НІСД НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ
NATIONAL INSTITUTE FOR STRATEGIC STUDIES NISS

Центр безпекових досліджень
Center for Security Studies

ДЕРЖАВА ТА ПРИВАТНИЙ СЕКТОР НА ЗАХИСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ВІД ВЗАЄМОДІЇ ДО ПАРТНЕРСТВА

Аналітична доповідь

Київ 2021

УДК 321.01.003.52:355.01.008.8 **https://doi.org/10.53679/NISS-analytrep.2021.23**
Д-36

Автори:

О. Д. Маркєєва, завідувач відділу державної та громадської безпеки центру безпекових досліджень Національного інституту стратегічних досліджень, заслужений юрист України;

Б. Л. Розвадовський, головний консультант відділу державної та громадської безпеки центру безпекових досліджень Національного інституту стратегічних досліджень, к.ю.н, доцент.

За участі:

Асоціації професіоналів корпоративної безпеки України (АПКБУ):
С. П. Погребного, голови опікунської ради АПКБУ;
І. А. Герасимовича, голови правління АПКБУ;
М. Л. Погребицького, члена правління АПКБУ;

Представництва ASIS International в Україні (ГО ASIS Ukraine):
В. І. Панчака, голови правління ГО ASIS Ukraine;
П. М. Шатковського, експерта.

Д-36 **Держава** та приватний сектор на захисті національної безпеки: від взаємодії до партнерства : аналіт. доп. / [О. Д. Маркєєва, Б. Л. Розвадовський]. – Київ : НІСД, 2021. – 72 с.

ISBN 978-966-554-330-5

Присвячено проблемам формування ефективного державно-приватного партнерства у сфері національної безпеки. Проаналізовано теоретичні підходи до державно-приватного партнерства та їхні особливості в безпековій сфері. Досліджено кращий світовий досвід (США, ЄС, Німеччини, Великої Британії, Польщі, Бельгії та інших країн) із розбудови довіри між державним і приватним сектором у сфері національної безпеки. Розглянуто нормативно-правові та організаційні засади державно-приватного партнерства в Україні, наведено ефективні приклади такої взаємодії. Окреслено перспективні напрями розвитку безпекового державно-приватного партнерства в Україні та можливі способи їх імплементації. Визначено, що недержавний (приватний) сектор безпеки має стати невід'ємним складником системи забезпечення національної безпеки України.

Розраховано на фахівців, які займаються теоретичною й практичною діяльністю у сферах національної безпеки і оборони, державного управління, приватної та корпоративної безпеки, науковців, викладачів, аспірантів, докторантів і студентів, а також працівників недержавного (приватного) сектору, які цікавляться сучасними проблемами державно-приватного партнерства.

УДК 321.01.003.52:355.01.008.8

ISBN 978-966-554-330-5

Зміст

ТЕЗИ
до вступного слова директора Національного інституту стратегічних досліджень Олександра БОГОМОЛОВА

на засіданні круглого столу
«Держава та приватний сектор на захисті національної безпеки: від взаємодії до партнерства»

Шановні колеги та запрошені експерти!

Радий вітати вас на круглому столі, присвяченому розвитку державно-приватного партнерства у сфері національної безпеки.

1. За сучасних мінливих безпекових умов жодна держава не здатна самотужки ефективно реагувати на загрози, зокрема гібридного характеру. Адже потенціал державних інституцій обмежений національними рамками, а ресурси держав не є невичерпними.
2. Уряди шукають ефективні шляхи та методи гарантування безпеки в межах національних територій. Найбільш життєздатними є суспільства/нації, здатні гнучко пристосовуватися до безпекових викликів і протидіяти загрозам.
3. Спостерігається чітка тенденція до поступового делегування низки функцій держави недержавним суб'єктам. Нині це не лише адміністративні послуги, спільні інфраструктурні, фінансові проєкти, а й деякі функції у сфері національної безпеки і оборони. Уряди західних держав розглядають державно-приватне партнерство як невід'ємний елемент національної безпеки, принцип упроваджений у національні безпекові стратегії та реалізується на практиці.
4. Партнерство є виправданим з міркувань спроможності приватних структур ефективніше виконувати певні функції держави завдяки відсутності бюрократичних обмежень, вищій оперативності, наявності власних ресурсів і мотивації (бізнес-інтересу).

5. Україна має безцінний досвід безпекового державно-приватного партнерства в умовах протидії російській агресії. Недержавні громадські та бізнесові структури є важливими складниками українського суспільства, що відіграли значну роль у захисті державного суверенітету України.
6. Відповідно до Стратегії національної безпеки України «Безпека людини – безпека країни» одним із напрямів реалізації пріоритетів національних інтересів України та забезпечення національної безпеки є розвиток державно-приватного партнерства, зокрема у сферах:

- створення ефективної системи безпеки та забезпечення стійкості критичної інфраструктури;
- модернізації транспортної інфраструктури;
- розвитку оборонно-промислового комплексу.

7. Водночас розвиток державно-приватного партнерства у сфері національної безпеки потребує вдосконалення законодавчої бази, розбудови довіри між державою і приватним сектором, спільного розроблення конкретних заходів партнерства.
8. Організований Національним інститутом стратегічних досліджень круглий стіл та підготовлена фахівцями Інституту та експертами у сфері корпоративної безпеки аналітична доповідь мають надати поштовх для розвитку державно-приватного партнерства у сфері національної безпеки.

Ця доповідь є спробою створення аналітичного продукту на засадах державно-приватного партнерства і відображає спільну думку фахівців Інституту та запрошених експертів щодо стану та шляхів розвитку цього партнерства.

Передмова

За сучасних умов жодна держава в особі її уповноважених органів не здатна самостійно та ефективно реагувати на кризи, оскільки потенціал державних інституцій спрямований передусім на сфери політики, законодавства, фінансів, використання людських ресурсів тощо і неадекватний масштабним, часто непередбачуваним загрозам національній безпеці.

Це змушує шукати нові, ефективніші шляхи та методи гарантування безпеки в межах національних територій. У наш час спроможність суспільств протидіяти викликам мінливого світу залежить від емерджентності цих суспільств, здатності якісно змінюватися та реагувати на загрози, зокрема протидіяти кризовим явищам. Адекватна відповідь на сучасні кризи є запорукою виживання держави. На думку французького політика Лорана Фабіуса, після часів Її Величності Держави настав час для держави-партнера, свідомої того, що вона може й не може, держави «епохи синтезу», більш ефективної і доступної, оскільки вона є відкритою[1].

Окремі функції держави у сучасних суспільствах поступово делегуються або передаються приватним суб'єктам на аутсорсинг. Це відбувається, зокрема, у сферах надання адміністративних послуг, економічній (інфраструктурні, фінансові проєкти, концесії) тощо. Приватні структури спроможні ефективніше виконувати певні функції держави через відсутність бюрократичних обмежень, вищу оперативність, наявність власних ресурсів і мотивації (бізнес-інтересу).

Партнерські відносини державного та приватного секторів на підставі спільних інтересів становлять зміст державно-приватного партнерства (*далі* – ДПП).

За часів стрімкого розвитку й поширення новітніх технологій глобально змінюється філософія і зміст безпекових, зокрема і воєнних, загроз. Ядерні сили як основний чинник безпеки держав періоду Холодної війни поступаються в ефективності стримувального впливу й

[1] Fabius L. Le rôle et la place de l'Etat en France. In *Drago Roland.* Le rôle et la place de l'État au début du XXIe siècle. PUF, 2001. 400 p. URL: https://www.puf.com/content/Le_r%C3%B4le_et_la_place_de_l%C3%89tat_au_d%C3%A9but_du_XXIe_si%C3%A8cle

наступу новим технологіям, які можуть бути власністю не лише держави, а й окремих осіб чи приватних компаній. Так, діяльність Ілона Маска, Річарда Бренсона свідчить про успішну конкуренцію приватного бізнесу з державними космічними програмами.

У низці документів і праць у сфері безпеки і оборони, опублікованих останніми роками на Заході та в Україні, зазначаються глибокі зміни в характері загроз національній безпеці, пов'язані з розвитком технологій, змінами клімату, боротьбою за обмежені ресурси. Зокрема, розвиток технологій штучного інтелекту та їх подальший вплив на створення військової техніки, кіберзасобів обіцяє суттєво змінити воєнні стратегії майбутнього. Стійкість і військова міць держави вже значною мірою залежать від наявності ефективних зв'язків державних структур із приватним сектором, їхньої здатності формувати мережі та підтримувати баланс між державним і приватним інтересами. Таким чином, національна безпека стає результатом колективних дій держави і суспільства.

Уряди західних держав розглядають ДПП як невід'ємний елемент національної безпеки. Цей принцип упроваджений у національні безпекові стратегії та реалізується на практиці. Наразі йдеться *не про потребу* ДПП як таку, а про *форми,* в яких воно має відбуватися[2].

[2] Goldsmith S. Eggers W. D. Governing by Network: The New Shape of the Public Sector. Washington, DC: Brookings Institution Press, 2009. URL: https://www.brookings.edu/wp-content/uploads/2016/07/governingbynetwork_chapter.pdf

1. Політико-правові умови розвитку державно-приватного партнерства в забезпеченні національної безпеки

В Україні використання моделей ДПП у сфері національної безпеки і оборони є ще достатньо новим, але має значний потенціал. Зазвичай державна політика в цій сфері спирається на власний сектор безпеки і оборони, який є системою передусім державних інституцій (органів державної влади, військових формувань, правоохоронних органів тощо). Ця система в пострадянських державах є ригідною щодо зв'язків і традицій і несприйнятливою до глибоких якісних реформ.

Під впливом активних внутрішніх і зовнішніх чинників, зокрема збройної агресії Російської Федерації проти України, окупації Криму і частини територій Донецької та Луганської областей, Україна виявила спроможність до асиметричних відповідей на загрози. В умовах гібридної війни, в якій воєнні засоби були лише доповненням до широкого арсеналу дипломатичних, інформаційних тощо впливів, державні інститути й приватний сектор – бізнес-структури, громадські організації, волонтери – змогли результативно взаємодіяти. Така взаємодія не була врегульована в правовому полі, не передбачена державними планами й програмами. Це був живий, природний процес захисту національних інтересів, унаслідок якого було здобуто унікальний досвід.

Нині завдання модернізації системи забезпечення національної безпеки України вимагає застосування концепту *національної стійкості*. Це потребує, зокрема, налагодження ефективної взаємодії між усіма державними і недержавними суб'єктами безпекової сфери, а також певного перерозподілу відповідальності в цій сфері: недержавні суб'єкти, місцеві громади, громадські об'єднання, громадяни беруть на себе певні функції у безпековій сфері, а держава створює для цього сприятливі умови й посилює координацію й контроль[3].

[3] Шляхи модернізації системи забезпечення національної безпеки у контексті розбудови національної стійкості : аналіт. зап. / Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/shlyakhi-modernizacii-sistemi-zabezpechennya-nacionalnoi-bezpeki-u

1.1.Стан законодавства

У результаті реалізації інтеграційних прагнень України вдосконалено вітчизняне законодавство з питань національної безпеки і оборони. Положення, що регулюють діяльність органів сектору безпеки і оборони, наближені до норм і стандартів ЄС та НАТО. Імплементовано «безпекові» положення Угоди про асоціацію між Україною та Європейським Союзом[4]. За участю експертів Офісу зв'язку НАТО в Україні, Консультативної місії ЄС з реформування сектору цивільної безпеки в Україні, Групи з розбудови оборонних інститутів (США) розроблений та ухвалений Верховною Радою України ***Закон України «Про національну безпеку України»***[5].

Однією з новацій Закону є твердження про те, що *громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки* (тут і далі курсив наш. – *Авт.*), є одним із чотирьох взаємопов'язаних складових елементів сектору безпеки і оборони України поряд із силами безпеки, силами оборони та оборонно-промисловим комплексом (ст. 12).

Водночас п. 17 ч. 1 ст. 1 Закону визначає сили безпеки як «*правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України*». Тобто недержавні структури безпеки не розглядаються як складовий елемент сил безпеки. Водночас загрози й ризики, з якими сьогодні стикається приватний сектор і яким протидіють недержавні структури безпеки, також підпадають під визначення загроз національній безпеці України, наведених у п. 6 ч. 1 ст. 1 Закону.

Натомість у більшості європейських країн сектор безпеки включає приватні організації сектору безпеки: охоронні підприємства, недержавні служби безпеки, приватні оборонно-промислові компанії тощо,

---

[4]Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Закон України від 16 вересня 2014 р. № 1678-VII. *Відомості Верховної Ради України*. 2014. № 40. Ст. 2021.

[5]Про Національну безпеку України : Закон України від 21 червня 2018 р. №2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241

а також цивільні організації, які досліджують безпекове середовище чи надають консультації з відповідних питань: громадські організації, аналітичні й дослідні центри, засоби масової інформації певної спрямованості, волонтери й волонтерські рухи тощо.

Зазначимо також, що поза межами законодавства, яке регулює цілі й засади національної безпеки, наразі перебувають безпека бізнесу і корпоративна безпека як об'єкти захисту. Тобто приватний інтерес не розглядається щодо забезпечення національної безпеки. Апріорі вважається, що держава й корпорація мають різні безпекові інтереси, що є нелогічним, адже доброчесний бізнес зацікавлений у стабільності державних інститутів.

Ризики бізнесу (приватного сектору) мають свої особливості й відрізняються від контексту ризиків публічного (державного) сектору. За результатами опитування, проведеного в 2020 р., найбільшими ризиками приватного сектору є, зокрема, незаконні дії державних, у т. ч. правоохоронних, органів, рейдерство, кібератаки.

Довідково. У 2020 р. ТОВ «Юридична фірма Саєнко Харенко» за підтримки українського представництва організації ASIS International (США)[6] та Асоціації професіоналів корпоративної безпеки України (АПКБУ) було проведене анонімне опитування щодо рівня безпеки ведення бізнесу в Україні, ринкової оцінки підприємницького клімату, аналізу основних кризових ситуацій для бізнесу та встановлення тих чи інших способів їх імовірного вирішення. В опитуванні взяли участь понад 100 представників середніх і великих компаній зі штатом понад 500 працівників, а безпосередніми респондентами були топменеджери підприємств, керівники служб безпеки, юридичні радники та посадовці з управлінськими повноваженнями у своїх компаніях. Дві третини з-поміж опитаних представляли вітчизняний бізнес, ще третина – підприємства з іноземними інвестиціями та представництва транснаціональних корпорацій, що ведуть свій бізнес в Україні. За результатами дослідження було встановлено 11 найбільш поширених кризових ситуацій, визначених переважною більшістю учасників опитування. До переліку таких потрапили[7]: незаконні дії державних

[6] Заснована в 1955 р. найбільша у світі організація професіоналів у сфері безпеки, що об'єднує понад 34 тис. членів у 162 країнах та сприяє глобальному просуванню корпоративної безпеки, а також забезпеченню досконалості і лідерства у сфері управління приватним безпековим сектором. *Див.*: URL: https://www.asisonline.org/

[7] Збережено формулювання опитування (*Прим. ред.*).

> органів; незаконні дії правоохоронних органів; незаконні конкурентні дії; кібератаки; кримінальні прояви; медіаатаки; рейдерство; корпоративні конфлікти; затримання топменеджменту чи власника бізнесу та членів його родини[8].

Аналіз значної кількості конкретних ситуацій дозволяє стверджувати, що через неналежне нормативне регулювання в Україні набула загрозливого поширення практика штучної криміналізації господарських, фінансових та інших цивільно-правових відносин, спрямована не на викриття і переслідування злочинів, а виключно на вчинення тиску на суб'єктів господарювання.

У такий спосіб **бізнес умотивований дбати не так про безпеку держави, як про безпеку від держави**. Це зводить нанівець можливість виникнення й розвитку відносин довіри між державою та бізнесом, які є фундаментальною основою ДПП.

Закон окреслює можливу взаємодію держави з приватними партнерами в забезпеченні національної безпеки. Так, реалізація Стратегії національної безпеки (ст. 26), Стратегії розвитку оборонно-промислового комплексу (ст. 30) і Стратегії кібербезпеки (ст. 31) здійснюється з використанням механізмів державно-приватного партнерства.

