ЄВРОПЕЙСЬКЕ ПРИВАТНО-ДЕРЖАВНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРБЕЗПЕКИ: ПІДХОДИ ДО ФОРМУВАННЯ ТА НОРМАТИВНО-ПРАВОВІ ЗАСАДИ

Анотація

Розглянуто законодавство ЄС щодо приватно-державного співробітництва у сфері кібербезпеки. Досліджено пріоритетні напрями стратегії співпраці приватного та державного сектору в галузі кібербезпеки, окреслено колізії, складнощі та точкове неспівпадіння інтересів різних учасників процесу.

Ключові слова: кібербезпека, стратегія Європейського приватно-державного співробітництва.

ЄВРОПЕЙСЬКЕ ПРИВАТНО-ДЕРЖАВНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРБЕЗПЕКИ: ПІДХОДИ ДО ФОРМУВАННЯ ТА НОРМАТИВНО-ПРАВОВІ ЗАСАДИ

Одним із пріоритетних завдань Стратегії кібербезпеки України є налагодження співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури, розвиток державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період[1]. Водночас реальні процеси налагодження ефективного державно-приватного партнерства у сфері кібербезпеки поки що знаходяться в початковому стані, а чинні форми такого партнерства обмежуються діяльністю Громадських рад при основних суб’єктах національної системи кібербезпеки держави.

[1] http://zakon2.rada.gov.ua/laws/show/96/2016#n11

На противагу цьому ЄС, який активно розбудовує власні спроможності для забезпечення кібербезпеки держав-членів, так само здійснює і масштабну діяльність у налагоджені державно-приватного партнерства у сфері кібербезпеки.

Сучасний стан *acquis communautaire*[2] в галузі кібербезпеки на загальноєвропейському рівні знаходиться в точці свого найінтенсивнішого розвитку. З огляду на системність характеру загроз для кібербезпеки у поєднанні з постійним зростанням кіберзлочинності в останні роки, Європейська Комісія у співпраці з країнами-членами ЄС, іншими інституціями Європейського Союзу та відповідними зацікавленими сторонами розробила узгоджену політику дій, що має регулювати цей сектор.

Згідно проведеного у 2017 р. Pricewaterhouse Cooper опитування,[3] щонайменше 80 % європейських компаній досвідчили принаймні одного інциденту протягом останніх трьох років у галузі кібербезпеки.

У липні 2016 р. Європейська Комісія після низки громадських консультацій з усіма зацікавленими сторонами підписала угоду в галузі індустрії кібербезпеки, тим самим активізувавши зусилля, спрямовані на боротьбу з кібер-загрозами у формі державно-приватного партнерства[4].

План дій, ініційований Європейською Комісією (Agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats),[5] окреслив рамки державно-приватного партнерства в галузі кібербезпеки, що надалі регулюватимуть цю сферу правових та економічних відносин. На реалізацію цієї стратегії було виділено 450 мільйонів євро, основним джерелом перерозподілу коштів є програма досліджень та інновацій «Горизонт 2020». Також учасники ринку кібербезпеки представлені Європейською

---

[2] Acquis communautaire (з фр. *доробок спільноти*) сукупність спільних прав і зобов'язань, обов'язкових до виконання для усіх країн-членів ЄС. Доробок постійно змінюється і узагальнюється. правова система Європейського Союзу, яка включає акти законодавства Європейського Союзу (але не обмежується ними), прийняті в рамках Європейського співтовариства, Спільної зовнішньої політики та політики безпеки і Співпраці у сфері юстиції та внутрішніх справ.

[3] Огляд глобального стану інформаційної безпеки 2017, http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[4] http://europa.eu/rapid/press-release_IP-16-2321_en.htm

[5] http://europa.eu/rapid/press-release_IP-16-2321_en.htm

організацією з кібербезпеки (ECSO) задекларували намір реалізації своїх інвестицій у рамках цієї ініціативи.

