

ЄВРОПЕЙСЬКИЙ ДОСВІД ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА: ПІДХОДИ ДО ФОРМУВАННЯ ТА НОРМАТИВНО-ПРАВОВІ ЗАСАДИ

Бойко Вікторія Олександрівна,

кандидат історичних наук

ORCID: 0000-0002-7546-9909

У статті проаналізовано ініціативи ЄС щодо державно-приватного партнерства у сфері кібербезпеки, відзначено наскрізне акцентування на полегшення доступу підприємств малого та середнього бізнесу, що працюють у галузі кібербезпеки, до нових ринків. Досліджено пріоритетні напрями стратегії співпраці приватного та державного сектору в галузі кібербезпеки, окреслено колізії, складнощі й точкові розбіжності інтересів різних учасників процесу та можливі варіанти співпраці.

Розглянуто загальноєвропейські спроби створити платформу для забезпечення кібербезпеки різних секторів, як-от: енергетика, охорона здоров'я, транспорт та фінанси, а також долучення до цього процесу науково-дослідних центрів та інших зацікавлених сторін. Проаналізовано комплексність ситуації щодо дотримання балансу захисту об'єктів критичної інфраструктури у демократичних суспільствах з огляду на цифрову взаємозалежність та взаємопроникнення інформаційно-комунікаційних технологій та промислових систем управління. У цьому контексті у статті звертається увага на ініціативу Європейської Комісії зі створення механізму для держав-членів з метою координації із приватним сектором у сфері кіберзагроз, що покликана сприяти стратегічному співробітництву та обміну інформацією, зберігаючи при цьому рівень довіри між учасниками процесу. На загальноєвропейському рівні на виконання рішень із впровадження цієї ініціативи розпочала роботу Публічно-приватна платформа мережевої та інформаційної безпеки, що призначена для визначення ефективних практик кібербезпеки та сприяння подальшому виконанню Директиви ЄС щодо мережевої та інформаційної безпеки.

Зазначається, що, незважаючи на низку ініціатив Європейської Комісії та інших органів ЄС, багато приватних європейських компаній зволікає із виконанням законодавства в цій сфері. Одним із основних каменів спотикання є питання довіри й контролю та розкриття чутливої корпоративної інформації.

Ключові слова: кібербезпека, кіберзагрози, стратегія Європейського державно-приватного партнерства, проекти державно-приватного партнерства, Директива ЄС щодо мережевої та інформаційної безпеки, Директива Ради ЄС про ідентифікацію та проектування європейської критичної інфраструктури та оцінку необхідності покращення її захисту.

Boiko Viktoria

EUROPEAN EXPERIENCE OF PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF CYBERSECURITY: APPROACHES TO CONSTRUCTION AND LEGAL FRAMEWORK

The article analyzes the EU initiatives on public-private partnership in the field of cybersecurity, making a cross-cutting emphasis on facilitating the access of small and medium-sized businesses operating in the field of cybersecurity to the new markets.

The priority directions of the private and public sector cooperation strategy in the field of cyber security have been explored; the conflicts, difficulties and point of differences of participants' interests, as well as possible ways of cooperation have been outlined. European efforts to create platforms for securing cybersecurity in various sectors as well as the inclusion of research centers and other stakeholders in this process are considered. The complexity of the situation regarding the balance of protection of objects of critical infrastructure in democratic societies has been analyzed in the context of the digital interdependence and interpenetration of ICTs and industrial control systems. Article looks at the European Commission initiative to create a coordination mechanism for Member States to counterpart with the private sector for threats and cyber-attacks prevention, thereby promoting strategic cooperation and information exchange, while maintaining a level of trust among the participants in the process. The Commission also launched a public-private platform at the EU level, the so-called Network and Information Security (NIS) Public-Private Platform to identify effective cybersecurity practices to facilitate further implementation of the Directive.

It is noted that despite the importance of public-private partnership for all participants in the process, a number of private European companies are delaying the implementation of legislation in this area. One of the key stumbling blocks is the question of trust and control and the disclosure of sensitive corporate information.