Водночас механізми взаємодії держави й приватного сектору у сфері національної безпеки законодавством України не врегульовано. Зокрема, чинний ***Закон України «Про державно-приватне партнерство»***[9] стосується лише правовідносин партнерства у сфері об'єктів нерухомості, інфраструктури (концесій) тощо. Але він не працює на розвиток української економіки внаслідок пасивності («концептуальних лінощів») держслужбовців[10].

Поза правовим полем ДПП наразі є низка специфічних активностей: охорона, детективна діяльність, розвідка, військовий консалтинг, правоохоронна, контррозвідувальна, антитерористична діяльність тощо. При цьому безпекові умови, в яких перебуває Україна, вимагають нагальної зміни політико-правових умов у цій сфері. ***Закон України «Про***

---

[8] Оцінка безпеки ведення бізнесу в Україні. URL: https://cutt.ly/PTXPIR3

[9] Про державно-приватне партнерство : Закон України від 01 липня 2010 р. № 2404-VI. *Відомості Верховної Ради України*. 2010. № 40. Ст. 524.

[10] Козлов С. Державі потрібен приватний партнер. Чи розуміє це держава? / ZN, UA. 2021. 30 лип. URL: https://zn.ua/ukr/macrolevel/derzhavi-potriben-privatnij-partner-chi-rozumije-tse-derzhava.html

охоронну діяльність»[11] є нормативно-правовим актом, що регулює приватну охоронну діяльність як один із видів господарської діяльності у сфері надання послуг з охорони власності та громадян. Він є обмеженим щодо реалізації ДПП, державні органи відповідно до Закону виконують роль регулятора, контролера, а не партнера або замовника послуг.

Досі юридично не врегульовано діяльність *приватних військових компаній* (ПВК), які могли би надавати широкий спектр безпекових послуг. Водночас закони України «Про зовнішньоекономічну діяльність» (ст. 4), «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» (абзац 17 ст. 1), «Про протимінну діяльність» (ст. 36) дозволяють іноземним суб'єктам господарської діяльності надавати цілу низку послуг на комерційному ґрунті, до яких можна віднести значну частину послуг, що їх надають ПВК. ***Закон України «Про протимінну діяльність»***[12] (п. 10 ч. 1 ст. 1) передбачає, що операторами протимінної діяльності можуть бути підприємства, установи та організації незалежно від їхньої форми власності, зокрема міжнародні та іноземні, що залучаються до протимінних заходів.

Тривають спроби врегулювати на законодавчому рівні приватну детективну діяльність. ***Проєкт закону «Про приватну детективну діяльність»*** (реєстр. № 3010) ухвалено в першому читанні 17.02.2021 р. Проте, на думку експертів, він містить низку суттєвих недоліків: приватним детективам фактично не надається прав, яких не має звичайний громадянин відповідно до положень чинного законодавства. Діяльність приватних детективів у межах прав, наданих законопроєктом, мало чим відрізнятиметься від надання послуг за цивільним договором доручення; детективна таємниця фактично є різновидом професійної таємниці, як адвокатська чи нотаріальна.

Закон України «Про розвідку»[13] (ст. 23) містить норму, що регулює взаємодію розвідувальних органів, зокрема з підприємствами будь-

---

[11] Про охорону діяльність: Закон України від 22 березня 2012 р. № 4616-VI. *Відомості Верховної Ради України*. 2013. № 2. Ст. 8.

[12] Про протимінну діяльність : Закон України від 6 грудня 2018 р. №2642-VIII. *Відомості Верховної Ради України*. 2019. № 6. Ст. 39.

[13] Про розвідку : Закон України від 17 вересня 2020 р. № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20#top

якої форми власності, у формі *сприяння* на підставі угод, укладених з дотриманням законодавства. ***Закон України «Про боротьбу з тероризмом»***[14] (ч. 6 ст. 4) зазначає, що до участі в антитерористичних операціях, за рішенням керівництва антитерористичної операції, можуть бути залучені з дотриманням вимог цього Закону підприємства, установи, організації незалежно від їх підпорядкованості та форми власності.

Закон України «Про основні засади забезпечення кібербезпеки України»[15] встановлює одним із принципів забезпечення кібербезпеки *державно-приватну взаємодію* (ДПВ), співпрацю з громадянським суспільством у сфері кібербезпеки та кіберзахисту (ст. 7). ДПВ передбачає участь приватних структур у запобіганні кіберзагрозам на об'єктах критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їхніх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період.

Кодекс цивільного захисту України[16] також лише опосередковано регулює питання державно-приватного партнерства – через «взаємодію» між власниками потенційно небезпечних об'єктів і відомствами, що контролюють їхню безпеку (ст. 8, п. 3, пп. 4–6, 8). Досить широким є перелік завдань і обов'язків суб'єктів господарювання у сфері цивільного захисту (ст. 20, п. 1), зокрема створення і використання матеріальних резервів для запобігання та ліквідації наслідків надзвичайних ситуацій. Також п. 8 ст. 32 Кодексу покладає на суб'єкти господарювання обов'язок утримання власним коштом захисних споруд цивільного захисту у стані готовності до використання за призначенням, включно із спорудами, що не увійшли до їхніх статутних капіталів у процесі приватизації (корпоратизації).

Отже, законодавство України містить декларативні положення про державно-приватне партнерство, які вимагають подальшого розвитку та конкретизації. Закон України «Про державно-приватне партнерство» безпосередньо не передбачає його реалізації у сфері національної безпеки, не відповідає вимогам сьогодення і, відповідно, має бути змінений.

---

[14] Про боротьбу з тероризмом: Закон України від 20 березня 2003 р. № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180.

[15] Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

[16] Кодекс цивільного захисту України : Закон України від 02 жовтня 2012 р. № 5403-VI. *Відомості Верховної Ради України*. 2013. № 34–35. Ст. 458.

1.2. Державні стратегії і плани

Хоча положення Закону України «Про національну безпеку України» є обмеженими в частині приватних суб'єктів та об'єктів захисту, Закон надав поштовх для формування відповідної державної політики. Розвиток ДПП віднесено до напрямів реалізації пріоритетів національних інтересів України та забезпечення національної безпеки відповідно до ***Стратегії національної безпеки України «Безпека людини – безпека країни»*** 2020 р. (*далі* – Стратегія)[17].

У Стратегії зазначено, що держава забезпечить дієву координацію й чітку взаємодію органів сектору безпеки і оборони, інших державних органів, територіальних громад, бізнесу, громадянського суспільства та населення в запобіганні й реагуванні на загрози та подоланні наслідків надзвичайних ситуацій (п. 47); держава створить ефективну систему безпеки та стійкості критичної інфраструктури, засновану на чіткому розподілі відповідальності її суб'єктів та державно-приватному партнерстві (п. 48); оборонно-промисловий комплекс забезпечуватиме потреби Збройних Сил України, інших складових елементів сектору безпеки і оборони України в озброєнні та військовій техніці, інвестуватиме в розвиток технологій, виробничих потужностей, людських ресурсів, залучатиме інвестиції, братиме участь у спільних міжнародних проєктах, *реалізуватиме потенціал державно-приватного партнерства*, виступатиме у такий спосіб драйвером економічного зростання (п. 61).

Таким чином, Стратегія декларує можливість державно-приватного партнерства в низці сфер. Цю норму втілено в галузевих документах щодо планування у сферах національної безпеки, розроблених відповідно до п. 66 Стратегії. Розвиток державно-приватного партнерства визначається в них як напрям подальшого вдосконалення державної політики. Так, у ***Стратегії воєнної безпеки України***[18] завданням з реалізації державної політики у військовій сфері, сфері оборони

[17] Про рішення Ради національної безпеки України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2016 р. № 392/2020. *Офіційний вісник України*. 2020. № 75. Ст. 2377.

[18] Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» : Указ Президента України від 25 березня 2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text

і військового будівництва в короткостроковій перспективі зазначено, зокрема, використання можливостей державно-приватного партнерства та військово-технічної співпраці для вітчизняного і спільного з партнерами розроблення, виробництва й оснащення сил оборони сучасним озброєнням, військовою та спеціальною технікою, забезпечення засобами ураження, в т. ч. безпілотними і роботизованими, довгострокове інвестування в розвиток військової інфраструктури.

Стратегічний оборонний бюлетень України[19] визначає оновлення до 2025 р. основних зразків озброєння і військової (спеціальної) техніки у спосіб оснащення сил оборони високотехнологічними сучасними системами озброєння з використанням сучасних процедур державно-приватного партнерства на договірній основі. Також відповідно до основних цілей і пріоритетів, визначених у Стратегії воєнної безпеки України, однією зі стратегічних цілей розвитку сил оборони передбачено забезпечення цих сил сучасним озброєнням і військовою (спеціальною) технікою, зважаючи на можливості ДПП, включно із використанням ДПП для розроблення й закупівлі нових, модернізації і підтримання технічної готовності наявних зразків озброєння і військової (спеціальної) техніки.

Стратегія розвитку оборонно-промислового комплексу України[20] передбачає сприяння розвитку підприємництва та подальшому сталому функціонуванню приватного сектору; скасування заборони на створення спільних підприємств і провадження спільної діяльності, залучення іноземного капіталу в розвиток виробничих потужностей українських підприємств, удосконалення системи державно-приватного партнерства.

Довідково. У Рішенні РНБО України від 18 червня 2021 р. «Про Стратегію розвитку оборонно-промислового комплексу України», крім імплементації вказаних положень Стратегії, перед Кабінетом Міністрів України поставлене завдання щодо проведення огляду системи вій-

[19] Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України» : Указ Президента України від 17 вересня 2021 р. № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/473/2021#Text

[20] Про схвалення Стратегії розвитку оборонно-промислового комплексу України на період до 2028 року : Розпорядження Кабінету Міністрів України від 20 червня 2018 р. № 442-р. URL: https://zakon.rada.gov.ua/laws/show/442-2018-%D1%80#Text

ського-технічної співпраці України з іноземними державами й розроблення Стратегії військово-технічного співробітництва[21] України з іноземними державами на п'ятирічний термін.

Удосконалення системи функціонування військово-технічної співпраці, розширення її видів в інтересах ефективного зміцнення оборонного потенціалу держави й поліпшення позицій України на світовому ринку озброєнь наразі практично неможливе без упровадження ДПП у цій сфері та має бути відображене у відповідних положеннях зазначеної Стратегії.

У ***Стратегії зовнішньополітичної діяльності України***[22] зазначено, що важливим аспектом регіональної співпраці є поліпшення інфраструктури державного кордону України із сусідніми державами – членами ЄС (Польщею, Словаччиною, Угорщиною, Румунією) у спосіб розбудови наявних і відкриття нових пунктів пропуску через державний кордон і сервісних зон, розвитку державно-приватного партнерства (п. 138).

У ***Стратегії інтегрованого управління кордонами на період до 2025 року***[23] (розділ «Мета Стратегії») зазначено, що документ спрямовано на запровадження ефективних інструментів співпраці та координування на внутрішньовідомчому, міжвідомчому, міжнародному рівнях, а також із приватним сектором.

Стратегія кібербезпеки України[24], констатуючи, що питання дієвої моделі ДПП у цій сфері наразі є невирішеними, наголошує, що розбудова національної системи кібербезпеки ґрунтується, зокрема, на співпраці та інклюзивному діалозі всіх суб'єктів забезпечення кібербезпеки, зміцненні довіри, зокрема відповідно до умов державно-приватного партнерства. Для цього Україна у взаємодії з приватним секто-

[21] Збережено назву, зазначену в Рішенні РНБО України (*Прим. ред.*). *Див.*: URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text

[22] Про рішення Ради національної безпеки і оборони України від 30 липня 2021 року «Про Стратегію зовнішньополітичної діяльності України» : Указ Президента України від 26 серпня 2021 р. № 448/2021. URL: https://zakon.rada.gov.ua/laws/show/448/2021#Text

[23] Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року : Розпорядження Кабінету Міністрів України від 24 липня 2019 р. № 687-р. URL: https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text

[24] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

ром сформує ефективну, засновану на довірі модель відносин у сфері кібербезпеки, зокрема у спосіб урегулювання на законодавчому рівні питання державно-приватного партнерства у сфері кібербезпеки, визначення форми та методів здійснення такого партнерства, зміцнення взаємної довіри та передбачення можливості запровадження експериментальних проєктів у цій сфері.

Відповідні положення містяться у проєктах Стратегії забезпечення державної безпеки, Стратегії громадської безпеки та цивільного захисту України.

Таким чином, державно-приватне партнерство у сфері національної безпеки в Україні ґрунтується на досвіді протидії російській агресії, є необхідним за сучасних безпекових умов, має перспективи для розвитку, вимагає вдосконалення законодавчої бази та спільного розроблення конкретних заходів партнерства.

Водночас реалізації цих намірів заважає відсутність базового законодавства, пострадянська правова культура та брак досвіду. Практичні підходи до ДПП вимагатимуть сприйняття приватного учасника саме як партнера, а не як підпорядкованого суб'єкта або об'єкта недовіри й утиску.

2. Іноземний досвід

У розвинених країнах світу застосування ДПП у забезпеченні національної безпеки є поширеною практикою. У ***Європейському Союзі*** розвитку взаємодії державного та приватного сектору приділяється значна увага. Зокрема, в офіційних документах Європейської Комісії[25] вказується на необхідність реалізації механізмів ДПП на загальноєвропейському рівні, що передбачає визначення пріоритетних напрямів державної політики, цільових завдань і критеріїв оцінки їх виконання у сфері безпеки, а також визначення та поширення інноваційних підходів до гарантування безпеки. Також наголошується, що у сфері реалізації політики безпеки ДПП забезпечує стійкість критичної інфраструктури для посилення національної безпеки загалом.

Підґрунтям державно-приватної взаємодії у боротьбі з тероризмом є підвищення рівня безпеки у спосіб формування взаємної довіри між державним і приватним секторами, вироблення й дотримання чітких цілей і стратегій, розподілу обов'язків і повноважень[26].

З метою налагодження ДПП у сфері кібербезпеки Європейська Комісія в липні 2016 р. після низки громадських консультацій з усіма зацікавленими сторонами уклала угоду в індустрії кібербезпеки[27]. У цей саме час Європейський Парламент ухвалив Директиву ЄС щодо мережевої та інформаційної безпеки[28], якою передбачено створення координаційного механізму реагування держав-членів у взаємодії з приватним сектором на кібератаки, що сприяє стратегічній співпраці та обміну інформацією, підтриманню довіри між учасниками. Найбільш передовими у розробленні й застосуванні національних страте-

[25] Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:52009DC0149&from=EN

[26] Dunn-Cavelty M., Suter M. Public-Private Partnerships are no Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. 2009. Vol. 2(4). Pp. 179–187.

[27] The Directive on Security of Network and Information Systems (NIS Directive). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[28] Directive (EU) 2016/1148 of the European Parliament and of the Council. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

гій кібербезпеки поміж держав – членів ЄС є Норвегія, Естонія, ФРН, Австрія, Угорщина та Нідерланди[29].

Створення організаційно-правових механізмів захисту критичної інфраструктури в Євросоюзі було розпочато ще в 2004 р. у спосіб підготовки загальної стратегії. Європейська Комісія оприлюднила офіційне повідомлення, в якому містилися пропозиції щодо додаткових заходів удосконалення європейської системи запобігання, готовності та реагування стосовно терористичних атак, спрямованих проти об'єктів критичної інфраструктури ЄС. Передбачено, що Європейська програма захисту критичної інфраструктури та Європейська інформаційна мережа попередження загроз критичній інфраструктурі забезпечуватимуть упровадження та реалізацію такого загального підходу.

У ***Великій Британії*** положення щодо доцільності зміцнення ДПП закріплено у Стратегії національної безпеки, Антитерористичній стратегії, Стратегії захисту кіберпростору та урядовому Плані розвитку національної інфраструктури. Розвитку ДПП також активно сприяє Національний центр кібербезпеки, який надає консультативні послуги приватним компаніям та організаціям щодо фізичної безпеки національної інфраструктури[30] (до роботи Центру залучено експертів у сфері безпеки з команди з реагування на комп'ютерні надзвичайні ситуації CERT-UK і співробітників Служби безпеки (MI5), а головною метою його діяльності є підвищення рівня кіберзахисту об'єктів критичної інфраструктури, мереж державного та приватного секторів, надання консультацій операторам і громадянам для функціонування та ведення бізнесу з використанням інформаційних мереж та інтернету[31]).