Метою партнерства є створення платформи для кібербезпеки різних секторів, таких, як енергетика, охорона здоров'я, транспорт та фінанси, а також включення в цей процес органів влади, науково-дослідних центрів та інших зацікавлених сторін, платформи, яка розвивала б дослідницький та інноваційний потенціал сектору. Така співпраця покликана зменшити негативний ефект роздробленості ринку кібербезпеки ЄС, неповної його врегульованості, що виявляється у різниці в процедурах сертифікації, з тим, щоб кожен постачальник послуги в галузі кібербезпеки міг реалізувати свою діяльність у кожній країні-члені ЄС однаково, легко уникаючи політики протекціонізму.

Ці рамки співпраці підкреслюють особливу важливість інновацій, що з'являються на перетині інтересів вищезгаданих учасників ринку – від нішевих ринків, на кшталт криптографії, з одного боку, до добре розвинених ринків з новими бізнес-моделями (наприклад, ринок антивірусного програмного забезпечення). Даною ініціативою Європейська Комісія намагалась полегшити доступ до виходу на нові ринки підприємствам малого та середнього бізнесу, що працюють у галузі кібербезпеки.

Основою цілого плану дій слугують *Стратегія єдиного цифрового ринку (Digital Single Market Strategy for Europe)* 2015 р.[6], *Кіберстратегія Європейського Союзу* 2013 р. (Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace)[7] та *Директива ЄС щодо мережевої та інформаційної безпеки (NIS* Directive on security of network and information systems*)*, яка має бути включена в національне законодавство країн-членів ЄС

---

[6] https://ec.europa.eu/commission/priorities/digital-single-market_en , http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

[7] https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

до 9 травня 2018 р. та у внутрішні статутні документи основних підприємств до 9 листопада 2018 р.[8].

Прийнята у 2013 р. *Європейська стратегія кібербезпеки*[9] визначила спільне бачення Європейської комісії та Високого представника Європейського Союз із закордонних справ та політики безпеки щодо відкритого та безпечного кіберпростору.

Стратегія визначає основні пріоритети, що регулюють проблеми як внутрішньо європейського, так і міжнародного законодавства. Пріоритети цієї ініціативи стосуються підвищення рівня захисту та стійкості європейських мереж та розвитку промислових і технологічних ресурсів для забезпечення кібербезпеки.

У відповідності до Стратегії у 2013 р. Європейська Комісія запропонувала перший всеосяжний елемент законодавства ЄС щодо кібербезпеки – *Директива ЄС щодо мережевої та інформаційної безпеки* (NIS Directive on security of network and information systems)[10]. Після трьох років переговорів цей документ був прийнятий із поправками, далі послідувала його імплементація на національному рівні.

Також *Директива ЄС щодо мережевої та інформаційної безпеки* (NIS Directive on security of network and information systems) передбачила створення координаційного механізму реагування держав-членів у координації з приватним сектором на погрози та власне самі кібер-атаки, тим самим сприяючи стратегічному співробітництву та обміну інформацією, підтримуючи рівень довіри між учасниками процесу. Комісія також запустила державно-приватну платформу на рівні ЄС – т.зв. *Платформу мережевої та інформаційної безпеки (Network and Information Security (NIS) public private Platform)*[11] для визначення ефективної практики кібербезпеки з метою сприяння подальшому впровадженню Директиви. Результатом діяльності

[8] https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

[9] http://eur-lex.europa.eu/procedure/EN/202369

[10] COM/2013/048 - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0048

[11] https://ec.europa.eu/digital-single-market/en/news/nis-platform-kick-meeting-working-groups

Платформи у третьому кварталі 2015 р. став *Стратегічний порядок денний дослідження кібербезпеки* (SRA - Cybersecurity Strategic Research Agenda) на базі Платформи мережевої та інформаційної безпеки[12].

