НІСД НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ
NATIONAL INSTITUTE FOR STRATEGIC STUDIES NISS

Аналітична записка
Серія «Національна безпека», № 3, 2019

ПРО ДЕЯКІ АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

С. І. Кондратов, старший науковий співробітник
відділу енергетичної та техногенної безпеки
Національного інституту стратегічних досліджень

В аналітичній записці розглянуто стислий аналіз проблем започаткування та розвитку державно-приватного партнерства (ДПП) у сфері забезпечення захисту та стійкості критичної інфраструктури (КІ) в Україні. Виділено основоположні принципи побудови партнерських стосунків у цій сфері. Надано стислий аналіз проблем започаткування ДПП в Україні. Сформульовано ряд конкретних рекомендацій РНБО України та ЦОВВ, які будуть залучені до захисту КІ в Україні.

1. Вступ

Серед численних інфраструктурних об'єктів і систем, від яких залежить повсякденне життя населення, суспільства та держави, останнім часом особливу увагу привертає ***критична інфраструктура (КІ)***. У державах-членах НАТО та ЄС цей термін означає ті об'єкти і системи (далі – об'єкти), знищення або вихід з ладу (повний або частковий) яких призвів би до швидких важких наслідків з точки зору життєдіяльності населення, безпечного функціонування суспільних інститутів і державних органів, національної економіки, національної безпеки і оборони.

Національні системи захисту КІ країн-членів НАТО та ЄС розраховані на запобігання виникненню кризових ситуацій і на протидію розвитку кризових сценаріїв, які можуть реалізовуватися через припинення надання життєво-важливих послуг і доступу до ключових ресурсів, розповсюдження негативних наслідків безпекової події в результаті *ефектів доміно* та *каскадних ефектів* на інші об'єкти, які можуть належати до інших секторів економіки, соціальної сфери, сфери національної безпеки і оборони.

Відтак, із самого визначення КІ та процедури віднесення об'єктів до неї випливає, що державна система забезпечення захисту та стійкості КІ, її параметри, плани і процедури реагування на безпекові інциденти та кризи мають бути розраховані на ймовірну реалізацію найбільш небезпечних комплексних сценаріїв, що ***потребує забезпечення готовності до мобілізації усіх наявних в державі ресурсів, належного рівня координації дій, взаємодії та обміну інформацією між суб'єктами такої системи.*** До останніх слід віднести, насамперед, компетентні державні органи, державні служби надання допомоги у надзвичайних ситуаціях, місцеві органи влади та місцеві громади, ***власників та операторів об'єктів, віднесених до КІ.***

У країнах-членах НАТО та ЄС частка об'єктів, віднесених до КІ, які знаходяться у приватній власності, може сягати 85 % (приклад – США), і це обумовлює виключну важливість взаємовідносин між державою і приватним сектором у цій сфері. Це знайшло своє відображення у національних

законодавствах згаданих країн, державних планах та програмах, в яких, як правило, йдеться про ***необхідність розбудови саме "державно-приватного партнерства".***

На теперішньому початковому етапі створення державної системи захисту КІ в Україні, за відсутності національного переліку об'єктів КІ, можна лише приблизно оцінювати, яка їх частка буде представляти приватний сектор. Тим не менше, зарубіжний досвід та роль, яку відіграють приватні компанії у таких галузях національної економіки, як наприклад, енергетика і зв'язок, дозволяє стверджувати, що взаємовідносинам між державою і приватним сектором у цій сфері в Україні також має бути надана пріоритетна увага.

Далі представлений короткий огляд основних підходів до розв'язання проблем розвитку ДПП у країнах-членах НАТО та ЄС.

2. Огляд підходів до розв'язання проблем розвитку ДПП у сфері забезпечення захисту і стійкості КІ (ЗСКІ)

При розгляді загальних підходів до започаткування та розбудови ДПП у сфері забезпечення ЗСКІ, а також проблем, які виникають на цьому шляху, в даній публікації були використана інформація, представлена в аналітичний доповіді "*Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України*", підготовленій відділом інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень (НІСД). Це пов'язане з тим, що кібербезпека є одним з головних напрямів забезпечення безпеки КІ, а проблеми розвитку ДПП у сфері кібербезпеки значною мірою схожі з тими, що існують у сфері захисту КІ.