Keywords: cybersecurity, cyber threats, European public-private partnership strategy, public-private partnership projects, EU Directive on network and information security, 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.

Постановка проблеми. Актуальні дискусії щодо державно-приватного партнерства (ДПП) у кіберсфері переважно торкаються питань необхідності створення простору безпеки та зменшення ризиків, а також збалансування безпеки із потребою інтернет-свободи та права на втручання держави у децентралізований кіберпростір¹.

Втім сприйняття кіберпростору як стійкого та децентралізованого середовища, що має здатність самоврегулюватися, у міжнародних безпекових студіях доволі швидко змінилось на бік усвідомлення необхідності контролю та регулювання з метою зменшення потенційних та реальних ризиків і загроз. Ситуацію ускладнює і той факт, що цілу низку структурних вразливостей кіберпростору неможливо усунути за рахунок спроможностей якогось окремого суб'єкта².

З одного боку, це посилює прагнення до тотальної сек'юритизації кіберсфери, що вже окреслюється як певна тенденція. Це, у свою чергу, призводить до домінування на порядку денному в низці провідних країн Європи, зокрема у Німеччині, питань контролю та ухвалення законодавства, що спрямоване на ще до недавня слабко контрольовані сфери, на кшталт соціальних мереж. Наслідком такого сек'юритизаційного тренду стають законодавчі акти, подібні до німецького закону, спрямованого проти кримінального контенту в Інтернеті, — т. з. NetzDG (Netzwerkdurchsetzungsgesetz).

З іншого боку, державно-приватне партнерство є запорукою залучення різних акторів у спільний процес формування відповідальності за безпекову ситуацію в кіберпросторі: від кібергігієни³ до боротьби із кіберзлочинністю та попередження атак на об'єкти критичної інфраструктури.

А позаяк більша частина критичної інфраструктури, у т. ч. оборонний сектор, енергoresурси, електроенергетичні мережі, галузі охорони здоров'я, комунальних послуг, зв'язку,

¹ Див.: Radu, Roxana, Chenou, Jean-Marie, & Weber, Rolf H. (2014). The evolution of global internet governance: principles and policies in the making. Vol. 56: *Springer Science & Business Media*; Chenou, Jean-Marie. (2014). From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s. *Globalizations*, 11 (2), 205–223; Eriksson, Johan, & Giacomello, Giampiero. (2009). Who controls the internet? Beyond the obstinacy or obsolescence of the State. *International Studies Review*, 11 (1), 205–230.

² Mueller, Milton, Schmidt, Andreas, & Kuerbis, Brenden. (2013). Internet security and networked governance in international relations. *International Studies Review*, 15 (1), 86–104.

³ Кібергігієна – комплекс практичних та превентивних заходів, які реалізують користувачі з метою збереження конфіденційності даних та захищеності від крадіжок, зовнішніх атак. Це практичні кроки, націлені на підвищення безпеки в Інтернеті серед широкого кола користувачів.

транспорту, освіти, банківський сектор та сфера фінансів, перебуває у приватній власності і лише незначна — регулюється державою, державно-приватні відносини стають основоположними для успішного забезпечення національної безпеки та суверенітету.

Мета статті — схарактеризувати багатовимірність питання кібербезпеки, зокрема об'єктів критичної інфраструктури. Оскільки існує прямопропорційна залежність між рівнем демократичності суспільства та рівнем цифрової взаємозалежності і взаємопроникненням інформаційно-комунікаційних технологій (ІКТ) і промислових систем управління, країни стоять перед складним набором проблем із забезпечення функціонального державно-приватного партнерства в кіберсфері.