Положення щодо організації ДПП у ***Німеччині*** закріплено у Стратегії кібербезпеки, Концепції основних заходів захисту критичної інфраструктури, Національній стратегії захисту критичної інфраструктури. На підставі цих положень у більшості секторів критичної інфраструктури запроваджено державно-приватну взаємодію між операторами надання послуг, їх асоціаціями та відповідними державними установами, зокрема Федеральним відомством інформаційної безпе-

[29] Глобальный индекс кибербезопасности и профили по киберблагополучию. Отчет. Женева: ABIResearch, 2015. 516 с.

[30] National Cyber Security Centre (United Kingdom). URL: https://en.wikipedia.org/wiki/National_Cyber_Security_Centre_(United_Kingdom)

[31] About the NCSC. URL: https://www.ncsc.gov.uk/information/about-ncsc

ки. Співпраця між ними базується на угодах про нерозголошення інформації та відповідному кодексі поведінки. Федеральне відомство з охорони Конституції Німеччини надає операторам рекомендації щодо захисту критичної інфраструктури, зокрема стосовно протидії розвідувальній діяльності спецслужб іноземних держав та іншим загрозам у цій сфері.

У ***США*** ефективне ДПП визнається важливою вимогою для забезпечення стійкості систем і життєво важливих для країни об'єктів, їхня «недієздатність або знищення таких систем чи об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення або має своїм результатом поєднання будь-яких з перелічених вище наслідків»[32]. Відповідно до Директиви Президента США з національної безпеки № 7[33] Міністерство внутрішньої безпеки та федеральні агентства організовують співпрацю з приватним сектором, встановлюють пріоритети захисту критичної інфраструктури та координують дії відповідних органів виконавчої влади та приватного сектору через координаційні ради (міжгалузеві, галузеві, регіональні тощо).

Досвід США щодо запровадження ДПП у безпековій сфері викладено в Додатку 1.

Організація впровадження ДПП у сфері захисту критичної інфраструктури ***Канади*** покладається на уряд. Згідно з національною стратегією захисту критичної інфраструктури Канади уряд залучає державний і приватний сектори до спільної роботи з визначення пріоритетів і ключових заходів щодо зменшення загроз критичній інфраструктурі, а також забезпечення місцевих органів влади та операторів об'єктів критичної інфраструктури планами реагування на надзвичайні ситуації[34].

Взаємодія між державним і приватним секторами у сфері цивільного захисту, зокрема запобігання надзвичайним ситуаціям, що є особливою формою ДПП, розглядаються державами - членами ЄС,

[32] Hyogo Framework for Action 2005–2015: Building the Resilience of Nations and Communities to Disasters. URL: https://www.unisdr.org/2005/wcdr/intergover/official-doc/L-docs/Hyogo-framework-for-action-english.pdf

[33] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. URL: http://www.dhs.gov/homeland-security-presidential-directive-7

[34] National Strategy for Critical Infrastructure – Public Safety Canada. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

США, Канадою насамперед відповідно до завдань захисту критичної інфраструктури. Рекомендації щодо залучення приватного сектору до нагляду і управління кризовими ситуаціями у спосіб спільного координування та співпраці, планування і реалізації заходів щодо запобігання стихійним лихам містяться у Хіогській рамковій програмі дій на 2005–2015 роки, ухваленій на Всесвітній конференції ООН зі зниження ризику лих (2005 р.); Практичному посібнику з питань ефективного управління у сфері державно-приватного партнерства, підготовленого Європейською економічною комісією ООН у 2008 р.; Директиві Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію та позначення європейської критичної інфраструктури та оцінки необхідності підвищення рівня її захисту; інших документах ООН та Євросоюзу.

Відповідальність за організацію захисту критичної інфраструктури, її координацію зазвичай покладається на правоохоронні та спеціальні органи й центри, зокрема: у США – на Міністерство внутрішньої безпеки; у Канаді – на Міністерство суспільної безпеки та готовності до надзвичайних ситуацій; у Великій Британії – на урядову установу Центр захисту національної інфраструктури, підпорядковану Генеральному директору MI5; у Німеччині – на Федеральне міністерство внутрішніх справ; у Польщі – на Урядовий центр безпеки, який є надміністерською організацією та підпорядкований безпосередньо прем'єр-міністру.

Авангардом формування та розвитку ДПП вважають Велику Британію, Францію, Німеччину та США. У цих країнах створення правового підґрунтя та інституційне забезпечення є засадничими чинниками формування ефективної моделі державно-приватного партнерства у сфері безпеки.

З огляду на викладене, можна стверджувати, що формування ефективної системи ДПП у сфері національної безпеки має стати невід'ємною умовою захисту й розвитку України. Дотримання міжнародних зобов'язань, зазначених у безпекових конвенціях ООН та Ради Європи, передбачає розроблення відповідних засад упровадження ДПП у сфері національної безпеки України.

3. Підходи до практичного впровадження ДПП в окремих сферах національної безпеки

3.1. Військова сфера, сфера оборони та військового будівництва

Запровадження ДПП у цій сфері викликане передусім дефіцитом бюджетних коштів та інших ресурсів для забезпечення потреб оборони держави, зокрема виробництва та закупівлі сучасних зразків озброєння та військової техніки. Водночас питома вага приватного сектору економіки України є переважальною. Аналіз даних Міністерства економічного розвитку і торгівлі України (2020 р.) свідчить, що питома вага чистого доходу від реалізації продукції суб'єктів господарювання приватного сектору економіки становить майже 90 %[35].

Розроблення й виробництво озброєння та військової техніки

Досвід відбиття російській агресії свідчить про готовність приватних підприємців вкладати свій капітал у розроблення й виробництво озброєнь для Збройних Сил України. Підприємці самі визначають потреби військових, самі вкладають гроші у створення нових зразків озброєння та військової техніки (*далі* – ОВТ) і, ризикуючи цими коштами, очікують на державне замовлення своєї продукції. Так, безпілотний авіаційний комплекс розвідки та коригування вогню артилерії (БпАК) А1-СМ «Фурія», який був розроблений та серійно випускається приватною компанією НВП «Атлон Авіа», у квітні 2020 р. було взято на озброєння Збройних Сил України.

Така діяльність підприємців виникла спонтанно, є такою й дотепер. Без підтримки держави, без потрібного спрямування ця ініціатива може зникнути.

[35] Питома вага державного сектору в економіці. URL: https://www.me.gov.ua/Documents/List?lang=uk-UA&id=3f9cbf0b-24bf-48f8-8360-04d559e41d60&tag=UpravlinniaDerzhavnimSektoromEkonomikiIs

Довідково. У ***Стратегії розвитку оборонно-промислового комплексу України*** закріплено необхідність забезпечення доступу суб'єктів господарювання всіх форм власності до участі у проєктах зі створення та виробництва оборонної продукції, упровадження та реалізації державно-приватного партнерства, сприяння залученню інвестицій на внутрішньому та зовнішньому ринках, а головними пріоритетами визначено, зокрема, забезпечення розвитку оборонно-промислового комплексу завдяки широкій інтеграції із високотехнологічним цивільним сектором промисловості. Важливою умовою розвитку ОПК визначено **забезпечення інноваційної діяльності у сфері оборонно-промислового комплексу, зокрема у спосіб:**

• *стимулювання* приватної підприємницької ініціативи у виконанні завдань розвитку оборонно-промислового комплексу;

• *створення* на базі підприємств оборонно-промислового комплексу державної та приватної форм власності об'єднань (із залученням наукових організацій, підприємств, закладів вищої освіти і фінансових установ) для впровадження у виробництво високих технологій, комерціалізації науково-технічних розробок, виконання програм розвитку регіонів і програм реструктуризації підприємств оборонно-промислового комплексу;

• *створення* учасниками різних форм власності індустріальних і технологічних парків у сфері високих технологій для забезпечення запуску, виведення на ринок і виробництва високотехнологічної продукції, послуг і технологій в інтересах оборони і безпеки держави, зокрема завдяки інтеграції із науковими і/або освітніми організаціями;

• *залучення* кадрів, капіталу, використання компетенцій, інновацій, технологій та досвіду управління приватних підприємств і організацій у спосіб застосування механізмів державно-приватного партнерства в оборонно-промисловому комплексі для спільного вирішення завдань забезпечення національної безпеки, підвищення ефективності використання коштів державного бюджету і активів підприємств, установ і організацій в оборонно-промисловому комплексі, спільного розроблення та реалізації інвестиційних та інноваційних проєктів, удосконалення управління та інформаційно-аналітичного забезпечення оборонно-промислового комплексу, налагодження трансферу технологій;

• *упровадження* економічних механізмів ефективної взаємодії наукових установ і виробничих комплексів різних форм власності, державно-приватного партнерства підприємств, які забезпечують розроблення, виготовлення, модернізацію і ремонт продукції військового призначення та подвійного використання.

Умови діяльності приватних підприємств, що співпрацюють із Міністерством оборони України, мають бути внормовані, зокрема на законодавчому рівні.

1. Міноборони має здійснювати свою політику у сфері закупівель передбачувано для виробників і постачальників військового майна, офіційно оголошувати потреби Збройних Сил, пріоритети розвитку озброєння. Інакше кажучи, ***приватному сектору економіки необхідно забезпечити доступ до змісту державного оборонного замовлення***. Ці пріоритети не повинні змінюватися щороку, реалізовуватися через закупівлю відповідних зразків озброєння. У країнах НАТО діє 10-річний план закупівлі озброєння, що публікується в інтернеті для широкого загалу. Це надає можливість приватним компаніям планувати свою науково-технічну діяльність, здійснювати підготовку кадрів, виробництво, взаємодіяти з контрагентами і постачальниками складників і сировини, зміцнювати свої позиції на міжнародному ринку озброєнь.

Необхідно також законодавчо встановити можливість укладення довгострокових (до 5 років) контрактів на розроблення складних систем озброєння. Це уможливить ритмічне фінансування протягом зазначеного часу незалежно від перебігу фінансового року в Україні.

2. З метою унормування взаємодії державного та приватного секторів оборонної промисловості України необхідно ухвалити низку законодавчих актів, передусім ***Закон України «Про розроблення та виробництво озброєння та військової техніки»***.

3. З метою розвитку ДПП у сфері оборони можливо запровадити ***інститут партнера Міноборони***. Статус партнера Міноборони надається підприємствам усіх форм власності, в яких понад половина продукції виробляється для Міноборони. Партнери Міноборони можуть бути повноправними або асоційованими (залежно від встановлених критеріїв), а також мати певну спеціалізацію: розроблення/виробництво озброєння, тилове забезпечення, медичне забезпечення, капітальне будівництво тощо.

У такий спосіб Міноборони отримує надійного виконавця та має доступ до сучасних технологій.

На продукцію, розроблену завдяки такому партнерству, Міноборони матиме виключне право інтелектуальної власності. Партнер отримує дохід, добру репутацію, певні податкові/митні пільги, право на державну підтримку в разі тимчасової відсутності потреб у його продукції.

4. Для залучення ресурсів, зокрема приватних підприємств, до розвитку озброєння доцільно запровадити ***форвардні контракти***.

Форвардні контракти розглядаються як одна із форм державно-приватного партнерства[36]. За цим контрактом виконавець зобов'язаний власним коштом розробити зразок озброєння, а замовник зобов'язаний закупити заздалегідь визначену кількість одиниць цього озброєння, якщо його характеристики задовольняють технічним вимогам, затвердженим замовником. Мінімальні обсяги закупівель, вартість і технічні вимоги узгоджуються під час укладення контракту.

5. Формування системи ***приватної фінансової ініціативи***. Широко відома британська концепція Private Finance Initiative – PFI[37], ухвалена в 1992 р. урядом Дж. Мейджора, стала одним із напрямів інвестиційної політики держави та найважливішою формою державно-приватного партнерства. Основною причиною використання PFI була обмеженість бюджетних коштів для реалізації планів уряду щодо розвитку різних суспільно важливих сфер. Перевагою PFI є те, що вона дозволяє реалізовувати великі проєкти для потреб оборони, не витрачаючи багато державних коштів, а також стимулювати розвиток нових технологій. При цьому приватні компанії створюють, а інколи й керують великими проєктами, а потім уряд оплачує їх використання. Така система сприяє інвестиційній участі держави, зниженню її ризиків. Практично всі ризики проєктування, будівництва та експлуатації покладаються на приватного партнера. Але PFI-проєкти вигідні й для приватних компаній, оскільки, по-перше, для компаній полегшено доступ до пільгових державних кредитів; по-друге, їхнім партнером є держава – постійний та надійний суб'єкт господарювання; по-третє, органи влади не втручаються в поточну адміністративно-господарську діяльність свого партнера. Це дозволяє приватній компанії завдяки використанню інновацій, ноу-хау, кооперації та інших заходів знижувати собівартість продукції і підвищувати прибутковість проєкту.

[36] Дихановський В. М. Форвардні контракти для розвитку озброєння. *Виклики і ризики : Безпековий огляд*. 2020. 30 квіт. С. 48. URL: https://www.opk.com.ua/форвардні-контракти-для-розвитку-озб/

[37] Dykhanovskyi V., Semon B., Ansari I. Methodology for the development of key technologies. *Наука і оборона*. 2019. № 1. С. 48–53.

Приватні військові послуги

За оцінками Міноборони України, світовий ринок легальних приватних військових послуг сягає 300 млрд дол. США на рік; лише в Європі в цій сфері задіяно 1,6 млн осіб. Послугами приватних військових компаній користуються ООН, держави Північної і Південної Америки, Близького Сходу, Азії, Африки та Європи.

В Україні за часи незалежності створено значний потенціал для успішного виходу на цей ринок: понад 360 тис. громадян України набули бойового досвіду. Це люди, які можуть бути працевлаштовані приватними військовими консультантами або для роботи за кордоном. Правове врегулювання цієї діяльності в Україні та державна участь на ринку військового консалтингу дозволять створити нові робочі місця, попередити подальшу криміналізацію військового середовища, сприяти збереженню мобілізаційного ресурсу держави. Присутність України як повноцінного гравця на світовому ринку приватних військових послуг сприятиме додатковим валютним надходженням у країну.

> ***Довідково.*** Наприклад, в Іраку оплата праці суб'єктів військово-консалтингової діяльності становить від 100 дол. до 1000 дол. США на день залежно від спеціалізації і характеру виконуваних завдань. Крім того, для багатьох суб'єктів військово-консалтингової діяльності передбачене значне соціальне забезпечення та відповідне страхування[38].

За характером послуг, що їх можуть надавати приватні військові компанії, експерти виділяють такі їх типи[39]:

- компанії бойового забезпечення: послуги з підтримання бойових дій місцевих сил безпеки і оборони (за термінологією НАТО – тактична підтримка), включно із безпосередньою участю в бойових операціях (зазвичай неофіційно);
- військові консалтингові компанії: послуги з планування, створення, реформування й розвитку сил безпеки і оборони, зокрема органів розвідки й контррозвідки, їх бойової та спеціальної підготовки тощо;

[38] Валецкий О. Частные военные компании, их создание, развитие и опыт работы в Ираке и других регионах мира. URL: http://www.vrazvedka.ru/main/analytical/valeckiy.html

[39] Горовенко В., Тютюнник В. Приватні воєнні компанії: міжнародний досвід і можливі шляхи його реалізації в Україні / Ukrainian Military Pages. 2015. 02 листоп. URL: https://www.ukrmilitary.com/2015/11/private-military-companies.html

- військові логістичні компанії: послуги з обслуговування й експлуатації складних систем озброєння, військової техніки та комп'ютерних систем; матеріально-технічне забезпечення військ; будівництво військових об'єктів;
- приватні охоронні компанії (озброєна охорона): охорона/захист людей та об'єктів в умовах воєнного конфлікту, у зонах підвищеного ризику, зокрема на території країн з нестабільною обстановкою, охорона суден, захист від піратів, перемовини з піратами (медіація);
- приватні (недержавні) розвідувальні компанії: надають державі послуги у сфері розвідувальної, інформаційно-аналітичної, контррозвідувальної діяльності. У США до таких компаній належать, зокрема, Strategic Forecasting Inc. (Stratfor), Booz Allen Hamilton Holding Corporation, у Великій Британії – AEGIS Security & Investigations і Haklyut & Company.

США, Південно-Африканська Республіка, Велика Британія, Німеччина, Швейцарія, Китайська Народна Республіка ухвалили нормативно-правові акти, які регулюють діяльність приватних військових компаній, зокрема військовий консалтинг. В Україні приватна військова діяльність досі є неврегульованою, незважаючи на те, що низка приватних компаній надають відповідні послуги на території України та за кордоном (ТОВ «Омега Консалтинг Груп», Maritime Security Company ALBATROSS Ltd., Artan Group та ін.).