Зарубіжні дослідження показують, що сприятливі умови для партнерства у сфері безпеки КІ створюються там, де сторони дійшли розуміння, що ***поодинці жодна з них не здатна забезпечити досягнення***

цілей захисту КІ.

Разом з тим, таке розуміння не може виникнути автоматично, адже ***для цього потенційні партнери повинні мати спільне бачення рівня загроз та ризиків для об'єктів КІ, що у свою чергу, потребує наявності у них спільного доступу до певних масивів інформації***. Наприклад, це може, з одного боку, стосуватися інформації про діяльність та плани терористів, а з іншого, – стану контртерористичного захисту на конкретному об'єкті КІ, включаючи його потенційні уразливості, заходи, що вживаються власником/оператором для зменшення відповідних ризиків тощо.

Належний рівень обміну інформацією між суб'єктами має ключове значення для розвитку ДПП, оскільки є основою для створення атмосфери довіри між партнерами. Така атмосфера є важливою умовою ефективності процесу, адже капіталовкладення у безпеку здійснюються, в основному власниками/операторами об'єктів КІ, і вони мають бути переконані, що такі інвестиції є необхідними. Таке переконання може сформуватися лише на основі належної поінформованості.

Таким чином у рамках ДПП держава повинна взяти на себе зобов'язання щодо надання надійної та своєчасної інформації про загрози і ризики для КІ. Натомість, приватний сектор, у свою чергу, має інформувати державні органи про суттєві зміни на об'єктах КІ, про поточний стан безпеки конкретних об'єктів, їх можливі уразливості та заходи з метою зменшення відповідних ризиків тощо.

Водночас, спільне усвідомлення необхідності розвивати започатковане ДПП, включаючи обмін інформацією, не звільняє процес від принципових труднощів, пов'язаних з ***потребою у постійному пошуку балансу між заходами із забезпечення безпеки та конкурентоздатністю бізнесу, а також між необхідністю в обміні інформацією та вимогами до захисту інформації з обмеженим доступом***, у т.ч. розвідувальної та комерційної. У рамках цього напряму державний сектор має забезпечити умови, які будуть

стимулювати інвестиції власників/операторів об'єктів КІ у безпекові заходи, а приватний сектор має усвідомлювати у повній мірі свою відповідальність за безпеку об'єктів КІ.

Очевидно, що сталий розвиток ДПП потребує надійної організаційно-правової основи (про досвід США див. Приклад 1 у Додатку). У більшості країн-членів НАТО та ЄС застосовуються схожі підходи до ДПП, але, звичайно, з урахуванням національних особливостей. При цьому, відповідні стратегії, програми, плани дій тощо приймаються на виконання нормативно-правових актів (НПА) національного рівня (див. Приклад 2 у Додатку).

У передових країнах світу для розбудови ДПП використовують різноманітні інструменти, серед яких важливе місце займають ***координаційні ради, форуми і платформи, які забезпечують контакти, обмін інформацією, узгодження позицій між партнерами на постійній основі*** (про досвід США див. Приклад 3 у Додатку).

Для започаткування ДПП в Україні з використанням апробованих у НАТО та ЄС підходів, слід виділити ряд ключових вимог до процесу реалізації концепції партнерства.

На думку експерта з Нідерландів Вінсента Коувенховена (*Vincent Kouwenhoven*), ДПП не можливе за відсутності:

- ***взаємної довіри та встановлених обмежень, спрямованих на недопущення зловживань;***
- чітких, недвозначних цілей та стратегій, зафіксованих у документах;
- чіткого розподілу ризиків, відповідальності та повноважень.