Аналіз наукових досліджень та публікацій з теми дослідження. Погляд багатьох дослідників є доволі стриманим щодо однозначно швидкого успіху кібербезпекового державно-приватного партнерства. Втім навіть найбільші скептики не заперечують, що ДПП є вкрай необхідним і важливим кроком із забезпечення національної безпеки. У цьому сенсі Стівен Голдсміт (Stephen Goldsmith) та Вільям Еггерс (William D. Eggers) слушно зауважують, що «важливо аналізувати не те, чи потрібне державно-приватне партнерство взагалі, а те, у яких формах воно має відбуватися» [1].

Виклад основного матеріалу. Уряди багатьох західних країн розглядають критичну інфраструктуру, що перебуває в приватній власності, як ключовий елемент національної безпеки, втім мандат для нагляду за мережевою безпекою такого елементу складно реалізувати без порушення права на конкуренцію та уникнення протекціоністського підходу. Водночас приватний сектор не до кінця готовий брати на себе відповідальність за національну кібербезпеку. Цей виклик урядам щодо управління національною кібербезпекою викликає питання про те, наскільки добре ці країни мають змогу сприяти своїй безпеці в інформаційному віці. Визнання недоліків у «партнерстві» є важливим кроком на шляху їх вирішення.

Відтак Європейський Союз (ЄС) активно розбудовує власні спроможності для забезпечення кібербезпеки держав-членів та здійснює масштабну діяльність у налагодженні державно-приватного партнерства у сфері кібербезпеки. Зважаючи на системність характеру загроз для кібербезпеки у поєднанні із постійним зростан-

ням кіберзлочинності в останні роки, Європейська Комісія (ЄК) у співпраці з країнами — членами ЄС, іншими інституціями Євросоюзу та відповідними заінтересованими сторонами розробила узгоджену політику дій, що має регулювати функціонування цього сектору.

У липні 2016 р. Європейська Комісія після низки громадських консультацій з усіма заінтересованими сторонами підписала угоду в галузі індустрії кібербезпеки, тим самим активізувавши зусилля, спрямовані на боротьбу з кіберзагрозами у формі ДПП [2].

В ініційованому Європейською Комісією Плані дій (Agreement with Industry on Cybersecurity and Steps up Efforts to Tackle Cyber-Threats)⁴ окреслено рамки ДПП в галузі кібербезпеки, що надалі регулюватимуть цю сферу правових та економічних відносин. На реалізацію цієї стратегії було виділено 450 млн євро, основним джерелом перерозподілу коштів є програма досліджень та інновацій «Горизонт 2020». Також учасники ринку кібербезпеки, представлені Європейською організацією з кібербезпеки (European Cyber Security Organisation, ECSO), задекларували намір реалізації своїх інвестицій у межах цієї ініціативи.

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, до добре розвинених ринків з новими бізнес-моделями, наприклад, ринок антивірусного програмного забезпечення. Цією ініціативою Європейська Комісія намагалася полегшити доступ до виходу на нові ринки підприємствам малого та середнього бізнесу, що працюють у галузі кібербезпеки.

Основою плану дій слугують такі документи: Стратегія єдиного цифрового ринку 2015 року (Digital Single Market Strategy for Europe) [3]; Кіберстратегія Європейського Союзу 2013 року (Cyber Security Strategy of the European Union:

⁴ Див.: http://europa.eu/rapid/press-releases_IP-16-2321-en.htm

An Open, Safe and Secure Cyberspace)⁵; Директива ЄС щодо мережевої та інформаційної безпеки (NIS Directive on Security of Network and Information Systems), яка мала 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. [2].

Прийнята в 2013 р. *Європейська стратегія кібербезпеки* [4] визначила спільне бачення Європейської Комісії та Високого представника Європейського Союзу із закордонних справ та політики безпеки щодо відкритого та безпечного кіберпростору. Стратегія визначає основні пріоритети, що регулюють проблеми як внутрішньоєвропейського, так і міжнародного законодавства. Пріоритети цієї ініціативи стосуються підвищення рівня захисту та стійкості європейських мереж та розвитку промислових і технологічних ресурсів для забезпечення кібербезпеки.