Наразі Верховна Рада України розглядає ***Законопроєкт «Про військово-консалтингову діяльність»*** (реєстр. № 3005 від 04.02.2020 р.), метою якого є врегулювання зазначеного питання. Документ містить низку застережень щодо участі персоналу приватних військових компаній у бойових діях на території інших країн та використання зброї на території України.

> ***Довідково.*** Відповідно до Законопроєкту № 3005 приватні військові компанії надають військові та охоронні послуги. Перелік військових послуг є досить широким: навчання особового складу збройних сил або інших силових чи правоохоронних органів іноземної держави; надання кадрової, фінансової, логістичної та інформаційно-аналітичної підтримки навчання; обслуговування та ремонт військової техніки і обладнання; послуги військового консалтингу; забезпечення постачань військової техніки та обладнання; виконання будівельних робіт

військового призначення; розмінування території, будівель і споруд; надання медичних і парамедичних послуг; надання послуг з мирного врегулювання військових конфліктів (медіація); управління ризиками, проведення навчань сил безпеки, консультації щодо ризиків для безпеки.

За висновком Головного науково-експертного управління Апарату Верховної Ради України, законопроєкт містить низку вад, що можуть створити ризики для національної безпеки на території нашої держави, умови для висування претензій Україні за дії суб'єктів надання військових послуг на території інших країн.

Усі послуги, надавані на умовах ДПП, що можуть призвести до використання зброї або спеціальних засобів персоналом приватних військових компаній, не повинні здійснюватися не тільки в межах нашої держави, а й на міжнародному рівні.

Зважаючи на світові тенденції розвитку сфери надання військових і безпекових послуг приватними військовими компаніями, єдиним шляхом розвитку ДПП у цій сфері є ***законодавче врегулювання їхньої діяльності***. Необхідно чітко передбачити перелік військових послуг, що можуть надаватися приватними військовими компаніями, механізми ліцензування й контролю за їхньою діяльністю, підтримки цих компаній з боку держави, а також засади правового й соціального захисту їхнього персоналу.

Розвідка і контррозвідка

Приватні компанії можуть співпрацювати із вітчизняними спецслужбами з питань розвідувальної, розвідувально-аналітичної, контррозвідувальної діяльності. На думку експертного середовища приватного сектору безпеки (Дод. 2), в Україні наразі можна застосовувати на практиці положення Закону «Про розвідку», який є найбільш адаптованим до можливостей ДПП.

Низка положень Закону містить норми, що дозволяють здійснювати ДПП у сфері безпеки, зокрема: розділ II ст. 12 п. 4 пп. 6, 11, 17, 18, 19, ст. 18.; розділ IV ст. 32 п. 4, ст. 34 п. 1, п. 3. Для практичного впровадження ДПП на підставі цього Закону Раді національної безпеки і оборони України необхідно відповідно до розділу II п. 2 пп. 4 визначити можливість залучення недержавного (приватного) сектору безпеки до виконання розвідувальних завдань в інтересах національної безпеки України.

На підставі цих положень Закону нині можливо:

- реалізувати можливості державно-приватного партнерства за широким спектром питань: діяльність структур прикриття (утворення, реорганізація, ліквідація, відчуження коштів/майна, легендування співробітників тощо);
- забезпечити надання приватним сектором експертних інформаційно-аналітичних послуг завдяки збору й обробці даних, отриманих від власних джерел, а також на підставі відкритих джерел інформації;
- надати можливість приватному сектору сприяти придбанню й доставці в Україну товарів, складників, безпосередня закупівля яких державою є неможливою або недоцільною;
- надати можливість приватному сектору брати участь у процесі цивільного контролю за діяльністю розвідки.

3.2. Сфера державної та громадської безпеки

Приватний сектор володіє низкою переваг для успішного вирішення завдань із протидії тероризму, боротьби з кіберзлочинністю, захисту критичної інфраструктури, усунення наслідків надзвичайних ситуацій, техногенних та екологічних катастроф тощо. Це передусім можливість вільно залучати кошти й ресурси, більш ефективне, незарегульоване управління, оперативність, технічний і фаховий потенціал. Держава може делегувати приватному партнеру відповідні повноваження.

Антитерор. Захист критичної інфраструктури

Державно-приватне партнерство є одним із важливих чинників створення ефективної системи захисту критичної інфраструктури в Україні. Реалізація ДПП у цій сфері дозволить зміцнити систему забезпечення національної безпеки, зокрема посилити її здатність до попередження кризових ситуацій, терористичних і диверсійних загроз.

Значна кількість підприємств критичної інфраструктури України належить до об'єктів приватної (повністю або сумісно із державою) власності. Приватні власники як ніхто інший зацікавлені в їхній безпеці, вони повинні та готові її забезпечувати разом із державою, використовуючи власні ресурси.

Терористичні акти та диверсії є інструментом цілеспрямованого підриву спроможності держави забезпечувати сталий розвиток суспільства та економіки. Підтвердженням цьому є політика РФ і керованих нею угруповань щодо порушення функціонування та знищення об'єктів промисловості, транспортної інфраструктури, об'єктів електро-, газо- і водопостачання для населення та промислових споживачів Донецької та Луганської областей, а також акти стосовно енергетичних об'єктів країни (диверсії на наземному магістральному газопроводі високого тиску «Богородчани – Долина» в Івано-Франківській області та «Уренгой – Помари – Ужгород» в Полтавській області).

Довідково. У Європейському Союзі створення відповідних правових механізмів розпочалось у 2004 р. Підготовлено загальну стратегію захисту критичної інфраструктури. Європейська Комісія запропонувала державам-членам вжити додаткових заходів з метою вдосконалення європейської системи запобігання, готовності та реагування стосовно терористичних атак, спрямованих проти елементів критичної інфраструктури ЄС. Європейська програма захисту критичної інфраструктури та Європейська інформаційна мережа попередження загроз критичній інфраструктурі забезпечують реалізацію такого загального підходу.

Закон «Про боротьбу з тероризмом»[40] містить положення про залучення до участі в антитерористичних заходах (операціях) підприємств, установ, організацій незалежно від підпорядкованості та форми власності, їхніх посадових осіб (ст. 4). Це дозволяє визначити загальними напрямами ДПП запобігання, виявлення та припинення терористичної діяльності, усунення та мінімізацію її наслідків, антитерористичне забезпечення об'єктів можливого терористичного посягання. На практиці ці дії означають:

- підвищення ефективності систем і режимів охорони найбільш уразливих об'єктів можливих терористичних посягань, зокрема у спосіб розроблення та впровадження уніфікованих стандартів, правил, технічних умов і вимог, обов'язкового оформлення паспортів антитерористичної захищеності таких об'єктів;

[40] Про боротьбу з тероризмом : Закон України від 20 березня 2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text

- опрацювання комплексу заходів щодо забезпечення якнайшвидшого відновлення штатного режиму функціонування об'єктів, передусім об'єктів критичної інфраструктури, щодо яких вчинено терористичний акт;
- підтримання готовності сил і засобів суб'єктів боротьби з тероризмом до виконання завдань за призначенням, належний рівень їхнього ресурсного та інформаційного забезпечення, своєчасне приведення у готовність таких сил і засобів відповідно до рівня терористичної загрози;
- запровадження на всій території країни ефективного контррозвідувального режиму як системи виявлення та попередження зовнішніх і внутрішніх загроз суспільству й державі.

Концепція створення державної системи захисту критичної інфраструктури[41] проблемою цієї сфери визначає, зокрема, нерозвиненість державно-приватного партнерства. Відповідно, розбудова ДПП у сфері захисту критичної інфраструктури та визначення зобов'язань держави й власників (розпорядників) об'єктів критичної інфраструктури є способом підвищення безпеки критичної інфраструктури та забезпечення її стійкості. На загальнодержавному рівні передбачається забезпечити формування засад ДПП на ґрунті взаємної довіри, обміну інформацією, створення стимулів для інвестування в заходи щодо захисту критичної інфраструктури; запровадження уніфікованих підходів щодо вимог до підвищення рівня захисту. Концепцією також передбачено врегулювати засади ДПП законом про критичну інфраструктуру та її захист.

Закон України «Про критичну інфраструктуру»[42] дозволяє реалізувати мету Концепції щодо запровадження ДПП. Автори Закону зважили на те, що переважна більшість об'єктів критичної інфраструктури є в приватній власності, й головна відповідальність за їхній захист покладається на власників/операторів. Тому встановлення ефективного державно-приватного партнерства дозволить досягти належного рівня стійкості та захищеності національної системи. ДПП

[41] Про схвалення Концепції створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 06 грудня 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

[42] Прийнято Закон «Про критичну інфраструктуру». URL: https://www.rada.gov.ua/news/Novyny/216426.html

як спосіб забезпечення стійкості системи дозволить поширити новітні технології на державний сектор, сприятиме оптимізації використання та економії бюджетних коштів. Закон містить низку положень щодо державно-приватної взаємодії, яку віднесено до основних принципів функціонування державної системи захисту критичної інфраструктури.

У Законі визначено напрями реалізації ДПП у сфері захисту критичної інфраструктури, зокрема: обмін інформацією; визначення повноважень і відповідальності державних органів й операторів критичної інфраструктури у сфері забезпечення безпеки та стійкості критичної інфраструктури; визначення порядку взаємодії між ними; створення системи підготовки кадрів; залучення експертного потенціалу, наукових установ, професійних об'єднань і громадських організацій до підготовки галузевих проєктів і нормативно-правових актів у сфері захисту критичної інфраструктури тощо.

Закон також визначає місце й роль правоохоронних і спеціальних органів СБУ, МВС, Нацполіції, Нацгвардії. Зокрема, на МВС покладається розвиток державно-приватної взаємодії стосовно загроз критичній інфраструктурі та створення ефективної системи управління її безпекою.

Громадська безпека

Розвитку державно-приватного партнерства у сфері громадської безпеки сприятиме передусім належний розвиток приватних охоронних, безпекових і детективних послуг. Суб'єкти підприємництва, що надають такі послуги, зможуть брати участь у ДПП, якщо держава уповноважить їх виконувати деякі функції, передані на аутсорсинг.

Приватна охоронна й детективна діяльність. Досвід розвинених країн, у яких надання цих послуг належно врегульовано, свідчить, що функціонування ринку детективних послуг підвищує гарантії безпеки громадян і бізнесу, захисту їхніх майнових прав. Ефективність приватних суб'єктів позитивно впливає на державні правоохоронні органи й стан правопорядку в державі.

Так, суб'єкти приватної детективної діяльності надають суттєву допомогу бізнесу у вивченні доброчесності та фінансового становища потенційних партнерів, що запобігає укладанню ризикованих угод, здійснюють пошук недобросовісних боржників та їхнього майна. На-

приклад, у Франції приватні детективні служби залучаються до виявлення фактів приховування доходів від оподаткування.

Результати пошукових заходів детективних агенцій сприяють підвищенню можливостей захисту учасників юридичних процедур щодо вирішення особистих і майнових спорів, зокрема в органах державного судочинства.

Крім того, сталою практикою є приватні послуги з охорони об'єктів, пошуку осіб, місцезнаходження яких невідоме, зниклого майна і тварин, виявлення фактів порушень прав інтелектуальної власності, насамперед незаконного використання товарних знаків, тощо.

В Україні наразі зазначений вид послуг на законодавчому рівні не визначений, хоча професія детектива вже давно фактично існує в нашій державі.

> ***Довідково.*** Охоронна та детективна діяльність як підвид економічної діяльності зазначена в класі 80.30 «Проведення розслідувань» Розділу 80 «Діяльність охоронних служб та проведення розслідувань» за КВЕД 2010, а кваліфікаційні вимоги до працівників у сфері надання детективних послуг затвердженні за кодом 5169 «Працівники захисних та охоронних служб» Класифікатора професій ДК 003:2010.

Діяльність із проведення розслідувань включено до профільних статутних завдань значної кількості недержавних охоронно-розшукових підприємств та агенцій практично в усіх регіонах України. Крім того, розслідування (пошук інформації) здійснюються інформаційними агенціями, журналістами під час журналістських розслідувань, а також самозайнятими підприємцями. Професійна підготовка приватних детективів в Україні здійснюється зазвичай приватними підприємствами.

Проєкт закону «Про приватну детективну діяльність» (реєстр. № 3010 від 04.02.2020 р.) передбачає можливість здійснення детективної діяльності через приватну детективну діяльність або через об'єднання приватних детективів. Це дозволить підвищити рівень захисту законних прав та інтересів людини та громадянина, суб'єктів господарювання. Ухвалення Закону має забезпечити належний державний контроль за цим видом діяльності.

Є перспективи й у подальшому розвитку приватної охоронної діяльності. Приватні охоронні підприємства є досить різними за своїми

цілями і завданнями, формами організації, якісним і кількісним складом, що є основною проблемою у вирішенні питання щодо залучення їх до державно-приватного партнерства. Доцільним є подальший розвиток ринку приватних охоронних послуг через удосконалення нормативно-правової бази та підвищення прозорості процедур ліцензування, правил здійснення такої діяльності, використання спеціальних засобів, зброї тощо.

Очікується, що робота приватних охоронних і детективних підприємств/агенцій певною мірою розвантажить поліцію, допоможе слідству, зокрема у справах приватного обвинувачення. Детективи сприятимуть стороні захисту, потерпілим у пошуку доказів, що допоможе адвокатам краще вибудовувати правову позицію в інтересах клієнтів.

Інформаційна підтримка з питань протидії тероризму, боротьби зі злочинністю. Отримання даних про пасажирів літаків, які прямують до України, дозволить виявляти пасажирів із потенційно високим рівнем ризику терористичної загрози та вживати попереджувальних заходів, аж до недопущення посадки таких осіб на літак у пункті вильоту. У разі затримання такої особи на території України саме на нашу державу покладається обов'язок повернення її до країни вильоту, що здійснюється за державний кошт. З огляду на це, важливою є імплементація в Україні системи отримання, передачі, використання та захисту даних про пасажирів API/PNR.

Довідково. API (Advance Passenger Information) – система попередньої інформації про пасажирів, що збирається авіаперевізником під час реєстрації. Зібрана інформація передається в електронному вигляді органу прикордонного контролю в пункті призначення рейсу. Прикордонники обробляють цю інформацію, виявляючи тих пасажирів, які мають високий ступінь ризику. Проте така ідентифікація здійснюється лише після вильоту.

Система діє ефективніше, якщо існують технічні можливості для здійснення обміну інформацією онлайн – завдяки інтерактивним програмам API. Тоді можна запобігти посадці пасажира з високим ступенем ризику на рейс у пункті відправлення.

PNR (Passenger Name Record) – загальна назва записів реєстрації пасажирів. Вона включає будь-які дані про особу, що подаються експлуатантами повітряних суден або їхніми агентами під час бронювання місця на рейс. PNR містить, наприклад, інформацію про попередні по-

їздки пасажирів (для програм заохочення), їхні потреби, стан здоров'я тощо. Така інформація може бути подана до системи контролю безпеки за 24–30 годин до вильоту. Аналіз цієї інформації правоохоронними органами може виявити певні особливості (незвичайний маршрут, спосіб оплати квитка, терміновість тощо), що є важливим для цілей безпеки та протидії тероризму.

Запровадження таких систем є вартісним проєктом. У світі поширена практика впровадження систем API–PNR на засадах ДПП.

Довідково. Приватна транснаціональна корпорація IDEMIA (головний офіс у Франції) надає урядовим структурам понад 450 країн послуги зі створення таких систем, зокрема з метою вдосконалення контролю за кордоном, митного контролю, протидії нелегальній міграції та злочинності[43]. Компанія спеціалізується на автоматичній ідентифікації, телекомунікаціях, фінансових послугах у мережі, громадській безпеці. На пострадянському просторі ще в 2018 р. було укладено контракт ДПП між Міністерством інвестицій та розвитку Республіки Казахстан (державний партнер) та ТОВ «Qazaqstan Identity & Security» на встановлення й техобслуговування приватним партнером Інформаційної Системи APCAS[44]. Однією з функцій Системи є оперативний аналіз інформації про авіапасажирів, що включає скринінг та профілювання за базами розшукуваних осіб.