Серед перелічених умов найважливішою, очевидно, є досягнення довіри між суб'єктами взаємодії. Адже виконання решти умов є апріорі не можливим, якщо сторони не довіряють одна одній.

Деякі західні експерти вважають, що ознакою зрілого ДПП у сфері безпеки є ***неієрархічність зв'язків у взаємовідносинах між державою та***

приватним бізнесом, коли рішення приймаються у рамках консенсусної моделі.

При цьому, навіть при зацікавленості сторін у партнерстві, ***процес його розбудови може наштовхуватися на проблеми, обумовлені відмінністю очікувань суб'єктів процесу щодо його результатів.***

Зокрема, ***з боку державних органів***, які несуть загальну відповідальність за безпеку КІ, інтерес до ДПП, ймовірно, буде полягати у такому:

- намаганні залучити кошти приватного сектору до фінансування певних безпекових заходів;
- спільному використанні різноманітних ресурсів;
- отриманні доступу до певної інформації щодо вразливості об'єктів КІ, у т.ч. стосовно кібератак;
- отриманні доступу для зовнішніх сил реагування на майданчики об'єктів КІ для тренувань і навчань.

Натомість, можна з упевненістю припускати, що для ***приватного сектору*** ДПП буде виглядати найбільш привабливим у такому:

- можливості участі у формуванні державної політики у сфері захисту КІ у т.ч.:
  - через участь своїх представників у розробці проектів НПА;
  - через участь своїх представників у діалозі з державними органами у консультативних (дорадчих) радах, на відповідних форумах і платформах;
- отриманні податкових пільг для інвестування у заходи з безпеки об'єктів, віднесених до національної КІ;
- своєчасному отриманні від компетентних державних органів надійної інформації (у т.ч. розвідувальної) про загрози та ризики елементам КІ;
- методологічній підтримці з боку держави щодо забезпечення

готовності КІ адекватно реагувати на загрози та ризики, включаючи відповідне навчання та тренування.

Наявність належних НПА щодо розвитку ДПП у сфері захисту КІ є необхідною умовою для забезпечення сталості процесу. Документальне оформлення партнерства здійснюється, зокрема, через підписання спільних документів (меморандумів) про партнерство. Такі документи, як правило, включають положення про цілі та завдання партнерства, про спільне бачення існуючих і потенційних загроз та ризиків, про необхідність співпраці для їх зменшення тощо.

Відповідно до кращого зарубіжного досвіду, крім документального оформлення партнерства, рекомендовано ***налагодження особистих стосунків між партнерами*** (про досвід США див. Приклад 4 у Додатку).

Вище обговорювалися, головним чином, напрями ДПП, які охоплюють взаємовідносини типу "державні органи − власники/оператори об'єктів КІ", але практика ДПП далеко не обмежується цією парою основних суб'єктів. Наприклад, у США та Великій Британії ***велика увага приділяється залученню приватних компаній до науково-технічних досліджень*** з метою впровадження інноваційних технологій для захисту КІ. (див. Приклад 5 у Додатку стосовно досвіду Великої Британії).

При цьому, на думку колишнього високопосадовця Міністерства внутрішньої безпеки США, а нині керівника приватної компанії Тома Челлуччі (Tom Cellucci), цей напрям партнерства можна ще більше посилити, якщо урядові установи у повній мірі усвідомлять ринкову привабливість завдань, що стоять перед ними і зможуть чітко й коротко (у форматі функціональних вимог) сформулювати для приватного сектору, у чому полягає проблема та надати йому оцінку обсягів потенційного ринку споживачів.

На основі вивчення зарубіжного досвіду можна зробити висновок, що незважаючи на певні складнощі у реалізації національних моделей

ДПП, необхідність його розбудови у країнах-членах НАТО та ЄС є загальновизнаною.

На завершення цього стислого огляду, націленого на виокремлення суттєвих особливостей процесу розбудови ДПП, сформулюємо кілька загальних міркувань щодо урахування зарубіжного досвіду в цій сфері в Україні, а саме:

1. Стан ДПП у сфері захисту КІ значною мірою відображає загальний стан взаємовідносин "держава – приватний бізнес" у тій чи іншій країні.