Відповідно до Стратегії у 2013 р. Європейська Комісія запропонувала перший всеосяжний елемент законодавства ЄС щодо кібербезпеки – Директиву ЄС щодо мережевої та інформаційної безпеки (NIS Directive on Security of Network and Information Systems), яка була прийнята Європейським парламентом 6 липня 2016 р. і набрала чинності у серпні цього ж року [5]. Після трьох років переговорів цей документ був прийнятий із поправками, далі відбулася його імплементація на національному рівні.

Також Директива NIS 2016 р. передбачила створення *координаційного механізму реагування* держав-членів у координації із приватним сектором на погрози та власне кібератаки, тим самим сприяючи стратегічному співробітництву та обміну інформацією, підтримуючи рівень довіри між учасниками процесу.

Відбувся запуск державно-приватної платформи на рівні ЄС, що має назву Платформа мережевої та інформаційної безпеки (Network and Information Security (NIS) Public Private Platform)⁶ для визначення ефективної практики кібербезпеки з метою сприяння подальшому

впровадженню Директиви. Результатом діяльності у цьому напрямі став Стратегічний порядок денний дослідження кібербезпеки (Cybersecurity Strategic Research Agenda, SRA) на базі Платформи мережевої та інформаційної безпеки [6]. Окрім вищеперелічених ініціатив, Європейська Комісія фінансує через FP7 та СІР (Сьому рамкову програму та Програму з конкурентоспроможності та інновацій) іще кілька проектів з кібербезпеки.

Відповідно до Постанови (ЄС) № 460/2004 Європейське Співтовариство заснувало в 2004 р. Європейське агентство з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security, ENISA) [7] з метою сприяння забезпеченню високого рівня розвитку культури інформаційної безпеки в межах ЄС. Пропозиція щодо модернізації мандата ENISA була прийнята 30 вересня 2010 р. [8]. Нормативно-правова база електронних засобів зв'язку, яка діяла з листопада 2009 р., передбачала зобов'язання щодо безпеки постачальників електронних засобів зв'язку⁷, а також зобов'язання країн-членів до травня 2011 р. транспонувати ці положення до законодавства на національному рівні.

Відтак усі сторони, у віданні яких є персональні дані (наприклад, банки чи лікарні), відповідно до нормативно-правової бази захисту даних⁸ 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 даних⁹ т. з. «контролери даних» повинні повідомляти національні наглядові органи про порушення режиму безпеки персональних даних.

Згідно із Директивою Ради ЄС 2008/114 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) у Європейській програмі захисту критично важливої інфраструктури [9] визначено загальний «парасольковий» підхід

⁵ Повідомлення про Стратегію кібербезпеки Європейського Союзу – відкритий та безпечний кіберпростір. URL: <https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace> (дата звернення: 07.03.2019).

⁶ NIS Платформа – Перша зустріч робочих груп. URL: <https://ec.europa.eu/digital-single-market/en/news/nis-platform-kick-meeting-working-groups> (дата звернення: 07.03.2019).

⁷ Див. статті 13а та 13b Рамкової директиви.

⁸ Директива 2002/58 від 12 липня 2002 р.

⁹ Пропозиція до Регламенту Європейського Парламенту та Ради про захист фізичних осіб стосовно обробки персональних даних та вільного переміщення таких даних (Загальні положення про захист даних). URL: <http://eur-lex.europa.eu/procedure/EN/201286> (дата звернення: 07.03.2019).

щодо захисту критично важливої інфраструктури у 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 рівнях. На саміті ЄС – США 2010 р.¹⁰ було створено робочу групу з питань кібербезпеки та кіберзлочинності. Також є низка мультилатеральних угод щодо співпраці у цій галузі з Організацією економічного співробітництва та розвитку, Генеральною Асамблеєю Організації Об'єднаних Націй, Міжнародним союзом електрозв'язку, Організацією з безпеки та співробітництва у Європі, Всесвітнім самітом з питань інформаційного суспільства (WSIS) та Форумом з питань управління Інтернетом (IGF). Європейська Комісія 6 травня 2015 р. прийняла Стратегію єдиного ринку цифрових технологій (Digital Single Market, DSM) [10]. Ця політика стала ще одним із засадничих положень для регулювання ДПП з питань кібербезпеки у сфері технологій та рішень для забезпечення мережевої безпеки впродовж 2016 р.