Упровадження систем автоматичної ідентифікації в пунктах пропуску на кордоні дозволить:

- попередити в'їзд і транзит територією України небажаних осіб, які можуть бути причетними до терористичної діяльності;
- підвищити ефективність прикордонних, правоохоронних органів, спеціальних служб та органів правосуддя;
- уживати заходів щодо запобігання підробці та шахрайству при використанні документів, що встановлюють особу, та проїзних документів;
- розвивати міжнародну співпрацю у сферах боротьби з тероризмом та безпеки цивільної авіації.

[43] IDEMIA supports French law enforcement's efforts to fight organized crime and illegal immigration. URL: https://www.idemia.com/idemia-supports-french-law-enforcements-efforts-fight-organized-crime-and-illegal-immigration

[44] Реализованный проект: Создание и внедрение автоматизированной системы по сбору данных об авиапассажирах. Паспорт проекта. URL: https://kppf.kz/ru/news/gchp/193

Запобігання надзвичайним ситуаціям і мінімізація їхніх наслідків. Цивільний захист

Співпраця між секторами щодо надзвичайних ситуацій є особливою формою ДПП, яка впроваджується з метою ***поліпшення управління кризовими ситуаціями***[45] завдяки спільній координації та співпраці між приватними та державними суб'єктами. У межах цієї моделі ДПП комерційний ланцюг постачання основних товарів і послуг доповнює ланцюг постачання громадських послуг таким чином, щоб пом'якшити кризову ситуацію. На відміну від інших форм метою цієї форми ДПП є не максимізація спільного прибутку, а *мінімізація вартості витрат* у спосіб обмеження бюджетних витрат з боку держави та прибутків приватного підприємства, що бере участь у процесі управління кризовою ситуацією.

Досить поширеною практикою у світі є участь приватного партнера в боротьбі з наслідками надзвичайних ситуацій, одним із напрямів якої є ***гуманітарна логістика***[46] – ефективне постачання необхідних речей постраждалим під час надзвичайної ситуації та/або гуманітарної кризи.

Складність гуманітарних ланцюгів постач виявляється в процесах планування та реалізації в умовах невизначеності та обмеженості в часі.

В Україні правове регулювання механізму ДПП щодо попередження та реагування на надзвичайні ситуації, зокрема в базових законодавчих актах, відсутнє. Водночас триває приватизація багатьох потенційно небезпечних підприємств, високим є ризик техногенних аварій через зношеність основних фондів підприємств і об'єктів, зокрема підвищеної небезпеки. Це викликає нагальну необхідність налагодження державно-приватного партнерства у сфері, активного залучення недержавних суб'єктів до розв'язання наявних проблем.

3.3. Кібербезпека. Протидія дезінформації

На позначення ДПП у сфері кібербезпеки запропоновано спеціальний термін – *кібербезпекове державно-приватне партнерство* (КДПП)[47].

[45] Wiens M. et. al. Collaborative Emergency Supply Chains for Essential Goods and Services. *Urban Disaster Resilience and Security*. Springer: Cham, 2018. Pp. 145–168.

[46] Thomas A. S., Kopczak L. R. From logistics to supply chain management: the path forward in the humanitarian sector. *Fritz Institute*. 2005. № 15. Pp. 1–15.

[47] *Детальніше див.*: Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberbezpeka.pdf

Україна має значний потенціал для формування повноцінної платформи КДПП у загальнонаціональних масштабах. Протидія російській агресії, зокрема терористичним та інформаційним атакам у кіберпросторі, засвідчує значний внесок волонтерів, бізнес-структур і громадських організацій у розвиток цієї діяльності. Патріотично налаштовані «хактивісти» («Українські кібервійська», «Кіберсотня», FalconsFlame, Trinity, RUH8 та ін.) здійснювали злами комп'ютерних терористів та їхніх російських кураторів, отримували доступ до поштових скриньок осіб, задіяних в організації та реалізації російської агресії проти України, відслідковували аккаунти у соціальних мережах та мережі інтернет, через які терористичні угруповання здійснювали агітацію та збирали кошти, блокували окремі електронні гаманці поплічників терористів, допомагали в ідентифікації осіб, які беруть участь у збройному протистоянні проти сил АТО/ООС на сході України, тощо[48].

Цей досвід дозволив значно розширити й деталізувати межі державно-приватної взаємодії у законодавстві, що регулює сферу кібербезпеки.

Довідково. Закон України «Про основні засади забезпечення кібербезпеки України» (ст. 10) визначає такі способи забезпечення державно-приватної взаємодії у сфері кібербезпеки:
«1) створення системи своєчасного виявлення, запобігання і нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;
2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;
3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;
4) партнерства та координації команд реагування на комп'ютерні надзвичайні події;
5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

[48] Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України. С. 64.

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;
7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;
8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;
9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;
10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;
11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі»[49].

Ці напрями взаємодії є фактично законодавчою рамкою розвитку КДПП і потребують подальшого розвитку в підзаконних актах.

КДПП є одним із визначальних елементів системи національної безпеки держави й потребує практичних кроків для розвитку. Метою такого партнерства потрібно визначити ***побудову цілісної та ефективної системи кібербезпеки держави, що складається як із захисних, так і з наступальних систем і засобів***.

Водночас на практиці процесу розвитку КДПП бракує системності, довіри партнерів, ініціативності. Ця сфера є закритою, зокрема щодо інформування фахівців, суб'єктів забезпечення кібербезпеки, і не дозволяє розвивати комунікації, реалізовувати нові проєкти тощо.

Беззаперечна важливість діяльності з *протидії дезінформації* зумовлена тим, що інформаційні атаки, зокрема із використанням дезінформації, є одним з найпоширеніших і найефективніших засобів ведення гібридної війни. За сучасних умов держава не здатна самотужки протидіяти численним інформаційним кампаніям із використанням медіа, соціальних мереж, «арт-шоу проєктів» тощо. Водночас значна кількість активних громадян, волонтерських груп і ІТ-компаній як в Україні, так і поза її межами від початку російської агресії з власної ініціативи залучилися до роботи з виявлення і

[49] Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

спростування різного роду дезінформаційних повідомлень, зокрема фейкових новин.

Протидія ворожим інформаційним впливам/дезінформації як елемент протистояння зовнішнім загрозам має бути впорядкована державою у спосіб розроблення та ухвалення відповідних концепції, стратегії і програм, до реалізації яких у межах ДПП або на добровільних засадах варто залучати значний потенціал недержавного сектору, зокрема приватних телевізійних і радіоканалів, інформаційних агенцій, відомих представників блогерського середовища тощо.

4. Напрями вдосконалення правового забезпечення державно-приватного партнерства у сферах національної безпеки і оборони

Нові виклики вимагають ухвалення законодавства, що має містити нові принципи державної політики щодо врегулювання проблемних питань розвитку ДПП, зокрема стосовно розподілу відповідальності між державою та приватним сектором, координування дій відомчих систем захисту і реагування на різні види загроз.

У цьому контексті варто розглянути низку пропозицій експертів з недержавних структур безпеки, оскільки створення умов для розвитку ДПП має бути «двостороннім рухом».

Варто погодитись, що для розвитку ДПП у сферах національної безпеки і оборони необхідно:

1) внести зміни до розділу 1, ст. 1 Закону України «Про національну безпеку України», якими чітко передбачити суб'єктність недержавного (приватного) сектору безпеки у системі забезпечення національної безпеки України, зокрема зазначити, що недержавний (приватний) сектор безпеки є невід'ємною складовою частиною вказаної системи;

2) імплементувати ці положення Закону у Стратегію національної безпеки України, зокрема передбачити розроблення ***Стратегії розвитку державно-приватного партнерства у забезпеченні національної безпеки***;

3) доповнити Закон України «Про державно-приватне партнерство» окремим розділом «Державно-приватне партнерство у сфері національної безпеки», зважаючи на всі особливості такого партнерства щодо захисту інформації;

4) розробити законопроєкти щодо внесення змін до чинного законодавства України, ухвалити підзаконні нормативно-правові акти.

Експерти АПКБУ та ASIS Ukraine[50] пропонують у Законі України «Про національну безпеку України» розширити зміст ст. 12 «Склад

[50] АПКБУ – Асоціація професіоналів корпоративної безпеки України. *Див.*: http://corporatesecurity.org.ua/; ASIS Ukraine – українське представництво ASIS International (США). *Див.*: https://asisukraine.org/

сектору безпеки і оборони», передбачивши у четвертому складнику сектору безпеки і оборони *поряд із громадянами й громадськими об'єднаннями «недержавні структури безпеки, які добровільно або на засадах державно-приватного партнерства беруть участь у забезпеченні національної безпеки»*. У ч. 2 ст. 12 Закону уточнити окремим положенням, що *недержавними структурами безпеки є приватні охоронні структури, приватні служби та суб'єкти корпоративної безпеки, детективні агенції, приватні аналітичні й розвідувальні структури, приватні суб'єкти воєнного консалтингу, інші приватні структури, що діють у сфері приватної та корпоративної безпеки, зокрема технічні, кібербезпекові, інформаційні, інженерні тощо*.

Доцільно також формувати періодичний ***Огляд недержавних структур безпеки***, передбачивши це у ст. 27 Закону.

Потрібно ухвалити закони України ***«Про охоронну діяльність»***, ***«Про детективну діяльність»***, ***«Про військово-приватний консалтинг»***, ***«Про цивільний обіг зброї»***, ***«Про службу безпеки суб'єктів господарювання»***, ***«Про комерційну таємницю і конфіденційну інформацію»***.

У державі має функціонувати орган, який формуватиме порядок денний ДПП у сфері національної безпеки та забезпечуватиме майданчик для комунікацій. Представники АПКБУ та ASIS Ukraine запропонували два варіанти створення такого органу, а саме:

1) **Координаційний комітет з питань взаємодії з недержавним сектором національної безпеки** при РНБО України відповідно до ст. 14 Закону України «Про Раду національної безпеки і оборони України». Основні функції: опрацювання напрямів, шляхів, механізмів ефективного розвитку ДПП у сфері національної безпеки, координація діяльності органів виконавчої влади та сектору безпеки і оборони з недержавними структурами безпеки. До складу Комітету мають увійти представники державних органів (на рівні уповноважених заступників керівників), зацікавлених у взаємодії із приватним сектором, наприклад, Національної поліції, СЗРУ, СБУ, ГУР Міноборони, НАБУ, ДБР, Міноборони, Бюро економічної безпеки України. Очолювати комітет запропоновано двом особам-співголовам: від державних органів та від приватного сектору. Від недержавного сектору до Комітету могли б увійти представники структур недержавного сектору безпеки та їх об'єднань, які фактично присутні на ринку безпекових

послуг. Передбачено, що створення Комітету значно посилить спроможності системи національної безпеки України;

2) **Урядовий координаційний орган забезпечення національної стійкості**, створений відповідно до п. 3 Рішення Ради національної безпеки і оборони України від 20 серпня 2021 р. «Про запровадження національної системи стійкості»[51]. Цей варіант дозволить реалізувати на практиці один із ключових принципів національної стійкості – забезпечення широкої державно-приватної взаємодії.

На думку експертів, представники недержавних структур безпеки мають залучатися й до інших ланок *механізму інституційного забезпечення національної системи стійкості*, передбачених вказаним Рішенням РНБО України:

- постійних структур міжвідомчої взаємодії з питань забезпечення національної безпеки та стійкості;
- допоміжних і дорадчих органів з питань забезпечення національної стійкості;
- національної мережі аналітично-експертних, наукових та навчально-методичних центрів розвитку стійкості;
- постійних структур міжвідомчої взаємодії з питань забезпечення безпеки й стійкості регіонів і територіальних громад;
- допоміжних і дорадчих органів з питань забезпечення стійкості регіонів і територіальних громад;
- регіональної мережі аналітично-експертних, наукових і навчально-методичних центрів розвитку стійкості тощо.

Довідково. Цікавим є досвід Польщі, де вже створено інституції і механізми для розвитку ДПП: орган виконавчої влади у системі Міністерства економіки та посада Урядового уповноваженого з питань ДПП. Ці органи здійснюють програмні (створення стратегій/планів), координаційні, моніторингові, аналітичні та організаційно-юридичні функції.

Однією з необхідних умов розвитку ДПП у безпековій сфері є нормативно-правове врегулювання *цивільного обігу зброї*. Врегулювання

[51] Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : Указ Президента України від 27 вересня 2021 р. № 479. URL: https://zakon.rada.gov.ua/laws/show/479/2021#Text

цього питання має позитивно вплинути на ринок безпекових послуг і розвиток приватного сектору безпеки.

> ***Довідково.*** За даними Small Arms Survey[52], що досліджує проблеми обігу нелегальної стрілецької зброї у світі, в Україні в незареєстрованому обігу перебуває від 3 до 5 млн одиниць стрілецької зброї. За інформацією МВС України, у цивільному обігу зареєстровано близько 1,3 млн одиниць легальної стрілецької зброї. Точна кількість нелегальної зброї невідома. За даними різних соцопитувань, громадських організацій, приблизними підрахунками силовиків, ця цифра коливається в межах від 400 тис. до 5 млн одиниць, що збігається з даними Small Arms Survey.

Незважаючи на таку кількість зброї в цивільному обігу, ці правовідносини досі не врегульовано жодним законом. Законопроєкти №№ 4335, 4335-1 про обіг цивільної вогнепальної зброї та бойових припасів до неї ухвалено не було. Усі питання, пов'язані з обігом цивільної зброї, вирішуються виключно підзаконними нормативними актами МВС України та інших міністерств і відповідних структур. Причому ці нормативні акти дублюють положення ще радянських документів і містять низку анахронізмів, що не зважають на усталені суспільні відносини у сфері обігу зброї.

Донедавна МВС було монополістом надання озброєних послуг охорони (Державна служба охорони МВС) та одночасно ліцензіаром і регулятором ринку охоронних послуг. Нині послуги охорони надає Національна поліція (Поліція охорони), а МВС надає адміністративні послуги з ліцензування охоронної діяльності. Проте бюрократичний вплив на ринок охоронних послуг зберігається, що заважає його легальному розвитку. Наразі Україна є єдиною державою в Європі, в якій відсутнє законодавче регулювання обігу цивільної вогнепальної зброї[53].

Серед законодавчих умов формування **кадрового резерву** важливим є врегулювання правил *залучення* до співпраці з органами сектору безпеки і оборони *компетентних фахівців* приватного сектору.

---

[52] Незалежний проєкт Small Arms Survey – Огляд стрілецької зброї – здійснюється в Інституті міжнародних досліджень і розвитку в Женеві, Швейцарія. *Див.*: https://www.smallarmssurvey.org/

[53] Корнієнко М. В., Сокол Д. О. Деякі питання нормативно-правової регламентації права на вільний доступ до вогнепальної зброї. *Право і суспільство*. 2019. № 6. С. 36. URL: http://pravoisuspilstvo.org.ua/archive/2019/6_2019/part_1/8.pdf

Пропонується відновити ***інститут офіцерів резерву*** на особливий період, зокрема для зміцнення системи територіальної оборони. Ухвалення Закону України «Про основи національного спротиву»[54] створило сприятливе правове поле для реалізації цієї ініціативи.

Одним із напрямів залучення кадрів може стати започаткування навчально-освітніх ініціатив у межах ДПП у сфері національної безпеки. Відповідно до цих ініціатив можна передбачити механізми переходу спеціалістів-безпековців з державного сектору у приватний, підготовку до сертифікаційних програм за міжнародними стандартами тощо.

Подібні ініціативи сприятимуть поліпшенню адаптації, перепідготовці звільнених, зокрема в разі скорочення штату, співробітників правоохоронних органів і держслужбовців. Навчання має відбуватися у сфері корпоративної безпеки з наступним підвищенням кваліфікації у цій професії, створенням кадрового резерву для служб безпеки середніх і великих компаній, працевлаштуванням у громадських і бізнес-структурах, формуванням спільноти професіоналів корпоративної безпеки у взаємодії з правоохоронними органами України.

Удосконалення правових засад державно-приватного партнерства має ґрунтуватися на сучасних реаліях, коли монополія держави на забезпечення безпеки як суспільного блага не забезпечує належного реагування на широкий і мінливий спектр загроз. Цю функцію держава може виконувати як безпосередньо – через органи сектору безпеки і оборони, так і опосередковано – із залученням недержавного сектору безпеки на засадах ДПП.

У розвинених державах у межах ДПП надаються послуги: поліційні, пожежної охорони, окремих видів військової справи, захисту інформації, кібербезпеки тощо.