Окрім вищеперелічених ініціатив, Європейська Комісія фінансує через FP7 та CIP (7 Рамкову Програму та Програму з Конкурентоспроможності та Інновацій) ще ряд проектів з кібербезпеки. Підтримка також надається з фондів Рамкової програми Horizon 2020.[13]

Відповідно до Постанови (ЄС) № 460/2004 Європейське співтовариство заснувало у 2004 р. *Європейське агентство з мережевої та інформаційної безпеки* (*ENISA - European Union Agency for Network and Information Security*)[14] з метою сприяння забезпеченню високого рівня розвитку культури інформаційної безпеки в межах ЄС. Пропозиція щодо модернізації мандату ENISA була прийнята 30 вересня 2010 р. [15] Переглянута нормативно-правова база електронних засобів зв'язку[16], яка діяла з листопада 2009 р., передбачала зобов'язання щодо безпеки постачальників електронних засобів зв'язку,[17] а також зобов'язання країн-членів до травня 2011 р. транспонувати ці положення у законодавство на національному рівні.

Відтак, усі сторони, у віданні яких є персональні дані, – до прикладу банки чи лікарні, – відповідно до нормативно-правової бази захисту даних[18] зобов'язані були запровадити заходи безпеки для захисту цих персональних даних. Крім того, відповідно до пропозиції Європейської Комісії від 2012 р. щодо Загального регулювання захисту даних,[19] т. з. "контролери даних", повинні повідомляти національні наглядові органи про порушення режиму персональних даних.

---

12 https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/view

13 SWD(2016) 210

14 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

15 COM(2010) 521.

16 Див. http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

17 Статті 13a та 13b Рамкової директиви.

18 Директива 2002/58 від 12 липня 2002

19 http://eur-lex.europa.eu/procedure/EN/201286

Відповідно до *Директиви Ради 2008/114 / ЄС від 8 грудня 2008 р. Про ідентифікацію та проектування європейської критичної інфраструктури та оцінку необхідності покращення її захисту (Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)* в Європейській програмі захисту критично важливої інфраструктури[20] визначено загальний «парасольковий» підхід до захисту критично важливої інфраструктури в ЄС. *Директива про безпеку мережі та інформаційних систем* повинна застосовуватися без шкоди для Директиви 2008/114.

На міжнародному рівні ЄС працює над кібербезпекою як на двосторонньому, так і на багатосторонньому рівні. На саміті ЄС-США 2010 р.[21] було створено робочу групу з питань кібербезпеки та кіберзлочинності. Також є низка мультилатеральних угод щодо співпраці у цій галузі із Організацією економічного співробітництва та розвитку, Генеральною Асамблеєю Організації Об'єднаних Націй, Міжнародним союзом електрозв'язку, Організацією з безпеки та співробітництва в Європі, Всесвітнім самітом з питань інформаційного суспільства (WSIS) та Форумом з питань управління Інтернетом (IGF).

6 травня 2015 р. Європейська комісія прийняла Стратегію єдиного ринку цифрових технологій (DSM)[22]. Дана політика стала ще одним із започатковуючих положень для регулювання державно-приватного партнерства з питань кібербезпеки у сфері технологій та рішень для забезпечення мережевої безпеки впродовж 2016 р.

Колізії, складнощі та точкове неспівпадіння інтересів різних учасників процесу. Проблематика та механізми взаємодії

---

20 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

22 https://ec.europa.eu/commission/priorities/digital-single-market/

Не зважаючи на те, що державно-приватне партнерство є вигідним для обох секторів, деякі приватні компанії зволікають із виконанням законодавства в цій сфері. Одним із ключових каменів спотикання є питання довіри, контролю та розкриття корпоративної інформації.

