековій сфері : аналітичний звіт / Дослідницький інститут економіки та безпеки ; наук. ред. В.П. Горбулін. Київ : REICST, 2024. 167 с.

40. Дослідження щодо особливостей державно-приватного партнерства у сфері кібербезпеки : науковий звіт / Рада досліджень безпеки і оборони ; кер. проекту О.В. Литвиненко. Київ : РДБО, 2024. 134 с.

41. Дубов Д. (ред.) Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. Київ: НІСД, 2018. 84 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvratn_partnerstvo_Ciberbezpeka.pdf (дата звернення: 09.10.2025).

42. Європейський інвестиційний банк. Державно-приватне партнерство у сфері безпеки та оборони: аналітичний звіт. Люксембург : ЕІВ, 2025. 156 с.

43. Європейський інвестиційний банк. Нові державно-приватні партнерства у сфері безпеки в Данії, Великій Британії та ЄС. Люксембург : ЕІВ, 2025. 78 с.

44. Залучення приватного капіталу в оборонну галузь та національну безпеку: рекомендації та механізми : аналітична доповідь / авт. кол.: С.І. Пирожков, О.М. Суходоля, Г.М. Перепелиця та ін. ; Національна академія наук України, Інститут економіки промисловості. Київ : НАН України, 2024. 178 с.

45. Ільїна А. Особливості стратегії національної безпеки. *Шевченківська весна – 2024: публічне управління та державна служба*: матеріали щоріч. Всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених. Київ: ННІ ПУДС КНУ, 2024. С. 128-129.

46. Квеліашвілі І.М. Механізми публічного управління в умовах воєнного часу: трансформація взаємодії держави та бізнесу. *Аспекти публічного управління*. 2024. Т. 12. № 2. С. 78–87. DOI: 10.15421/152411.

47. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр> (дата звернення: 14.10.2025).

48. Кудінов С. Міжнародний досвід партнерства приватних компаній у

сфері національної безпеки. *Державне управління та місцеве самоврядування*. 2023. № 4. С. 45-52.

49. Кудінов С.С. Державно-приватне партнерство у сфері національної безпеки: волонтерський рух та приватні ініціативи. *Аспекти публічного управління*. 2024. Т. 12. № 4. С. 56-67.

50. Кучеренко В.О. Міжнародний та вітчизняний досвід державно-приватного партнерства у сфері охорони та безпеки. *Економіка та держава*. 2024. № 6. С. 112-118.

51. Лаврентій Д.С. Європейський досвід публічно-приватного партнерства у оборонній сфері. *Науковий вісник Академії муніципального управління*. Серія : Управління. 2024. Вип. 2. С. 56–65.

52. Маркієва О. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід Естонії та Ізраїлю. *Підприємництво, господарство і право*. 2024. № 5. С. 134-141.

53. Маркієва О. Теоретичні підходи до державно-приватного партнерства у сфері національної безпеки. *Публічне управління та адміністрування в Україні*. 2022. Вип. 28. С. 45-51. DOI: 10.32843/2663-5240-2022-28-8.

54. Методи активізації публічно-приватного партнерства у сфері кібербезпеки : збірник наукових статей за матеріалами журналів «Кібербезпека в Україні» та «Information Security» (2023-2025) / уклад. Д.В. Дубов. Київ : ДП «НВЦ «Євроатлантикінформ», 2025. 234 с.

55. Методичні рекомендації ДПП. Міністерство економіки України, 2024. URL: <https://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=2bc79196-a3b2-41a9-86e2-f55f9a8f5c9c> (дата звернення: 19.10.2025).

56. Мех Ю.В. Державно-приватне партнерство в секторі безпеки України: інституційні механізми та проблеми координації. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2025. Вип. 78. С. 234-242.

57. Мех Ю.В. Державно-приватне партнерство в секторі безпеки:

нормативно-правові та практичні аспекти реалізації. *Право і безпека*. 2023. № 4(91). С. 134-142.

58. Міжнародна та національна безпека: теоретичні аспекти. Academia.edu, 30 січня 2023. URL: <https://www.academia.edu/95985490/> (дата звернення: 21.10.2025).

59. Мостовий В.О. Світовий досвід публічно-приватного партнерства: компаративний аналіз моделей. *Вісник Національної академії державного управління*. 2024. № 2. С. 78–86.

60. Національна безпека України: сучасні загрози. Матеріали VII Міжнар. наук.-практ. конф. Харків: Право, 2023. URL: https://ivpz.kh.ua/wp-content/uploads/2023/07/Електр_версія_Конф_Національна-безпека-України.pdf (дата звернення: 17.10.2025).