У ***Законі України «Про державно-приватне партнерство»*** доцільно відобразити принципи та основні форми здійснення ДПП, які дозволять розвивати його й у сфері національної безпеки.

Принципами правового регулювання ДПП у сфері національної безпеки мають стати:

- законність;
- добровільність, взаємна зацікавленість;

[54] Про основи національного спротиву : Закон України від 16 липня 2021 р. № 1702-IX. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text

- цивільно-правовий характер співпраці;
- оптимальний поділ завдань і ризиків між державним та приватним секторами.

Формами ДПП можуть бути:

- *спільне підприємство* – спільне використання ресурсів і поділ ризиків між урядом і приватним сектором включно з використанням спеціальних інструментальних засобів;
- *сервісний договір* – уряд наймає з метою надання певних послуг приватну компанію на певний період;
- *управлінський договір* – уряд бере на себе капітальні видатки, приватна компанія забезпечує обіговий капітал для реалізації проєкту;
- *договір оренди* – приватний партнер повністю бере на себе реалізацію контракту терміном до 10–20 років включно із фінансуванням, експлуатацією, управлінням якістю та ризиками;
- *концесія* – повне обслуговування контракту концесіонером (приватною компанією) включно із капітальними вкладеннями, експлуатацією, управлінням та обслуговуванням. Зазвичай діє схема «побудова об'єкта – його експлуатація – передача об'єкта державі»[55].

Доцільним також є укладення меморандумів між державними органами та організаціями приватного бізнесу з питань безпеки, створення відповідних консультативних майданчиків.

У цьому контексті цікавим є **досвід Бельгії** та **Нідерландів**. У *Бельгії* Міністерство юстиції та Федерація бельгійських підприємств ще в 2001 р. уклали протокольну угоду про постійну консультативну платформу для безпеки й підтримки бізнесу. Основною метою реалізації угоди є об'єднання зусиль для захисту бізнесу від злочинних зазіхань. Створено федеральний керівний комітет з представників уряду та бізнесу, відповідні робочі групи. Це дозволяє взаємні консультації з широкого спектра питань безпеки: протидії організованій злочинності, корупції, екстремізму тощо. Робочі групи залежно від теми, що розглядається, можуть складатися із представників поліції й розвідувальних служб, судових органів та інших зацікавлених урядових відомств та експертів з Федерації бельгійських підприємств.

[55] Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberbezpeka.pdf

У *Нідерландах* ініціатива щодо постійної консультативної платформи з питань корпоративної безпеки діє ще з 1994 р. Її метою є виявлення взаємних потреб, планування та організація навчання й виховання, а також розроблення і виконання плану дій з метою сприяння реалізації заходів щодо встановлених пріоритетів. Зокрема, створено канал для взаємного обміну терміновою інформацією про безпекові загрози між державними та приватними суб'єктами.

Використання нідерландського й бельгійського досвіду для створення в Україні консультативного органу (платформи) щодо узгодження державно-приватних ініціатив у сфері безпеки видається реальним та ефективним способом налагодження постійної взаємодії між державним і приватним секторами. Така платформа може бути створена на базі державних органів, зацікавлених у взаємодії із приватним сектором, і стати майданчиком для ініціатив і проєктів, що дозволять створити інституційну основу для ДПП у сфері національної безпеки.

Стратегія економічної безпеки України на період до 2025 року[56] декларує забезпечення гарантованого захисту національної економіки в умовах виникнення або посилення внутрішніх і зовнішніх загроз. Натомість конкретні напрями захисту бізнесу Стратегією не передбачені, як і напрями розвитку державно-приватного партнерства.

Довідково. У 2019 р. українські бізнесмени спільно з провідними незалежними експертними інститутами України розробили проєкт Доктрини економічної безпеки[57], в якому було перелічено основні чинники, що загрожують економічному розвитку загалом і бізнесу зокрема. Це корупція, організована злочинність, незахищеність права власності. Проте до Стратегії економічної безпеки на період до 2025 року ці положення включено не було.

Також було запропоновано скорочення неефективних установ, які не виконують свої функції, перезавантаження уражених корупцією важливих державних органів, запровадження нульової толерантності до корупції, скасування дубльованих повноважень різних держав-

[56] Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року» : Указ Президента України від 11 серпня 2021 р. № 347/2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021#Text

[57] Бізнес пропонує: як Україна має досягти економічної безпеки? URL: https://www.epravda.com.ua/publications/2019/07/17/649712/

них органів та посилення ролі Антимонопольного комітету України. Зазначалося, що уряд мусить протидіяти організованій злочинності зусиллями всіх правоохоронних органів, які не повинні зазнавати політичних впливів.

Оскільки **сфера кібербезпеки** є найбільш розвиненою з погляду запровадження ДПП, вона може стати свого роду зразком для практичного розвитку ДПП в інших безпекових сферах. Пропозиції щодо механізмів взаємодії у контексті стратегічних завдань розвитку ДПП у сфері кібербезпеки подано в Додатку 3.

На думку експертів АПКБУ та ASIS Ukraine, способами вирішення низки проблем розвитку ДПП у сфері кібербезпеки можуть стати такі дії держави:

- формування національних стандартів і мінімальних вимог у сфері управління ризиками критичної інфраструктури та кібербезпеки; публікація цих стандартів, їх популяризація та організація навчання фахівців з приватного сектору; створення профільного ринку послуг, на якому держава виступатиме лише регулятором і одним із споживачів. При цьому державні органи не повинні оцінювати ризики та здійснювати перевірки на відповідність стандартам за винятком перевірок своїх власних систем управління ризиками. І державні структури, і об'єкти критичної інфраструктури мають проходити регулярні зовнішні аудити систем управління ризиками;
- припинення практики створення національних центрів та органів, для яких на ринку немає (і ніколи не буде) достатньої кількості кваліфікованого персоналу. Держава може і має купувати відповідні послуги у приватного сектору за тендерними процедурами, зберігаючи за собою контрольну (відповідно до конкретних контрактів) і координаційну роль;
- створення системи стимулів для забезпечення обміну інформацією та координування зусиль у цій сфері. Наприклад, надання захищеної платформи для збору та аналізу інформації про кібератаки, регулярне інформування партнерів із приватного сектору про актуальні загрози та методи протидії, координування зусиль з відбиття кібератак, надання експертної допомоги в забезпеченні захищеності об'єктів, підвищення кваліфікації профільних фахівців, допомога держави наявним галузевим об'єднанням та

ініціативам щодо підготовки та впровадження необхідної нормативної бази;

- створення ефективного механізму міжнародної співпраці в цій сфері, зважаючи на потреби й очікування приватного сектору;
- мінімізація контрольної та каральної ролі держави та формування профільної нормативної бази відповідно до принципів взаємовигідної співпраці між приватним сектором і державними органами;
- створення передумов для делегування окремих державних завдань і функцій у сфері забезпечення безпеки приватним структурам на комерційному ґрунті.

Так, фізична охорона об'єктів критичної інфраструктури, експлуатація технічних систем безпеки, аудит систем управління ризиками, моніторинг та аналіз кіберзагроз, реагування на кіберінциденти, їх первинне розслідування та багато інших функцій можуть і мають здійснюватися найбільш підготовленими і компетентними комерційними організаціями на виконання держзамовлень. Це буде і дешевше, і ефективніше, ніж створення додаткових державних структур і безуспішних спроб сформувати необхідний ресурсний і кадровий потенціал коштом державного бюджету.

Основними ***ризиками у сфері ДПП***, що впливають на реалізацію проєктів, є значні бюджетні витрати, відсутність співвідношення ціни та якості, створення корупційних схем для відмивання коштів. Ці ризики стосуються переважно великих інфраструктурних проєктів (реконструкції доріг, комунальної інфраструктури, будові метрополітену тощо).

> ***Довідково.*** У 2018 р. Європейський суд аудиторів (Рахункова плата) у звіті «Публічно-приватне партнерство в ЄС: поширені вади та обмежені переваги» наголосив, що недоліки державно-приватного партнерства очевидні вже багато років, а також рекомендував державам-членам не заохочувати більш інтенсивне та масштабне використання державно-приватного партнерства, поки, зокрема, не буде впевненості в тім, що вибір на користь державно-приватного партнерства є таким, що забезпечує найвигідніше співвідношення капіталовкладень та якості отриманого продукту. Вадою реалізації проєктів у межах державно-приватного партнерства в країнах ЄС зазначається, зокрема, те, що зазвичай вони є найдорожчим способом фінансування проєктів, а також те, що у таких проєктах не дотримується достатній рівень прозо-

> рості, неадекватним є також розподіл ризиків між учасниками[58]. Тому ще в жовтні 2017 р. понад 150 організацій з усього світу підписали маніфест, в якому закликали Світовий банк та подібні органи припинити просування державно-приватного партнерства[59].

Отже, ДПП як і будь-яка модель відносин, що містить елемент фінансового та організаційного ризику, має приклади не лише успіхів, а й невдач. Це не означає, що необхідно взагалі відмовитися від упровадження ДПП. Водночас потрібно чітко розуміти, що спільні проєкти мають бути всебічно обґрунтованими, проаналізованими щодо можливих ризиків, партнери повинні бути рівноправними учасниками відносин, які поділяють між собою не лише результати успіху (фінансові, репутаційні), а й наслідки невдач.

Як свідчить досвід використання ДПП у США, державно-приватне партнерство може не виправдати очікувань через невиконання окремими гравцями рекомендацій уряду. Такі проблеми демонстрували, що хоча партнерські відносини між державним і приватним секторами є невід'ємною складовою частиною системи національної безпеки, проте **існують певні напрями безпеки, що мають бути збережені виключно за державою**.

[58] Special report 09/2018: Public Private Partnerships in the EU: Widespread shortcomings and limited benefits. Press Release. URL: https://www.eca.europa.eu/Lists/ECADocuments/INSR18_09/INSR_PPP_EN.pdf

[59] Зуєва Ю. Закордонні кейси з ДПП: порівняльний аналіз. *Юридична газета*. 2020. № 1 (707). URL: https://yur-gazeta.com/publications/practice/derzhavnoprivatne-partnerstvo/ zakordonni-keysi-z-dpp-porivnyalniy-analiz.html

Висновки та пропозиції

1. Недержавні громадські та бізнесові структури є важливим складником українського суспільства, що відіграє значну роль у захисті державного суверенітету України. Тому держава не може ігнорувати їхню роль у розбудові та розвитку системи національної безпеки.

Державно-приватне партнерство у сфері національної безпеки в Україні ґрунтується на досвіді протидії російській агресії, є необхідним за сучасних безпекових умов та має перспективи для розвитку. Наразі формування ефективної системи державно-приватного партнерства у сфері національної безпеки має стати невід'ємною умовою збереження і розвитку України. Крім того, розроблення відповідних засад упровадження державно-приватного партнерства у сфері національної безпеки України вимагають міжнародні зобов'язання нашої держави, зазначені в конвенціях ООН та Ради Європи у сфері безпеки.

Водночас упровадження механізму державно-приватного партнерства потребує розв'язання багатьох проблем – від розроблення базової та вдосконалення чинної законодавчої бази до розбудови довіри між державою і приватним сектором.

Практичні підходи до державно-приватного партнерства вимагатимуть сприйняття приватного учасника саме як партнера, а не підпорядкованого суб'єкта. Одним з наслідків цього є вимога спільного розроблення конкретних заходів партнерства. Відсутність формалізованих політико-правових механізмів державно-приватного партнерства не дозволяє прозоро захистити ані інтереси держави, ані інтереси бізнесу і витісняє вирішення низки важливих проблем взаємодії у непублічну сферу.

Спільні проєкти ДПП мають бути всебічно обґрунтованими, проаналізованими щодо можливих ризиків. Коли партнерські відносини між державним і приватним секторами стануть невід'ємною складовою частиною системи національної безпеки України, певні функції, ризики виконання яких можуть мати критичні наслідки, здійснюватимуться виключно державним сектором.

2. Питання механізмів і перспектив упровадження державно-приватного партнерства у сфері національної безпеки пропонується розглянути на засіданні Ради національної безпеки і оборони України. Це

може надати додатковий імпульс процесу його нормативно-правового та інституційного оформлення. У проєкті рішення РНБО України доцільно передбачити:

- розроблення проєкту Закону про внесення змін до Закону України «Про національну безпеку України» (розділ 1, ст. 1), якими чітко передбачити суб'єктність недержавного (приватного) сектору безпеки у системі національної безпеки України, зокрема зазначити, що недержавний (приватний) сектор безпеки є невід'ємною складовою частиною системи забезпечення національної безпеки України; імплементувати ці положення Закону у Стратегію національної безпеки України;
- розроблення проєкту Закону про внесення змін до Закону України «Про державно-приватне партнерство» щодо включення окремого розділу «Державно-приватне партнерство у сфері національної безпеки», зважаючи на всі особливості такого партнерства в частині захисту інформації;
- розроблення законопроєктів, які стимулюватимуть розвиток державно-приватного партнерства в окремих сферах, а також приватного ринку безпекових послуг;
- розроблення законопроєктів про внесення відповідних змін до пов'язаних законодавчих актів України.

3. На підставі оновленого законодавства у сфері ДПП та проведення огляду недержавних структур безпеки пропонується розробити Стратегію розвитку державно-приватного партнерства у забезпеченні національної безпеки, в якій, зокрема, передбачити розвиток недержавного (приватного) сектору національної безпеки України.

4. Пропонується також створити робочий орган при РНБО України з питань координації діяльності органів виконавчої влади та сектору безпеки і оборони з недержавними структурами безпеки або делегувати зазначені завдання урядовому координаційному органу з питань забезпечення національної стійкості.

Додатки

Додаток 1
Державно-приватне партнерство у сфері національної безпеки
у Сполучених Штатах Америки

Додаток 2
Огляд національного законодавства іноземних країн
у сфері забезпечення національної безпеки,
яке передбачає можливість залучення приватних структур
до заходів із забезпечення захисту публічних місць,
об'єктів критичної інфраструктури та забезпечення кібербезпеки

Додаток 3
Ідеї механізмів взаємодії для формулювання стратегічних завдань
розвитку ДПП у кіберсфері

Додаток 1

Державно-приватне партнерство у сфері національної безпеки у Сполучених Штатах Америки

У США державно-приватне партнерство має своє окреме визначення: це співпраця між державним сектором (урядом) і приватним (некомерційним) сектором, яка включає контракти на обслуговування, ланцюжки постачань, спеціальні партнерські відносини з питань поширення інформації, а також взаємодію з так званими цивільними аналітично-ситуаційними безпековими центрами (civic security switchboards).

Низка американських науковців у своїх працях підкреслювали, що участь приватного сектору є невід'ємною складовою частиною захисту національної безпеки та об'єктів критично важливої інфраструктури, а обговорення ролі приватного сектору в інших сферах, таких як розвідка, кібербезпека, транспортна безпека, охорона здоров'я, зниження ризиків тощо, демонструє поступове розуміння впливу бізнесу та його послуг на національну безпеку США.

З часів Другої світової війни державно-приватне партнерство залишалося важливим елементом національної безпеки. Приватний сектор змінював та перепрофільовував виробництво відповідно до пріоритетів часу, щоб задовольнити потреби уряду. Так, наприклад, Ford Motor свого часу побудувала цілий комплекс з виробництва військових літаків.

Зважаючи на нинішні широкі масштаби державно-приватного партнерства у сфері національної безпеки США, далі наведено чотири основні напрями та сфери, де ДПП досягло найбільшого успіху.

Захист об'єктів критичної інфраструктури

Відповідно до Директиви Президента США PPD-21 «*Про політику безпеки та стійкість критичної інфраструктури*», майже 85 % об'єктів критично важливої інфраструктури країни перебуває під охороною приватного сектору, що має вкрай важливе значення для національної безпеки США. *Міністерство внутрішньої безпеки США* (DHS) створило координаційний орган для полегшення обміну інформацією

та планування між державним і приватним секторами. *Управління захисту інфраструктури* (OIP) у рамках DHS займається аналізом загроз і уразливостей, координацією на національному та місцевому рівнях з підприємствами та урядовими установами, а також зниженням ризиків у таких секторах: хімічна промисловість, комерційні об'єкти, найважливіші виробничі підприємства, греблі, аварійні служби, ядерні реактори, матеріали та відходи. *Консультативна рада з партнерства в галузі критичної інфраструктури* (CISA) є основним стратегічним органом, що функціонує при DHS. CISA є зразком того, як партнерські відносини між державним і приватним секторами безпеки підвищують захист об'єктів критично важливої інфраструктури у США.