Довіра приватних підприємств

Компанії мають сумнів стосовно залучення уряду в розслідування справи після того, як кібератака на їхню компанію вже відбулась, позаяк це передбачає відкриття доступу до приватних даних компанії. Існує точка зору серед представників приватного сектору, що участь уряду лише ускладнить ситуацію. Крім того, у момент, коли приватна компанія залучає урядовий орган до розслідування кібератаки, компанія втрачає автономію щодо такого розслідування.

Оскільки певна інформація може бути класифікована як конфіденційна, багато компаній вважають, що обмін інформацією призведе до потенційних втрат позиції на ринку[23]. Крім того, деякі приватні компанії також можуть турбуватися, що передача конфіденційної інформації може пошкодити їхній репутації, тобто що відкрита для урядового розслідування інформація не залишиться конфіденційною після завершення такого розслідування[24].

Ще однією проблемою є складний регуляторний і правовий ландшафт у галузі кібербезпеки, у випадку порушення якого компанії можуть бути вимушені на більше, ніж реалізація стандартних зобов'язань щодо розкриття інформації. Приватні компанії можуть бути змушені розкривати навіть потенційні ризики уряду, Міністерству юстиції або навіть позивачам, які можуть постраждати від кіберзлочину.

У цілому ж приватні компанії відзначили відсутність довіри як ключову причину вагання щодо державно-приватної співпраці у цьому секторі[25].

---

23 http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf

24 http://www.sciencedirect.com/science/article/pii/S1874548209000274

25 https://publications.europa.eu/en/publication-detail/-/publication/80ca9f55-3dbb-11e6-a825-01aa75ed71a1

Варіанти механізмів побудови довіри

Для того, щоб зміцнити довіру між учасниками процесу в Нідерландах створили безпечну мережу інформації, до якої уряд отримує безпосередній доступ лише після того, як компанія виразить на це свою згоду.[26]

У такій моделі представники державного та приватного секторів працюють у спільній платформі над побудовою довіри, розвитком співробітництва та діалогу, враховуючи інтереси усіх учасників процесу.

Така співпраця стимулює створення нових послуг і розвиває індустрію власних програмних продуктів, поліпшує взаємодію суспільства і держави, а також підвищує прозорість діяльності та довіру до органів влади. Беручи до уваги цілі, викладені в Угоді,[27] Європейська Комісія розглянула наступні сценарії, пов'язані зі зміцненням індустрії кіберзахисту в Європі. Запропоновані варіанти були ретельно відібрані після аналізу доказів з різних джерел, включаючи дослідження ринку кібербезпеки, а також аналіз точок зору під час громадських консультацій, в яких взяли участь більше 250 різних організацій, що представляють як попит та пропозицію галузі індустрії кібер-безпеки.[28]

Ініціатива Європейської Комісії в області державно-приватного партнерство поклала початок розвитку довгострокової конкурентоспроможності та інновацій європейської кібербезпеки, втім сама по собі ще не є механізмом подолання проблеми розбалансованості внутрішнього ринку в галузі кібербезпеки.

З огляду на це, після ретельного аналізу та консультацій із зацікавленими сторонами Європейська Комісія продовжує роботу над додатковими заходами, які дозволятимуть європейським громадянам, підприємствам (включаючи малі та середні підприємства), органам державної

---

26 http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1478&context=jss

27 http://europa.eu/rapid/press-release_IP-16-2321_en.htm

28 SWD(2016) 215

влади отримувати доступ до цифрових технологій безпеки, найкращих практик забезпечення інформаційної інфраструктури.

Одним з інструментів вирішення цієї ситуації є розбудова механізму *економічних кластерів*, які можна широко визначити як групу економічних суб'єктів та інституцій, територіально розташованих неподалік і достатніх масштабів для розвитку спеціалізованої експертизи, послуг, ресурсів, умінь та навичок. Співпрацюючи разом малі та середні підприємства можуть бути більш інноваційними, створювати більше робочих місць та реєструвати більше міжнародних товарних марок та патентів, ніж ті, що працюють окремо.