Незважаючи на те, що ДПП є вигідним для обох секторів, деякі приватні компанії зволікають із виконанням законодавства в цій сфері. Одним із основних каменів спотикання є питання довіри, контролю та розкриття корпоративної інформації. Компанії мають сумнів стосовно залучення уряду до розслідування справи після того, як кібератака на їхню компанію вже відбулась, позаяк це передбачає відкриття доступу до приватних даних компанії. Серед представників приватного сектору існує думка, 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 позицій на ринку [11]. Крім того, деякі приватні компанії також можуть турбуватися про те, що передача конфіденційної інформації може зашкодити їхній репутації, тобто відкрита для урядового розслідування інформація не залишиться конфіденційною після завершення такого розслідування [12].

¹⁰ Саміт ЄС – США, 20 листопада 2010 р., Лісабон – Спільна заява. URL: http://europa.eu/rapid/press-release_MEMO-10-597_en.htm (дата звернення: 07.03.2019).

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. Загалом приватні компанії відзначили відсутність довіри як ключову причину вагання щодо державно-приватної співпраці у цьому секторі¹¹.

Для того щоб зміцнити довіру між учасниками процесу, у Нідерландах створили *безпечну мережу інформації*, до якої уряд отримує безпосередній доступ лише після того, як компанія надасть на це свою згоду [13]. У такій моделі представники державного та приватного секторів працюють над побудовою довіри, розвитком співробітництва та діалогу на основі спільної платформи, ураховуючи інтереси всіх 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 Угоді¹² між Європейською Комісією та бізнесом, було розглянуто кілька сценаріїв, пов'язаних зі зміцненням індустрії кіберзахисту у Європі. Запропоновані варіанти були ретельно відібрані після аналізу доказів з різних джерел, включно й досліджень ринку кібербезпеки, а також було враховано точки зору, озвучені під час громадських консультацій, у яких брали участь понад 250 різних організацій, що представляють попит і пропозицію у галузі індустрії кібербезпеки.

Ініціатива Європейської Комісії в сфері ДПП започаткувала розвиток довгострокової конкурентоспроможності та інновацій європейської кібербезпеки, утім 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 додаткови-

¹¹ Вивчення синергії між цивільним населенням та ринками захисту кібербезпеки. URL: <https://goo.gl/uLXE43> (дата звернення: 07.03.2019).

¹² Комісія підписує угоду з бізнесом про кібербезпеку та активізує зусилля, спрямовані на боротьбу з кіберзагрозами. URL: http://europa.eu/rapid/press-release_IP-16-2321_en.htm (дата звернення: 07.03.2019).

ми заходами, які дозволятимуть європейським громадянам, підприємствам (малим та середнім підприємствам включно), органам державної 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 визначити як групу економічних суб'єктів та інституцій, територіально розташованих неподалік і достатніх 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, патентів, ніж ті, що працюють окремо.

Приналежність до кластеру дозволяє компаніям, що беруть участь в ініціативі, підвищити конкурентоспроможність і, таким чином, досягти більшої продуктивності переважно шляхом підвищення продуктивності завдяки покращенню доступу до спеціалізованих поставальників, технологій та інформації та вищому інноваційному потенціалу компаній, які співпрацюють. Це пов'язано з передачею знань, генерацією нових ідей та акцентуванням на інноваціях. Кластери – здебільшого ринкове явище, найуспішніші з них створюються спонтанно внаслідок природних конкурентних переваг на ринку.