Кібербезпека

Компанії, які займаються інформаційними технологіями, відіграють украй важливу роль у досягненні національних цілей кібербезпеки у США. Наприклад, *Національний альянс з кібербезпеки* (NCSA) – це організація, яка підвищує обізнаність із проблемами кібербезпеки і надає користувачам можливість захистити себе від електронних загроз. Партнерство між державним та приватним секторами має вирішальне значення для місії NCSA. До Ради NCSA входять представники таких компаній як: AT&T Services Inc., Cisco Systems, Lockheed Martin, Microsoft, Google, Facebook, Bank of America, Visa та ін. Демонструючи співпрацю між NCSA і федеральним урядом, DHS започаткував найбільш помітну ініціативу, відому як *Щорічний національний місяць обізнаності про кібербезпеку* (NCSAM), який є прикладом партнерських відносин між державним та приватним секторами у сфері кібербезпеки.

Управління надзвичайними ситуаціями

Керівники підрозділів безпеки та ризиків приватних транснаціональних корпорацій, котрі мають власні штаб-квартири у США, дедалі активніше беруть участь в окремих аспектах національної безпеки, у т. ч. за напрямами захисту критичної інфраструктури, кібербезпеки чи безпеки портів. При цьому в рамках управління надзвичайними ситуаціями є окремий напрям взаємодії на рівні ДПП, а саме

реагування та діяльність з відновлення у випадку критичних аварій та надзвичайних ситуацій. Таке партнерство відбувається за координації *Федеральної агенції з надзвичайних ситуацій* (FEMA). Прикладами взаємодії є співпраця між державним і приватним секторами щодо подолання наслідків урагану «Катрина» та розливів нафти.

Безпека морських і авіаційних портів

Американські порти є життєво важливими центрами економічної діяльності у США. Наприклад, лише морські порти у США щорічно обробляють понад 2 млрд т вантажів. При такому великому обсязі товарів і кількості людей, що переміщуються, питання безпеки є національним пріоритетом. А так зване *Митне партнерство у боротьбі з тероризмом* (C-TPAT) є ініціативою приватного сектору, яка була підтримана урядом і створена для підвищення безпеки ланцюжків постачання продукції, сировини та матеріалів. Сьогодні понад шість тисяч американських компаній сертифіковано урядом у рамках програми C-TPAT, а це означає, що вони підтримують тісні робочі відносини з митницею та прикордонною службою США, можуть отримувати державні гарантії щодо ризиків свого ланцюжка постачань і допомагати державі у їх мінімізації. Такі програми, як C-TPAT, корисні для національної безпеки в забезпеченні широкої адміністративної основи для регулярної координації державного та приватного секторів.

Ще одним прикладом державно-приватного партнерства у США є так звана *Партнерська програма скринінгу в аеропортах* (SPP). У рамках цієї ініціативи приватні охоронні компанії, котрі мають відповідну кваліфікацію, виконують обов'язки, аналогічні покладеним на *Федеральне управління транспортної безпеки* (TSA) в аеропортах США.

Переваги та недоліки ДПП в інтересах національної безпеки

Партнерські відносини між державним та приватним секторами сприятимуть використанню різноманітних ресурсів, спеціалізації, міжсекторальній довірі, технологічним інноваціям тощо. Такі партнерські відносини мають значні позитивні наслідки для практики управління процесами, вирішення правових та етичних проблем,

прозорості взаємостосунків, розширення участі приватного сектору та довгострокового планування. Вони спроможні подолати бюрократичні бар'єри всередині уряду, посилити національну безпеку способами, які є неможливими для уряду чи бізнесу, коли вони діють поодинці.

Водночас відомі випадки, коли державно-приватне партнерство у сфері безпеки США не виправдовувало очікувань через невиконання окремими гравцями рекомендацій уряду. Зважаючи на розглянуте, доходимо такого висновку: хоча партнерські відносини між державним і приватним секторами є невід'ємною складовою частиною системи національної безпеки США, проте існують певні напрями, які мають зберігатися виключно за державним сектором.

Розуміння внутрішньої безпеки у США дедалі більше пов'язане не з тими чи тими агентствами, які координують таку співпрацю, а з ***налагодженням партнерства між ними***. Гнучкість, адаптивність і стійкість стали визначальними рисами програм національної безпеки на всіх рівнях управління.

Джерела

1. Beauregard R. A. Public-Private Partnerships as Historical Chameleons. Partnerships in Urban Governance: European and American Experience / ed. by Jon Pierre. London : MacMillan Press, 1997.
2. Closs D. J., McGarrell E. F. Enhancing Security throughout the Supply Chain : Special Report Series / IBM Center for the Business of Government, 2004.
3. Goldsmith S., Eggers W. D. Governing By Network: The New Shape of the Public Sector. Washington, DC : Brookings Institution, 2004.
4. Public-Private Policy Partnerships / ed. by Pauline V. Rosenau. Cambridge, MA : MIT Press, 2000.
5. Regan B. L. Enhancing Emergency Preparedness and Response: Partnering with the Private Business Sector. [Master's Thesis]. Naval Postgraduate School, 2009.
6. Schaeffer P. V., Loveridge S. Toward an Understanding of Types of Public-Private Cooperation. *Public Performance & Management Review*. 2002. 26:2.
7. Sheffi Y. Supply Chain Management under the Threat of International Terrorism. *International Journal of Logistics Management*. 2001.12:2.

Віктор Іванович Панчак,
голова правління Представництва ASIS International в Україні,
член правління Асоціації професіоналів корпоративної безпеки України,
віцепрезидент Компанії SK Security LLC, перший в Україні сертифікований
професіонал з корпоративної безпеки за найвищим глобальним стандартом CPP® –
Certified Protection Professional (сертифікат № 22432)

Додаток 2

Огляд національного законодавства іноземних країн у сфері забезпечення національної безпеки, яке передбачає можливість залучення приватних структур до заходів із забезпечення захисту публічних місць, об'єктів критичної інфраструктури та забезпечення кібербезпеки[60]

Огляд законодавства та національних стратегій безпеки переважно зосереджено на країнах, які за останні 5–10 років зазнали масштабних та резонансних терористичних атак. У більшості цих країн останніми роками відбулася істотна модернізація законодавства та стратегій у сфері забезпечення національної безпеки, основні акценти перенесено від заходів, спрямованих на протидію зовнішній агресії, до заходів із протидії гібридним загрозам, тероризму й кібератакам.

Спільною рисою є декларативний і реальний розвиток приватно-публічного партнерства у сфері протидії кіберзагрозам і терористичним атакам.

У деяких країнах (Австралія та Франція) передбачено збільшення ролі та прав представникам приватних охоронних структур у забезпеченні попередження терактів у громадських місцях.

Зважаючи на широкий і мінливий спектр загроз, які постали перед Україною, доцільно вивчити та імплементувати іноземний досвід залучення приватних структур до системи забезпечення національної безпеки за напрямами захисту об'єктів критичної інфраструктури, кібербезпеки та кіберзахисту, а також попередження терактів і забезпечення безпеки у громадських місцях.

Дані щодо безпекових документів різних країн та їхніх основних положень подано в *таблиці*.

[60] Підготовлено АПКБУ.

Таблиця

Держава	Основні документи у сфері національної безпеки	Основні положення концепції національної безпеки держави	Роль та місце приватного сектору безпеки у системі національної безпеки
Австралія та **Нова Зеландія**	Стратегія Австралії щодо захисту місць скупчення людей від тероризму (2017 р.) Стратегія Австралії щодо забезпечення кібербезпеки (2016 р.) ACT Security Industry Act 2003	• Національне законодавство не містить окремого закону, який визначав би основні засади забезпечення національної безпеки. • Уряд країни визначає стратегію національної безпеки за напрямами та реалізує її через відповідний план дій. • Визначає скупчення людей як місце, яке значна кількість людей відвідує на передбачуваній основі. • Власники та оператори місць скупчення людей, незалежно від форм власності, зобов'язані провести оцінку ризиків та аналіз вразливостей таких місць і забезпечити розробку, запровадження, вдосконалення та регулярний перегляд заходів із попередження терористичних атак. • Заохочує та рекомендує залучення приватних провайдерів безпеки до реалізації таких заходів. • Визначає основні напрями, за якими здійснюється забезпечення національної кібербезпеки та затверджує План дій за цими напрямами	Приватні провайдери та професіонали безпеки відіграють центральну роль у забезпеченні захисту місць скупчення людей від терористичних атак, оскільки в більшості випадків саме вони є першими, хто реагує на інцидент. Уряд забезпечує високий професіоналізм та достатню тренованість працівників приватної безпеки у спосіб запровадження жорсткого регулювання порядку працевлаштування, підготовки та реєстрації приватних охоронців. Приватний сектор розглядається як основний партнер у сфері забезпечення кібербезпеки. Взаємодія координується через Національний міжвідомчий центр кібербезпеки. Передбачено створення спільних центрів обміну інформацією про кіберзагрози на національному рівні та на рівні окремих штатів. Уряд забезпечує допомогу в організації кіберзахисту приватних підприємств через Національний Центр реагування на кіберінциденти (CERT)
США	Закон про національну безпеку (National Security Act 1947) Стратегія національної безпеки США (2018 р.)	• Національне законодавство містить окремий закон про національну безпеку, що переважно регулює питання, пов'язані із оголошенням та веденням війни. • Зростання конкурентоспроможності товарів місцевого виробництва.	Приватний сектор не відображено у Стратегії національної безпеки США 1947 року. Але держава залишає за собою **право використовувати приватний сектор** у разі виникнення загрози національній безпеці США.

	Закон про об'єднання та посилення Америки у спосіб надання інструментів, необхідних для виявлення та припинення тероризму (USA PATRIOT Act 2001). New York Police Department Shield Project	• Розвиток співпраці у торгово-економічних сферах. • Зменшення кількості іноземних позик (один із ключових моментів). • Після терактів 2001 року роль приватного сектору у забезпеченні безпеки об'єктів критичної інфраструктури значно розширено	В USA PATRIOT Act приватний сектор розглядається як один із основних елементів забезпечення безпеки об'єктів критичної інфраструктури та запроваджуються механізми публічно-приватного партнерства у цій сфері, залучаючи приватні корпорації та недержавні організації. Прикладом реалізації положень цього нормативного акта є програма «Щит» Департаменту поліції міста Нью-Йорка, яка передбачає використання структур приватної безпеки у загальній системі попередження та реагування на терористичні акти
Франція	Кодекс внутрішньої безпеки Франції (2012 р.) Стратегія національної оборони та безпеки (2017 р.) Національна стратегія кібербезпеки (2015 р.). Закон про попередження та протидію загрозам публічній безпеці та терористичним атакам на публічному транспорті (2016 р.) План дій проти радикалізації та тероризму (2018 р.)	• Питання забезпечення внутрішньої безпеки країни визначаються окремим кодифікованим актом. • Мінімізація зовнішніх ризиків. • Ліквідація бар'єрів для суб'єктів підприємництва. • Незалежність від зовнішніх факторів, що впливають на пріоритетні сектори економіки країни. • Після резонансних терактів національне законодавство зазнало змін, які, серед іншого, розширили роль приватних компаній із забезпечення безпеки	Прямих посилань на публічно-приватне партнерство у Кодексі внутрішньої безпеки та національної стратегії оборони та безпеки **не зазначається**. **Значну увагу приватно-публічному партнерству приділяє національна стратегія забезпечення кібербезпеки.** Закон про попередження та протидію загрозам публічній безпеці та терористичним атакам на публічному транспорті та кілька декретів президента республіки значно розширюють роль приватних структур у забезпеченні охорони об'єктів критичної інфраструктури, надають приватним охоронцям право носити та застосовувати вогнепальну зброю

Продовження табл.

Держава	Основні документи у сфері національної безпеки	Основні положення концепції національної безпеки держави	Роль та місце приватного сектору безпеки у системі національної безпеки
Велика Британія	Біла книга про національну безпеку і оборону Великої Британії Стратегія національної безпеки та стратегічний огляд сфери оборони та безпеки (2015 р.) Закон про індустрію приватної безпеки (Private Security Industry Act 2001) City of London Police ACT (Action Counters Terrorism) Awareness Program (Project Griffin)	• Боротьба з міжнародним тероризмом і розповсюдженням зброї масового знищення. • Нейтралізація транснаціональних загроз, що поширюються з територій так званих «проблемних» країн. • Посилено національне законодавство у сфері боротьби з міжнародним тероризмом; збільшено фінансовий контроль над організаціями, підозрюваними у причетності до терористичної діяльності	Доктрина ґрунтується на схемі, яка поєднує готовність спеціальних служб до надзвичайних ситуацій за участю **пересічних громадян** у забезпеченні безпеки на місцях. **Роль приватного сектору безпеки безпосередньо не окреслено.** Незважаючи на відсутність чіткого законодавчого регулювання залучення приватних охоронних структур до заходів із забезпечення національної безпеки, поліція Лондона вже кілька років реалізує Програму «Дії проти тероризму» (Проєкт Грифон), яка, серед іншого, передбачає використання структур приватної безпеки у загальній системі попередження та реагування на терористичні акти. Також стратегія національної безпеки передбачає реалізацію заходів із забезпечення кібербезпеки та захисту ОКІ у тісному партнерстві із приватним сектором
Японія	Біла книга оборони (2019 р.)	Політична безпека за допомогою створення трикутника «США – Японія – Європа»	Уряд визнав можливість участі сил **самооборони** у військових заходах.

		Економічна безпека спрямована на вирішення конфлікту Захід – Схід та Північ – Південь у спосіб надання зовнішньої допомоги, вкладення в міжнародні інститути з метою підтримки політики США. Військова безпека, спрямована на оборону островів Японії та створення спільно зі США «базових сил оборони»	Сучасна політика безпеки зазнала глобальних змін: • істотно розширено зону відповідальності; переглянуто законодавчу базу оборонної політики і функції **сил самооборони**; • кардинально переосмислено ставлення до висунутих самообмежень, зокрема **права на колективну самооборону** і права на військові дії
Німеччина	Біла книга про національну безпеку і оборону ФРГ (2016 р.)	Тісний контакт з питань міжнародної та національної безпеки з союзниками і партнерами. Використання комплексного підходу до забезпечення всіх аспектів безпеки (внутрішніх і зовнішніх, політичних, економічних, екологічних, соціальних та ін.). Реалізація принципу превентивності, який передбачає раннє виявлення криз і завчасне запобігання їх небезпечних наслідків.	Тісний контакт з питань міжнародної та національної безпеки з **союзниками і партнерами**, використання комплексного підходу до забезпечення всіх аспектів безпеки (внутрішніх і зовнішніх, політичних, економічних, екологічних, соціальних та ін.), а також реалізація принципу превентивності, який передбачає раннє виявлення криз і завчасне запобігання їхнім небезпечним наслідкам. **Прямих посилань на публічно-приватне партнерство не вказано**
Іспанія	Закон «Про національну оборону» (2005 р.) Стратегія національної безпеки (2017 р.)	Стратегія складається з 5 розділів, у яких розглядаються 12 ризиків для національної безпеки Іспанії, серед яких: збройні конфлікти, тероризм, кіберзагрози, організована злочинність, економічна і фінансова нестабільність, енергетична вразливість, нелегальна імміграція, поширення зброї масового знищення, шпигунство, надзвичайні ситуації природного характеру і катастрофи, вразливість морських кордонів і об'єктів життєзабезпечення і основних служб.	У якості новел законодавства у сфері національної безпеки Іспанії **закріплюються необхідність державно-приватного співробітництва в галузі національної безпеки і розвиток серед громадян Іспанії «культури безпеки»**

Закінчення табл.