2. Унікальність ситуації, в якій перебуває кожна країна, створює й унікальні умови при запровадженні навіть апробованих в інших країнах підходів. Тому спроби механічного перенесення зарубіжного досвіду без урахування національної специфіки можуть сформувати серйозні ризики для реалізації відповідних проектів і програм.

3. З іншого боку, необхідність урахування національних особливостей, зовсім не означає відсутності будь-яких закономірностей та фундаментальних принципів, які випливають з практики їх застосування у світі. Їх недооцінка чи ігнорування можуть призвести до фактичного нівелювання або, навіть, провалу започаткованих реформ і програм.

3. Проблеми започаткування та розвитку ДПП у сфері захисту КІ України

Потреба у започаткуванні ДПП у сфері захисту КІ обумовлена тим, що ефективне ДПП є одним з базових елементів державної системи забезпечення ЗСКІ, необхідність у створенні якої випливає:

по-перше, з надскладної безпекової ситуації, в якій перебуває наша країна, що характеризується "повним" спектром загроз та ризиків щодо об'єктів, які будуть віднесені до КІ;

по-друге, із заявленого Україною зовнішньополітичного курсу, що вимагає максимального зближення національних безпекових підходів, у т.ч. у сфері захисту КІ, з тими, які прийняті у країнах-членах НАТО та ЄС.

Звичайно, досягнення цілей розвитку ДПП у сфері захисту КІ не можливе без прогресу у вирішенні більш загального питання – ***прийняття профільного закону про критичну інфраструктуру та її захист***, розробка якого передбачена рішенням РНБО України та відповідним президентським указом, виданим ще у січні 2017 р. і не виконаним до цього часу.

Робота над цим законопроектом невиправдано затягнулася внаслідок ряду причин, серед яких у контексті даної теми необхідно звернути увагу на таке:

1. Представники деяких державних органів при обговоренні першої редакції законопроекту, підготовленої в Національному інституті стратегічних досліджень (НІСД), зробили акцент на тому, що термін "державно-приватне партнерство" згідно з чинним на той момент законодавством стосувався лише економічної діяльності, тому його використання у законопроекті вони оцінили як недоречне.

2. Внаслідок такої позиції та несприйняття концепції ДПП в процесі внесення змін до першої редакції законопроекту термін "державно-приватне партнерство" та відповідні положення про його започаткування і розвиток були вилучені з проекту закону.

3. Намагання деяких міністерств та відомств просувати суто відомчі підходи й інтереси призвело до того, що до тексту законопроекту були включені положення, які жодним чином не можна розцінювати як такі, що будуть сприяти створенню атмосфери довіри між державним і приватним секторами.

Повертаючись до заперечень щодо використання терміну "державно-приватне партнерство", слід погодитись з тим, що чинним ЗУ "Про державно-приватне партнерство" формат партнерства у взаємовідносинах між державою та приватним сектором у сфері національної безпеки і оборони не передбачений. Але це зовсім не означає, що така ситуація має бути законсервована. Більш того, чинним ЗУ "Про національну безпеку

України" (набрав чинності 08.07.2018) механізми ДПП розглядаються, як інструменти реалізації Стратегії національної безпеки України (Стаття 26), Стратегії розвитку оборонно-промислового комплексу України (Стаття 30), а також Стратегії кібербезпеки України (Стаття 31). Тобто, цим законом, з одного боку, була спростована хибна позиція щодо неможливості використання терміну у сфері нацбезпеки і оборони, а з іншого, – були створені правові підстави для розвитку національного законодавства у необхідному напрямі.