Як окрема державна політика у ЄС цей підхід отримав розповсюдження наприкінці 1990-х років, з того часу бізнес-ініціативи, вищі навчальні заклади та науково-дослідні інститути сприяли розвитку та появі нової державної політики, діючи як каталізатор і допомагаючи розкрити економічний та науковий потенціал окремих регіонів. У Європейському Союзі більшість кластерів, що зосереджують увагу на кібербезпеці, працюють у Західній Європі (G4C – у Німеччині, який успішно заохотив уряд підтримувати розвиток 17 регіональних кластерів кібербезпеки, *Rôle d'Excellence Cyber* – у Франції, Гаазький дельта-кластер – у Нідерландах, INCIBE – в Іспанії), нові ініціативи починають з'являтися також у Центральній та Східній Європі, наприклад, у Чехії та Естонії.

З метою вироблення майбутньої стратегії ДПП в галузі кібербезпеки Європейська Комісія провела низку громадських консультацій із заінтересованими сторонами. Онлайн-консультації розпочалися 18 грудня 2015 р., вони три-

вали 12 тижнів, унаслідок чого збиралися різні погляди щодо питання функціонування єдиного європейського ринку в галузі кібербезпеки. Це супроводжувалося Дорожньою картою [14] кращого регулювання для ДПП в галузі кібербезпеки.

Провідними європейськими гравцями у галузі кібербезпеки була заснована *Європейська робоча група лідерів кібербезпеки*. Вона працювала над низкою конкретних рекомендацій для європейських громадян, бізнесу та промислової політики в галузі кібербезпеки. До складу цієї групи входили такі компанії: Airbus Group, Atos, BBVA, BMW, Cybernetica, Deutsche Telekom, Ericsson, F-Secure, Infineon та Thales.

Свою доповідь Європейська робоча група лідерів кібербезпеки у січні 2016 р. представила на Міжнародному форумі з кібербезпеки в Ліллі (Франція). У доповіді [15] висвітлюються рекомендації щодо заходів, спрямованих на підвищення надійності інформаційних систем у ЄС. У доповіді також містяться рекомендації європейських лідерів щодо успішного розвитку з питань кібербезпеки. Робочою групою після проведення громадських консультацій було виявлено низку важливих тенденцій:

- більшість респондентів позитивно реагували на ініціативу ЄК щодо ДПП в галузі кібербезпеки, наголошуючи на важливості стратегічної спрямованості такої співпраці;
- критична інфраструктура, фінанси та банківська діяльність, енергетика та охорона здоров'я учасниками опитування розглядалися як галузі, що можуть принести найбільше соціально-економічних збитків у випадку великої кібератаки;
- серед респондентів відмічався загальний консенсус щодо пріоритетності захисту критичної інфраструктури. Значна частина респондентів зазначала, що бракує необхідних товарів і послуг на європейському ринку для забезпечення безперервного та цілісного потоку зв'язків у галузі кібербезпеки. Це, зокрема, стосується систем виявлення кібернападів та управління безпекою інформації та подій, достатньої кількості програмного та апаратного забезпечення, криптографічних стандартів і надійних хмарних сервісів;
- багато респондентів висловили думку про недостатньо розвинену у ЄС і внутрішньоринкову, і зовнішньоринкову конкуренто-

спроможність. Хоча деякі європейські продукти та послуги, на переконання респондентів, є конкурентоспроможними з їхніми відповідниками з інших частин світу, поставальники в різних країнах ЄС часто працюють у нішевих ринках, відтак не можуть швидко та без значних втрат долати національні кордони, що впливає на цінову конкурентоспроможність цих продуктів;

- 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 цим сприяла сумісності, надаючи перевагу комбінованому підходу до стандартизації — горизонтальним та багатогалузевим зв'язкам. Відповідаючи на запитання про майбутнє фокусування в галузі стандартизації, респонденти одностайно загострювали увагу на захисті 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 [16]. У той же час значна частка респондентів заявила, що вони не знають, чи схеми сертифікації взаємно визнаються, припускаючи, що наразі такі схеми не є такими, що взаємно визнаються 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 за своєю сутністю є транскордонною проблемою.