Приналежність до кластеру дозволяє компаніям, що беруть участь у ініціативі, підвищити конкурентоспроможність і таким чином досягти більшої продуктивності, переважно шляхом підвищення продуктивності, завдяки покращенню доступу до спеціалізованих постачальників, технології й інформації та більш високому інноваційному потенціалу співпрацюючих компаній. Це пов'язано з передачею знань, генерацією нових ідей та акцентуванням на інноваціях. Кластери – переважно ринкове явище, найуспішніші з яких створюються спонтанно внаслідок природних конкурентних переваг на ринку.

Як окрему державну політику в ЄС цей підхід отримав наприкінці 1990-х років, з того часу бізнес-ініціативи, вищі навчальні заклади та науково-дослідні інститути сприяли розвитку та появі нових державних політик, діючи як каталізатор і допомагаючи розкрити економічний та науковий потенціал окремих регіонів. У цьому контексті в Європейському Союзі більшість кластерів, що зосереджують увагу на кібербезпеці, можна знайти в Західній Європі (G4C у Німеччині, який успішно заохотив уряд підтримувати розвиток 17 регіональних кластерів кібербезпеки, Pôle d 'Excellence Cyber у Франції, Гаазький дельта-кластер в Нідерландах або INCIBE в Іспанії), нові ініціативи починають з'являтися також у Центральній та Східній Європі, наприклад у Чехії та Естонії.

Громадські консультації

Європейська Комісія провела ряд громадських консультацій із зацікавленими сторонами щодо планування майбутньої стратегії державно-приватного партнерства в галузі кібербезпеки. Онлайн-консультація була запущена 18 грудня 2015 р. на 12 тижнів для збору різних поглядів щодо питання функціонування єдиного європейського ринку в галузі кібербезпеки. Це супроводжувалося дорожньою картою[29] кращого регулювання для державно-приватного партнерства в галізу кібербезпеки.

Європейська робоча група лідерів кібербезпеки була у той самий час заснована провідними європейськими гравцями галузі кібербезпеки. Ця група працювала над низкою конкретних рекомендацій для європейських громадян та бізнесу та промислової політики в галузі кібербезпеки. До складу робочої групи входили Airbus Group, Atos, BBVA, BMW, Cybernetica, Deutsche Telekom, Ericsson, F-Secure, Infineon та Thales.

Група представила доповідь комісару Етьєнґері в січні 2016 р. на Міжнародному форумі з кібербезпеки в Ліллі. У доповіді[30] висвітлюються рекомендації щодо заходів, спрямованих на підвищення надійності та надійності в ЄС. У доповіді також рекомендується успішний розвиток європейських чемпіонів з кібербезпеки. ***Тенденції та спостереження після проведення громадських консультацій:***

- більшість респондентів позитивно реагували на ініціативу Комісії щодо державно-приватного партнерства в галузі кібербезпеки, наголошуючи на важливості стратегічної спрямованості такої співпраці;

- критична інфраструктура, фінанси та банківська діяльність, енергетика та охорона здоров'я розглядалися учасниками опитування як такі, що можуть принести найбільше соціально-економічних збитків у випадку великої кібер-атаки;

---

29 http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf

30 http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326

- серед респондентів відмічався загальний консенсус щодо пріоритетності захисту критичної інфраструктури. Значна частина респондентів зазначила, що бракує необхідних товарів і послуг на європейському ринку для забезпечення безперервного і цілісного потоку зв'язків у галузі кібербезпеки. Це, зокрема, стосується систем виявлення кібер-нападів та управління безпекою інформації та подій, достатньої кількості програмного та апаратного забезпечення, криптографічних стандартів та надійних хмарних сервісів;