Певну інформацію для роздумів надало також і проведення засідання створеної при НІСД міжвідомчої експертної робочої групи на тему розбудови ДПП у сфері захисту КІ в Україні, яке відбулося 18.04.2019 р. Зокрема, на запрошення не відгукнувся жоден з найбільших приватних банків України та міжнародних аеропортів Києва. Незначний інтерес проявили і національні провайдери мобільного зв'язку. Натомість, активну участь в обговоренні взяли представники енергетичних компаній (як державних, так і приватних), ПрАТ "Київводоканал", Українського союзу промисловців і підприємців. Інтерес до питань ДПП виявили і більшість ключових державних органів. Таким чином, засідання показало, що на даний момент у приватному секторі існує далеко неоднозначне ставлення до перспектив розвитку ДПП щодо КІ.

Як відзначалося вище, ДПП являє собою тип взаємовідносин між державним та приватним секторами, який на цей момент визнано найбільш оптимальним для сфери захисту КІ у країнах з розвинутою ринковою економікою та високою правовою культурою, до кола яких прагне долучитися і Україна. Це обумовлює необхідність пошуку "своєї" моделі ДПП у сфері захисту КІ, яка, з одного боку, запроваджувала основоположні принципи такого партнерства, а з іншого – враховувала специфічність безпекових, фінансово-економічних та інших умов, у яких перебуває наша країна.

Виходячи з наведеного вище, далі викладено ряд рекомендацій, спрямованих на реалізацію концепції ДПП у сфері забезпечення захисту та стійкості КІ в Україні.

4. Рекомендації

На основі огляду зарубіжного досвіду, прикладів найкращої практики та аналізу поточної ситуації навколо розбудови державної системи захисту КІ в Україні, а також беручи до уваги виключно важливу роль, яку має відіграти ДПП у цій сфері, вважаємо за доцільне надати такі рекомендації:

Апарату Ради національної безпеки і оборони України:

1. Розглянути можливість включення до плану роботи РНБО України на 2019 рік питання підготовки законопроекту "Про критичну інфраструктуру та її захист" з метою прискорення його представлення на розгляд Верховної Ради України.

2. У рамках завдань з реформування сектору національної безпеки і оборони проаналізувати стан взаємовідносин між державою та приватним сектором у сфері національної безпеки і оборони з метою розробки плану першочергових заходів, спрямованих на розв'язання проблем, що накопичилися у цій сфері.

3. Розглянути можливість включити до згаданого у пункті 2 плану розробку проекту Закону України "Про державно-приватне партнерство у сфері національної безпеки і оборони" та ініціювати розробку цього проекту законодавчого акту, зважаючи на те, що прийняття закону закладе, серед іншого, фундамент для імплементації положень статей 26, 30 та 31 чинного Закону України "Про національну безпеку України".

4. При розробці згаданого у п. 3 законопроекту включити до нього відповідні положення щодо державно-приватного партнерства при забезпеченні захисту та стійкості критичної інфраструктури.

5. Ініціювати розробку глосарію у сфері національної безпеки і оборони України задля підвищення ефективності функціонування сектору

безпеки і оборони через удосконалення процедур та планів взаємодії (у т.ч. у рамках державної системи захисту критичної інфраструктури), що не можливо без використання єдиного понятійно-термінологічного апарату.

Мінекономрозвитку України:

6. Підготувати довідковий матеріал для засідання РНБО України щодо стану готовності законопроекту "Про критичну інфраструктуру та її захист", включивши в нього пропозиції щодо доопрацювання законопроекту в т.ч. щодо відновлення діяльності відповідної робочої групи;

7. При доопрацюванні законопроекту "Про критичну інфраструктуру та її захисту" урахувати зауваження і пропозиції, що стосуються ДПП, максимально наблизивши підходи України у цій сфері з тими, що є загальновизнаними у країнах-членах НАТО та ЄС, шляхом:

- запровадження терміну "державно-приватне партнерство";
- вилучення із законопроекту положень, які суперечать умовам розбудови ДПП на основі довіри та взаємної вигоди партнерів.
-

МВС України, Міненерговугілля України, Мінінфраструктури, Держспецзв'язку України:

Рекомендувати, надати доручення профільним структурним підрозділам опрацювати питання створення робочих груп за участі представників приватного сектору, наукових установ, незалежних експертів з метою розробки проектів типових документів (положень) про консультативні ради (платформи) з питань державно-приватного партнерства у сфері забезпечення захисту та стійкості критичної інфраструктури.