Держава	Основні документи у сфері національної безпеки	Основні положення концепції національної безпеки держави	Роль та місце приватного сектору безпеки у системі національної безпеки
Польща	Стратегія національної безпеки Республіки Польща (2014 р.; 2020 р. – нова редакція)	Польща міцно закріпилася в європейських та євроатлантичних структурах. Є близьким союзникам США. Залежність Польщі від постач енергоносіїв є однією із зовнішніх загроз її безпеці. Першочерговими завданнями є поліпшення якості життя громадян, модернізація збройних сил, розвиток співпраці із «союзними арміями», зміцнення міжнародних позицій держави. НАТО є для РП найважливішою формою багатосторонньої співпраці, опорою стабільності в Європі, а також основою трансатлантичних відносин	Основними напрямами втілення Стратегії національної безпеки РП є: • здійснення реформ у невоєнних безпекових галузях (ухвалення доктрини щодо кіберзахисту); • реформування цивільної оборони; • інвестиції в енергетичну безпеку; **• залучення волонтерських організацій до безпекової системи**
Румунія	Нова Стратегія національної оборони Румунії (2015–2019 р.)	Пріоритетними цілями Стратегії нацбезпеки є забезпечення належного справедливого правосуддя і верховенства закону, забезпечення ефективності національних програм з попередження криз та антикризового управління, зміцнення безпеки транспортної та енергетичної інфраструктур і кібернетичної безпеки. Консолідація ролі країни в НАТО і ЄС, стратегічне партнерство Румунії з США, забезпечення безпеки у Чорноморському регіоні та поглиблення співробітництва з сусідніми країнами і країнами, що утворюють східний фланг НАТО	**Відомчі асоціації та компанії, котрі спеціалізуються у сфері надання послуг з безпеки та охорони, об'єднані під егідою Конфедерації служб безпеки, яка позиціонується як єдиний орган, що репрезентує приватний сектор безпеки у відносинах з публічним сектором**

Сінгапур	Акт індустрії приватної безпеки	Запровадження Координаційного Секретаріату Концепції економічної безпеки держави. Публічно-приватне партнерство у сфері національної безпеки. Прозора координація державою нормативно-правової бази, яка формує основу національної концепції – економічної безпеки держави	Публічний та приватний сектори безпеки є складовою частиною концепції національної економічної безпеки держави, яка адміністративно управляється профільним віце-прем'єрміністром. Приватний сектор визначає свої засадничі положення документом PRIVATE SECURITY INDUSTRY ACT. Документ встановлює основні ризики, які приватний сектор рекомендує залучити до Концепції національної економічної безпеки держави, а саме: 1) потреба у застосуванні багатогранного підходу до подолання кіберзагроз; 2) усунення соціальних розладів, спричинених технологічним процесом; 3) сприяння діалогу **публічно-приватного сектору** безпеки у питаннях боротьби з фальшивими новинами

Додаток 3

Ідеї механізмів взаємодії для формулювання стратегічних завдань розвитку ДПП у кіберсфері

Стандарт мінімальної кіберзахищеності бізнесу

a. Проблема. Бізнес готовий упроваджувати системи управління інформаційною і кібербезпекою, але через відсутність типового підходу та мінімального стандарту захищеності впровадження засобів захисту є нерівномірним, фрагментарним, непорівнюваним. Держава намагається регулювати стандарти безпеки держустанов, при цьому інколи розповсюджуючи аналогічну практику на приватний сектор, який виявляє спротив моделі заборон і державного примусу, навіть стосовно об'єктів критичної інфраструктури (ОКІ), не використовуючи системних підходів до розвитку ДПП. Через те, що існує велика кількість різних за величиною приватних підприємств, вони дуже повільно напрацьовують свої практики захисту, здебільшого вже після нанесення їм матеріальних чи репутаційних збитків від кібератак.

b. Гіпотеза. Прискорення процесу підвищення рівня захищеності приватного сектору відбудеться, якщо держава на принципах партнерства запропонує новий Стандарт мінімальної кіберзахищеності бізнесу (на прикладі аналогічного британського досвіду), законодавчо закріпивши механізм упровадження Стандарту на добровільній основі. Такий механізм має саморегулюватися.

c. Механізм реалізації. Розробити Стандарт мінімальної кіберзахищеності бізнесу (держава в особі ДССЗЗІ), який запропонувати бізнесу використовувати за декларативним принципом. Оцінку відповідності Стандарту має проводити юридична особа приватного права на добровільній платній основі. Така особа має видавати Сертифікат відповідності, підписаний кваліфікованим електронним цифровим підписом (ЕЦП). Реєстр юридичних осіб, які погодилися проводити оцінку відповідності, ведеться за декларативним принципом у вигля-

ді публічного рейтингу (хостинг та адміністрування сторінки публічного рейтингу – держструктура, можливо, РНБОУ), а уповноважена особа лише модерує кожний запис на предмет наявності та відповідності ЕЦП). Стандарт має бути простим, зрозумілим, виконуваним, дешевим, таким, що легко перевіряється та піддається автоматизованій перевірці.

d. Очікуваний результат. Яскравий приклад дієвого ДПП, за якого найбільш масовий сектор приватного бізнесу отримає орієнтир рівня мінімальної захищеності, а держава – стрімке зростання захищеності бізнесу в цілому, активізацію ринку захисних систем та послуг, збільшення бюджету в довгостроковій перспективі.

Механізм скоординованого розкриття вразливостей

a. Проблема. Україна має значний потенціал розвитку сегмента ринку, пов'язаного з пошуком і торгівлею вразливостями програмного забезпечення (ПЗ), але через недостатню врегульованість цієї сфери «розкривачі» вразливостей мають ризик потрапити під кримінальну відповідальність, а підприємства, на яких вразливості наявні, не мають надійного механізму їх отримати. При цьому в державі розвивається «чорний ринок» уразливостей, який приваблює спецслужби інших країн та міжнародний кримінал. Регулювання, що його використовує нині держава, є рестриктивним, та не досягає своєї мети.

b. Гіпотеза. Якщо забезпечити централізований механізм збору й оцінки вразливостей, застосувавши міжнародно визнані стандарти та таксономії вразливостей силами держави, але децентралізувати сфери платного отримання вразливостей від «розкривачів» та надання їх бізнесу, забезпечивши анонімність відносин між бізнесом і «розкривачами» перед державою, не буде потреби у рестриктивній моделі управління, що суттєво поліпшить бізнес-клімат у державі.

c. Механізм реалізації. Запровадити схему скоординованого розкриття вразливостей (за прикладом ЄС), які централізовано та на умовах анонімності надаються до органу колективного управління вразливостями, до якого на партнерських засадах (50/50) залучаються державні органи та представники профільного бізнесу для проведен-

ня безоплатної оцінки, критерії якої мають бути публічними. Результати оцінювання безкоштовно надаються тій юридичній особі приватного права, яка надала публічне зобов'язання виплати винагороди «розкривачеві» вразливості на умовах забезпечення його анонімності та за рахунок власника інформаційного активу чи системи, в якій вразливість була виявлена.

d. Очікуваний результат. За рахунок дієвого ДПП в Україні буде створено новий ринок скоординованого розкриття вразливостей, зменшено криміногенні ризики та відбудеться значне поліпшення захищеності бізнесу від кіберзагроз.

Відкриті дані

a. Проблема. Знеособлення персональних даних (ПД) під час поширення відкритих даних здійснюється у примітивний спосіб (видалення), що вносить плутанину в набори відкритих даних та суттєво зменшує можливості їх автоматизованої обробки. Така технічна проблема суттєво звужує межі ДПП у тих випадках, коли механізми партнерства спираються на відкриті дані, зменшуючи кількість та якість послуг бізнесу (корпоративна розвідка, аналіз судових рішень).

b. Гіпотеза. Якщо під час знеособлення ПД не видаляти ключові ідентифікатори, а шифрувати їх у спосіб, який не дозволить зворотного розшифровування, але буде достатнім для ототожнення записів, проблема буде вирішена.

c. Механізм реалізації. Розробити універсальний механізм криптографічного перетворення окремих ідентифікаторів фізичних і юридичних осіб, що видаляються під час публікації наборів даних, які підлягають оприлюдненню у формі відкритих даних. Механізм має забезпечити ототожнення таких ідентифікаторів без можливості їх зворотного розшифрування, що гарантуватиме необхідну деперсоналізацію даних під час їх оприлюднення у формі відкритих даних, але суттєво збільшить придатність таких масивів для автоматизованої обробки.

d. Очікуваний результат. Відбудеться суттєве збільшення можливостей ДПП у тих випадках, коли механізми партнерства спираються на відкриті дані, підвищиться конкуренція, знизиться привабливість ринку «викрадених масивів даних».

Стимулювання соціальної відповідальності бізнесу

a. Проблема. Недосконалість державного регулювання обігу ПД призвела до неможливості власника ПД проконтролювати їх обробку або відкликати згоду на їх обробку. Якщо зобов'язання України про захист ПД будуть виконуватись у спосіб упровадження рестриктивних правил та державного примусу, взаємодія суспільства і держави з приводу обігу ПД буде конфліктною.

b. Гіпотеза. Якщо делегувати вирішення цієї проблеми бізнесу, ініціювати утворення такого, що саморегулюється, механізму контролю обробки та обігу ПД на комерційній основі, зокрема відкликання раніше наданого дозволу на їх обробку, то проблема може бути врегульована без державного примусу та у неконфліктний спосіб.

c. Механізм реалізації. Виконання вимоги на видалення персональних даних або заборону їх подальшої обробки на добровільній платній основі має ініціювати юридична особа приватного права, забезпечуючи при цьому ведення обліку кількості вимог та фактів їх добровільного виконання кожним розпорядником персональних даних, який заздалегідь уклав відповідну угоду з цією юридичною особою приватного права. Реєстр юридичних осіб, які вирішили надавати такі послуги, ведеться за декларативним принципом у вигляді публічного рейтингу соціальної відповідальності розпорядників ПД (хостінг та адміністрування сторінки публічного рейтингу – Уповноважений з прав людини).

d. Очікуваний результат. Розпорядники, які отримали дозвіл від володільців ПД на їх обробку, будуть змушені захищатися від репутаційних ризиків, позаяк їхній рейтинг соціальної відповідальності залежатиме від обліку кількості вимог і фактів їх добровільного виконання кожним розпорядником персональних даних. Зацікавленість юридичних осіб приватного права у веденні публічного обліку базується на отриманні оплати від власників ПД, які обиратимуть для себе оператора управління ПД на конкурентній основі. Після опрацювання модель може бути використано в інших проблемних сферах як краща практика ДПП.

Міжнародний захист ІТ-бізнесу

a. Проблема. Обмежені можливості захисту бізнесу на міжнародному рівні від великих корпорацій та недружніх «регуляторних» дій окремих держав, які намагаються поширити «свій цифровий суверенітет» на територію України, зокрема й на ринки розробки ПЗ, у сфері контролю ПД, упровадження систем колективного захисту, дистрибуції ПЗ. Приватному сектору не вистачає партнерських відносин з державою, яка взяла на себе регулювання зовнішньої та міжнародної діяльності, але з часткою проблемних відносин приватного бізнесу з іноземними суб'єктами державні інституції не спроможні впоратись. З боку іноземних партнерів також відбувається розрив очікувань: вони пропонують підтримку, звертаючись першочергово до державних установ, які не мають кваліфікованого персоналу та можливостей для розвитку таких відносин, або не зацікавлені у вирішенні проблемних питань (навіть інколи самі їх створюють).

b. Гіпотеза. Потрібен міжнародний бізнес-омбудсмен кіберсфери, який представлятиме на міжнародному рівні інтереси українського ІТ-бізнесу та зможе допомагати у з'ясуванні спірних питань, вирівнюючи умови та статус у вирішенні проблем між українським бізнесом та міжнародними корпораціями.

c. Механізм реалізації. Створити при МЗС або Урядовому офісі з питань європейської та євроатлантичної інтеграції окрему дорадчу структуру підтримки на добровільних засадах, яка ініціює та організує постійно діючу конференцію з питань нових моделей відносин та розвитку ДПП у сфері міжнародних проблем ІТ-бізнесу.

d. Очікуваний результат. За рахунок концентрації проблемних питань та скарг буде напрацьовано практику вирішення спорів та запропоновано нові моделі відносин.

Інші проблеми ДПП у сфері кіберзахисту

1. Відсутність державних стандартів і механізмів управління ризиками та забезпечення безпеки в цих сферах. Дефіцит кадрів та профільної експертизи як у державному, так і в приватному секторах.

2. За рідкісним винятком (банки та енергетика дещо роблять у цій сфері) – відсутні механізми обміну інформацією та координації спільних зусиль на національному, регіональному та галузевому рівнях.

3. Слабкість механізмів міжнародної співпраці в цих сферах, відсутність стабільних контактів і постійного обміну інформацією та досвідом з іноземними органами, що відповідають за співпрацю у сфері захисту критичної інфраструктури (КІ) і кібербезпеки (КБ), без яких забезпечення захисту в умовах глобалізації – це практично нездійсненне завдання.

4. Відсутність довіри до державних органів, відповідальних за захист КІ та КБ з боку власників і операторів відповідних об'єктів і систем. Усі раніше пропоновані державою механізми «партнерства» у цій сфері, фактично партнерством не є, оскільки ґрунтуються на державному примусі й створюють додаткові збитки, або незручності бізнесу, а паралельно сприяють подальшому зростанню чисельності та зниженню ефективності державного апарату.

Дії держави, спрямовані на вирішення проблем

a. Формування національних стандартів та мінімальних вимог у сфері управління ризиками КІ та КБ. Публікація цих стандартів, їх популяризація, організація навчання фахівців приватного сектору. Створення профільного ринку послуг, на якому держава буде лише регулятором і одним із споживачів. Державні органи не повинні займатися оцінкою ризиків і перевірками на відповідність стандартам, за винятком перевірок своїх власних систем управління ризиками.

b. Припинення практики створення нескінченного переліку національних центрів та органів, для яких на ринку немає (і ніколи не буде) достатньої кількості кваліфікованого персоналу. Держава може і повинна купувати відповідні послуги на тендерній основі у приватному секторі, зберігаючи за собою контролюючу (в рамках конкретних контрактів) і координуючу функції.

c. Створення системи стимулів для забезпечення обміну інформацією та координації зусиль у цій сфері. Наприклад, надання захищеної платформи для збору та аналізу інформації про кібератаки, регулярне

інформування партнерів з приватного сектору про актуальні загрози та методи протидії, координація зусиль з відбиття кібератак, надання експертної допомоги у забезпеченні захищеності об'єктів, підвищення кваліфікації профільних фахівців, допомога держави наявним галузевим об'єднанням та ініціативам у підготовці та впровадженні необхідної нормативної бази.

d. Створення ефективного механізму міжнародного співпраці в цій сфері з урахуванням потреб та очікувань приватного сектору.

e. Мінімізація контролюючої та каральної ролі держави, формування профільної нормативної бази на основі принципів взаємовигідної співпраці між приватним сектором та державними органами. Створення передумов для делегування окремих державних завдань і функцій у сфері забезпечення безпеки приватним структурам на комерційній основі. Так, фізична охорона, експлуатація технічних систем безпеки, аудити систем управління ризиками, моніторинг та аналіз кіберзагроз, реагування на кіберінциденти, їх первинне розслідування та багато інших функцій можуть і повинні здійснюватися найбільш підготовленими і компетентними комерційними організаціями в рамках виконання держзамовлень. Це буде і дешевше, і ефективніше, ніж створення додаткових державних структур і безуспішних спроб сформувати необхідний ресурсний і кадровий потенціал за рахунок державного бюджету.

Максим Юрійович Літвінов,
кандидат юридичних наук,
Віктор Володимирович Дроботенко –
члени Асоціації професіоналів корпоративної безпеки України,
Представництва ASIS International в Україні, експерти з кібербезпеки

Наукове видання

Оксана Дмитрівна МАРКЄЄВА,
Броніслав Леонович РОЗВАДОВСЬКИЙ

ДЕРЖАВА ТА ПРИВАТНИЙ СЕКТОР НА ЗАХИСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ВІД ВЗАЄМОДІЇ ДО ПАРТНЕРСТВА

Аналітична доповідь

Відповідальна за випуск *І. О. Корецька*
Верстка *І. О. Корецька*
Редагування: *І. О. Корецька, Т. М. Філіппова*
Коректура *Т. В. Карбовнича*

Формат 60x90/$_{16}$. Ум. друк. арк. 4,5.
Наклад 150 прим. Зам. № ____

Видання підготовлено до друку
в Національному інституті стратегічних досліджень
вул. Пирогова, 7А, Київ, 01030
Тел./факс: (044) 234-50-07
e-mail: info-niss@niss.gov.ua
http://www.niss.gov.ua

ФОП Євенок О.О.
м. Житомир, вул. М. Бердичівська, 17 А
Polygraphyinzt@gmail.com
Свідоцтво суб'єкта видавничої справи ДК № 3544 від 05.08.2009 р.