61. Нормативно-правові акти ДПП. Мінекономіки, 2024. URL: <https://me.gov.ua/Documents/Detail?id=c5fe4de5-3213-413e-ac82-71fef98f6933> (дата звернення: 22.10.2025).

62. Оборонний сектор забезпечив 1,5 в.п. з 5% зростання ВВП у 2023 році. LB.ua, 14 січня 2024. URL: https://lb.ua/economics/2024/01/14/593690_oboronniy_sektor_zabezpechiv_15_vp.html (дата звернення: 07.10.2025).

63. Оборонно-промисловий комплекс України – драйвер побудови якісно нової української економіки. ResearchGate, May 2023. DOI: 10.5281/zenodo.8003421 (дата звернення: 08.10.2025).

64. Оборонно-промисловий комплекс України / Вікіпедія, травень 2025. URL: https://uk.wikipedia.org/wiki/Оборонно-промисловий_комплекс_України (дата звернення: 08.10.2025).

65. ОБСЄ. Новітні практики у державно-приватних партнерствах, пов'язаних з кібербезпекою: аналітичний огляд. Відень : OSCE, 2023. 89 с.

66. Органи публічної влади в політиці національної безпеки. *Наукові записки*. Серія: Право. 2024. DOI: <https://doi.org/10.36550/2522-9230-2024-17-252-256> (дата звернення: 18.10.2025).

67. Особливості застосування ДПП як механізму регіональної політики.

НІСД, 2023. URL: <https://www.niss.gov.ua/doslidzhennya/regionalniy-rozvitok/osoblivosti-zastosuvannya-derzhavno-privatnogo-partnerstva-yak> (дата звернення: 20.10.2025).

68. Офіційний сайт РНБО України, 2024. URL: <https://www.rnbo.gov.ua/> (дата звернення: 19.10.2025).

69. Панасюк В.В. Механізми публічно-приватного партнерства у сфері кібербезпеки: сучасний стан та перспективи розвитку. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1(37). С. 56-65.

70. Панасюк Т. Державна політика України у сфері забезпечення кібербезпеки: виклики та перспективи. *Вчені записки ТНУ імені В.І. Вернадського*. Серія : Державне управління. 2024. Том 35(74). № 3. С. 112-119.

71. Парламент Литви. Державно-приватне партнерство для проектів військового розміщення: досвід реалізації у містах Вільнюс, Шяуляй, Шилале. Вільнюс : Seimas, 2024. 45 с.

72. Пивовар М., Панько А. Особливості національної безпеки України в період воєнного стану: цілі, виклики та стратегія. *Вісник Національного університету «Львівська політехніка»*. Серія: Юридичні науки. 2024. Том 11, № 1(41). С. 263-269. DOI: <https://doi.org/10.23939/law2024.41.263> (дата звернення: 04.10.2025).

73. Попов М. Моделі державно-приватного партнерства: закордонний досвід та перспективи впровадження в Україні. *Інвестиції: практика та досвід*. 2024. № 7. С. 89-97.

74. Правові основи національної безпеки. *Інформація і право*. 2023. № 1(44). URL: https://ippi.org.ua/sites/default/files/16_23.pdf (дата звернення: 21.10.2025).

75. Прийнято Закон України про публічно-приватне партнерство. PRAVO.UA, 20 червня 2025. URL: <https://pravo.ua/pryiniato-zakon-ukrainy-pro-publichno-pryvatne-partnerstvo/> (дата звернення: 14.10.2025).

76. Прийнято Закон України про публічно-приватне партнерство / Офіційний портал Верховної Ради України, 19 червня 2025. URL:

<https://www.rada.gov.ua/news/razom/263288.html> (дата звернення: 09.10.2025).

77. Пріоритетні напрями розвитку публічно-приватного партнерства у сфері національної безпеки України : аналітичний огляд провідних українських видань / уклад. О.В. Литвиненко ; Національний університет оборони України. Київ : НУОУ, 2025. 98 с.

78. Про внесення змін до Стратегії національної безпеки України : Указ Президента України від 06.01.2025 № 16/2025. URL: <https://zakon.rada.gov.ua/go/16/2025> (дата звернення: 15.10.2025).

79. Про державно-приватне партнерство : Закон України від 01.07.2010 № 2404-VI. URL: <https://zakon.rada.gov.ua/laws/show/2404-17> (дата звернення: 14.10.2025).

80. Про затвердження Методики виявлення ризиків ДПП : Постанова КМУ від 16.02.2011 № 232. URL: <https://zakon.rada.gov.ua/laws/show/232-2011-п> (дата звернення: 22.10.2025).

81. Про затвердження плану заходів з реалізації Стратегії кібербезпеки. Законодавство України, 2023. URL: <https://zakon.rada.gov.ua/go/1163-2023-р> (дата звернення: 16.10.2025).

82. Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 19.12.2023 № 1163-р. URL: <https://www.kmu.gov.ua/npras/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163> (дата звернення: 10.10.2025).

83. Про концесію : Закон України від 03.10.2019 № 155-IX. URL: <https://zakon.rada.gov.ua/laws/show/155-20> (дата звернення: 23.10.2025).

84. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20> (дата звернення: 17.10.2025).

85. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 15.10.2025).

86. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 16.10.2025).

87. Про особливості управління об'єктами державної власності в ОПК : Закон України від 16.06.2011 № 3531-VI. URL: <https://zakon.rada.gov.ua/laws/show/3531-17> (дата звернення: 16.10.2025).

88. Про публічно-приватне партнерство : Закон України від 03.06.2025 № 2625-IX (у редакції 2025 року). URL: <https://zakon.rada.gov.ua/laws/show/2404-17> (дата звернення: 15.10.2025).

89. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 01.10.2025).

90. Проєкт Стратегія кібербезпеки України (2021-2025 роки). РНБО України, 2021. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 11.10.2025).

91. Публічно-приватне партнерство: концептуальні засади. Таврійський національний університет ім. В.І. Вернадського. URL: <https://tnu.edu.ua/sites/default/files/normativbasa/pppleksait.pdf> (дата звернення: 06.10.2025).

92. Резнікова О.О. Стратегічний аналіз безпекового середовища України. Національний інститут стратегічних досліджень, 2023. URL: <https://niss.gov.ua/news/statti/strategichnyu-analiz-bezpekovooho-seredovyshcha-ukrayiny> (дата звернення: 02.10.2025).

93. Розвиток оборонно-промислового комплексу / Кабінет Міністрів України, 2025. URL: <https://www.kmu.gov.ua/reformi/ekonomichne-zrostannya/rozvitok-oboronno-promislovogo-kompleksu> (дата звернення: 08.10.2025).

94. Серебряк С.В. Державно-приватне партнерство у сфері кіберзахисту: міжнародний досвід та перспективи для України. *Інформація і право*. 2024. № 3(50). С. 112-121.

95. Стратегічна панорама : науково-практичний журнал / Національний

інститут стратегічних досліджень. Публікації з тематики державно-приватного партнерства у сфері національної безпеки (2022-2025). Київ : НІСД, 2022-2025. Вип. 1-12.

96. Стратегічний аналіз безпекового середовища. *Вісник НУ «Львівська політехніка»*. 2023.

97. Стратегічний механізм забезпечення національної безпеки. *Вісник Херсонського національного технічного університету*. 2024. № 4(91). URL: https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/828 (дата звернення: 05.10.2025).

98. Стратегія кібербезпеки України / Держспецзв'язку, 2023. URL: <https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini> (дата звернення: 15.10.2025).

99. Сулій О. ОДУВС. Державно-приватне партнерство у сфері національної безпеки: міжнародний та вітчизняний контекст. *Вісник Львівського державного університету внутрішніх справ*. 2024. Вип. 3. С. 45-54.

100. Теорія публічного управління в умовах військових конфліктів: особливості публічно-приватного партнерства : колективна монографія / за ред. Н.Р. Нижник, С.О. Кравченка. Київ : НАДУ, 2024. 356 с.

101. Тесля А.В. Сучасний стан нормативно-правового регулювання державно-приватного партнерства в Україні. *Юридичний науковий електронний журнал*. 2024. № 8. С. 178-182. DOI: 10.32782/2524-0374/2024-8/42.

102. Українські юридичні фірми. Державно-приватне партнерство в секторі безпеки та оборони України: правовий аналіз : аналітична записка. Київ : Jurimex, 2025. 56 с.

103. Урядова команда реагування CERT-UA, 2024. URL: <https://cert.gov.ua/> (дата звернення: 19.10.2025).

104. Цибульник Н.Ю. Інформаційно-правова характеристика основних складових сектору безпеки держави. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. 2023. Випуск 80: частина 1. С. 607-612.

105. Цифрова армія : стратегія Міністерства оборони України щодо співпраці з приватним сектором : офіційний документ. Київ : Міноборони України, 2024. 45 с.

106. Чальцева О.М., Лобода Д.О. Державно-приватне партнерство як перспективний механізм повоєнного відновлення України. *Public networks and communications*. 2024. URL: <https://jpnac.donnu.edu.ua/article/view/16813> DOI: <https://doi.org/10.31558/2786-6505.2024.2.5> (дата звернення: 03.10.2025).

107. Шевчук О.А. Державно-приватне партнерство в сфері інноваційного розвитку: теоретичні положення та механізми формування. *Економіка та суспільство*. 2021. № 33. С. 112–119. DOI: 10.32782/2524-0072/2021-33-18.