- багато респондентів висловили думку стосовно слабкої внутрішньоринкової конкурентності, а також слабкість конкурентоспроможності назовні ЄС. Хоча деякі європейські продукти та послуги, на думку респондентів, є конкурентоспроможними з їхніми відповідниками з інших частин світу, постачальники в різних країнах ЄС часто працюють у нішевих ринках, відтак не можуть швидко та без значних втрат долати національні кордони, що впливає на їх цінову конкурентоспроможність;

- більшість респондентів, особливо малий та середній бізнес, наголосили на проблемах, пов'язаних із доступом до ресурсів для фінансування проектів та ініціатив у сфері кібербезпеки. Фонди ЄС, венчурні фонди та банківські кредити розглядаються як найбільш зручні фінансові інструменти для стимулювання зростання бізнесу;

- більшість респондентів виявили, що стандартизація підтримувала інновації, оскільки вона сприяла сумісності, віддаючи перевагу комбінованому підходу до стандартизації – горизонтальним та багатогалузевим. На питання про майбутнє фокусування в галузі стандартизації, серед респондентів було досягнуто міцного консенсусу щодо захисту критично важливої інфраструктури;

- учасники опитування поділилися низкою ідей щодо того, як може працювати схема сертифікації – від єдиного європейського рівня, відповідального за визначення будь-яких необхідних стандартів або вимог до

угод про взаємне визнання, що залишаються центральними [31]. У той же час значна частка респондентів заявила, що вони не знають, чи схеми сертифікації взаємно визнаються, роблячи припущення, що однак наразі вони не є взаємно визнаваними в усіх країнах-членах ЄС;

- багато учасників консультацій висловили думку про необхідність інтенсифікувати обмін інформацією між приватними структурами та урядом в області розвідувальної інформації в секторі інформаційної безпеки, оскільки питання кібербезпеки є по своїй сутності транскордонною проблемою.

Висновки

1. З метою оптимізації та впорядкування державно-приватного партнерства у сфері кібербезпеки, після ретельного аналізу та консультацій із зацікавленими сторонами Європейська Комісія ініціювала план дій, що дозволить європейським громадянам, підприємствам (включаючи малі та середні підприємства), органам державної влади отримувати доступ до цифрових технологій безпеки, найкращих практик забезпечення інформаційної інфраструктури.

2. Основою актуального плану дій слугують Стратегія єдиного цифрового ринку (Digital Single Market Strategy for Europe) 2015 р., Кіберстратегія Європейського Союзу 2013 р. (Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace) та Директива ЄС щодо мережевої та інформаційної безпеки (NIS Directive on security of network and information systems), яка має бути включена в національне законодавство країн-членів ЄС до 9 травня 2018 р. та у внутрішні статутні документи основних підприємств до 9 листопада 2018 р.

3. Консультації були попередньо проведені з такими цільовими групами, як великий бізнес, малий та середній бізнес, асоціації, дослідницькі інституції, академія, громадський сектор, органи державної влади, органи

[31] Senior Officers Group for Information Systems agreement (Council Decision of March 31st 1992 (92/242/EEC))

регіонального рівня. Тривалість консультацій у випадку ініціативи Єврокомісії становила 12 тижнів.

4. Багато учасників консультацій висловили думку про необхідність інтенсифікувати обмін інформацією між приватними структурами та урядом в області розвідувальної інформації в секторі інформаційної безпеки, оскільки питання кібербезпеки є по своїй сутності транскордонною проблемою.

5. Не зважаючи на те, що державно-приватне партнерство є вигідним для обох секторів, деякі приватні компанії зволікають із виконанням законодавства в цій сфері. Одним із ключових каменів спотикання є питання довіри, контролю та розкриття корпоративної інформації.

Рекомендації

Зважаючи на необхідність вирішення проблеми державно-приватного партнерства у сфері кібербезпеки відповідно до європейських демократичних практик, пропонуються наступні кроки, здійснення яких дозволить оптимізувати зазначену сферу:

1. З метою реалізації положень Стратегії кібербезпеки України, держава потребує чіткої та зрозумілої «Стратегії державно-приватного партнерства в сфері кібербезпеки», яка має формуватись за активного залучення зацікавлених сторін і більшою мірою бути продуктом недержавного сектору, ніж державних структур.