ДОДАТОК

Приклад 1. У США забезпечення партнерства, насамперед між державою та приватним сектором, включено до семи основоположних принципів виконання чинного Плану захисту національної інфраструктури 2013 (NIPP 2013[1]), прийнятого на виконання Політичної директиви Президента США (PPD-21[2]). Крім того, до згаданих принципів у документі віднесене набуття знань про ризики для КІ та про взаємозалежності між її елементами, а обмін відповідною інформацією у т.ч. у рамках ДПП, визнається імперативною вимогою для створення атмосфери довіри між усіма залученими сторонами.

Приклад 2. У Національній стратегії захисту критичної інфраструктури Німеччини як одне з ключових положень, зафіксовано зобов'язання забезпечувати підхід до захисту КІ на основі співробітництва між державними органами, службами надання допомоги і кризового реагування, приватними операторами та їх асоціаціями, науковими і дослідними установами, промисловими компаніями у сфері безпеки, міжнародними та наднаціональними структурами, а також населенням.

Приклад 3. У США ДПП розцінюється, як "фундамент для реалізації ефективних стратегій забезпечення безпеки та стійкості критичної інфраструктури"[3]. Міністерство внутрішньої безпеки США створило Консультативну раду з питань партнерства при захисті критичної інфраструктури (Critical Infrastructure Protection Advisory Council, CIPAC), що виконує роль форуму, на якому представники уряду та приватного сектору, організовані у координувальні ради, мають можливість разом брати участь у широкому спектрі заходів, спрямованих на безпеку та стійкість КІ. Крім того, у США створені секторальні координаційні ради (Sector Coordinating Councils), урядові координаційні ради (Government Coordinating Councils) та

[1] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[2] Presidential Policy Directive -- Critical Infrastructure Security and Resilience [Електронний ресурс]. – Режим доступу: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[3] Critical Infrastructure Partnership Advisory Council [Електронний ресурс]. – Режим доступу: https://www.dhs.gov/critical-infrastructure-partnership-advisory-council

міжсекторальні ради (cross-sector councils). Наприклад, щодо сектору комерційних об'єктів (СКО), Урядова координаційна рада координує діяльність залучених до забезпечення безпеки СКО державних органів. Натомість, Секторальна координаційна рада здійснює координацію дій операторів і власників об’єктів та систем сектору, які у свою чергу поділені на підсектори, що мають власні координаційні ради, а також різноманітні робочі групи й професійні об’єднання за конкретними безпековими напрямами.

Приклад 4. У США рекомендовано, ще до настання кризових умов розвивати особисті взаємини з офіційними представниками місцевих безпекових агенцій (пожежниками, службами швидкої медичної допомоги, представниками госпіталів, іншими правоохоронними відомствами тощо), місцевим бізнесом, організаціями місцевих спільнот, а також з державними офіційними особами (мерами, управлінцями міської влади, главами округів, штатів та представниками федеральних органів тощо). Визнано, що наявність "попередньо встановлених стосунків з ключовими особами… та обговорення з ними надзвичайних ситуацій і планів буде забезпечувати значно кращі контакти і швидке отримання допомоги у разі, якщо надзвичайна ситуація трапиться".

Приклад 5. Шість приватних компаній у Великій Британії отримали фінансування на суму, що перевищує 460000 фунтів на розробку технологій швидкого виявлення осіб, які мають при собі ножі, перебуваючи у великих скупченнях людей на вулицях, залізничних станціях у ході публічних заходів. Фінансування виділене після жорсткого первинного відбору і призначене для підготовки компаніями упродовж шести місяців ґрунтовних доказів перспективності запропонованих ними технологічних рішень.[4]

[4] Government funds research into knife-detection technology [Електронний ресурс]. – Режим доступу: https://www.gov.uk/government/news/government-funds-research-into-knife-detection-technology