2. Зважаючи на значну кількість стейкхолдерів у цьому процесі, він більшою мірою буде мати політичний, а не суто юридичний/технічний вимір. Зважаючи на це, ще до етапу проведення консультацій доречно розпочати заходи з підвищення довіри між учасниками ринку (недержавними суб'єктами) та державою в цілому. З цією метою в практиці інституцій ЄС ще до проведення консультацій було *створено платформу (як онлайн, так і офлайн) для обмінну дослідженнями та інноваціями, досвідом,* що має на меті формування простору довіри в учасників до процесу. Відтак,

пропонується утворення базової он-лайн платформи «**Кібердіалог**», яка має стати основою для проведення громадських консультацій із зацікавленими сторонами щодо планування майбутньої стратегії державно-приватного партнерства в галузі кібербезпеки.

3. З метою запуску платформи на базі Адміністрації Президента України (під головуванням одного з заступників Голови АПУ) пропонується утворення Ініціативної робочої групи, до якої мають увійти основні недержавні учасники ринку у сфері кібербезпеки (у т.ч. системних інтеграторів ПЗ, виробників антивірусного програмного забезпечення), представників профільних ІТ-асоціацій, а також представники наукових установ. Зазначена група проводить підготовчі заходи (семінари та робочі наради) з державно-приватного партнерства в галузі кібербезпеки (cPPP), а також з урахуванням пропозицій та зауважень галузевих недержавних суб'єктів готує базові пропозиції, які в подальшому мають стати основою платформи «Кібердіалог».

4. Діяльність цієї платформи має забезпечуватись належним комунікуванням з боку всіх державних установ, задіяних у цьому процесі: АПУ, Держспецзв'язку, СБУ, МВС, Нацбанку. Передусім, посилання на цю платформу мають бути розміщені на сайтах усіх державних установ, на ФБ-акаунтах відомств, а також, за можливості, згадуватись у виступах представників відомств для ЗМІ чи профільних публічних заходів.

5. Відповідний он-лайн проект має бути запущено на строк не менше 12 тижнів (варіант – до 24 тижнів) для збору різних поглядів щодо питання функціонування українського ринку в галузі кібербезпеки, а також з метою зібрати ключові пропозиції та зауваження зацікавлених сторін до чинної системи взаємодій меж державою та приватним сектором у сфері кібербезпеки.

6. Апарату РНБО України (у межах виконання Стратегії кібербезпеки України) запропонувати суб'єктам національної системи кібербезпеки

підготувати спільну візію державних органів на те, якою може і має бути співпраця між державою та недержавним сектором у сфері кібербезпеки.

7. Після завершення он-лайн консультацій з широкою громадськістю на базі Апарату РНБО України має бути утворено Спільну робочу групу з підготовки проекту Стратегії державно-приватного партнерства у сфері кібербезпеки, яка має максимально повно враховувати напрацювання Ініціативної групи. До процесу розробки (консультування) тексту Стратегії доречно залучити представників європейських структур, які або мають досвід створення відповідних стратегії, або задіяні сьогодні у процесах реформування сектору безпеки і оборони України: EUAM,[32] представників ЄК, які брали участь у розробці європейського плану дій (European public private partnership on cybersecurity).[33]

8. Зазначену Стратегію доцільно прийняти відповідним рішенням РНБО України в межах розвитку положень Стратегії кібербезпеки України.

В. О. Бойко,
відділ інформаційної безпеки та розвитку інформаційного суспільства,
Національний інститут стратегічних досліджень,
жовтень 2017 р.

[32] http://www.euam-ukraine.eu/ua/our-mission/our-priorities/
[33] http://europa.eu/rapid/press-release_IP-16-2321_en.htm