Висновки. Захист критичних систем від загроз кібербезпеки є нелегким завданням, позаяк різні учасники процесу мають унікальні операційні рамки, точки доступу та різні рівні розвиненості системи та рівня технологічного забез-

печення. Тенденції інтеграції апаратного та програмного забезпечення в поєднанні зі зростаючими мережевими взаємозв'язками підключених до Інтернету речей та промислового Інтернету речей пристроїв змушують переглянути ландшафт загроз та вектори можливих атак у всіх цифрових інфраструктурах.

Суб'єкти, які несуть кіберзагрозу, орієнтуються на об'єкти критичної інфраструктури, зокрема енергетичного сектору, при цьому мають різні цілі — від кібершпигунства та до здатності порушувати енергетичні системи у випадку збройних конфліктів. Через чутливість до загроз та змінювану матрицю загроз, що посилюється новими технологіями, як-от машинне навчання, європейські уряди приділяють особливу увагу управлінню ризиками для захисту від складніших шкідливих програм та автоматизованих атак.

Ефективний підхід до управління ризиками вимагає обміну інформацією, що допомагає уряду та промисловості стежити за шкідливими програмами, фішинговими загрозами, внутрішніми загрозами тощо. Обмін інформацією також встановлює робочі протоколи для зафіксованих кейсів для формування компендіумів та посібників з основ стійкості, що є критичним для успіху пом'якшення інцидентів.

Нові виклики вимагають нового підходу — прийняття відповідного законодавства, яке б містило нові принципи державної політики щодо врегулювання питання державно-приватного партнерства, у т. ч. стосовно розподілу відповідальності між державою та приватним сектором, координації дій відомчих систем захисту та скоординованої системи захисту і реагування на різні види загроз.

Відтак одним із пріоритетних завдань плану дій з імплементації Стратегії кібербезпеки України є розвиток державно-приватного партнерства в контексті запобігання кіберзагрозам, реагування на кібератаки та кіберінциденти, усунення їхніх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану та в інші особливі періоди. Водночас реальні процеси налагодження ефективного державно-приватного партнерства у сфері кібербезпеки поки що перебувають у початковому стані, а чинні форми такого партнерства обмежуються діяльністю громадських рад при основних суб'єктах національної системи кібербезпеки держави.

Список використаних джерел

1. Goldsmith, S., & Eggers, W. D. (2009). *Governing by Network: The New Shape of the Public Sector*. Washington, DC: Brookings Institution Press. URL: https://www.brookings.edu/wp-content/uploads/2016/07/governingbynetwork_chapter.pdf (дата звернення: 07.03.2019).
2. The Directive on Security of Network and Information Systems (NIS Directive). URL: <https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive> (дата звернення: 07.03.2019).
3. Digital single market. Bringing down barriers to unlock online opportunities. URL: <https://ec.europa.eu/commission/priorities/digital-single-market/> (дата звернення: 07.03.2019).
4. Strategic Research Agenda Final v0.96. URL: <http://eur-lex.europa.eu/procedure/EN/202369> (дата звернення: 07.03.2019).
5. Directive (EU) 2016/1148 Of The European Parliament and of the Council. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення: 07.03.2019).
6. Стійкість і безпека комунікаційної інфраструктури, мереж і послуг. URL: <https://goo.gl/mK4irQ> (дата звернення: 07.03.2019).
7. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML> (дата звернення: 07.03.2019).
8. REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL concerning the European Network and Information Security Agency (ENISA). URL: http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2010/sec_2010_1126_en.pdf (дата звернення: 07.03.2019).
9. Council Directive 2008/114/EC as of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114> (дата звернення: 07.03.2019).
10. Study on synergies between the civilian and the defence cybersecurity markets. URL: <https://goo.gl/uLXE43> (дата звернення: 07.03.2019).
11. Cybersecurity Partnerships: A New Era of Public-Private Collaboration. URL: <http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf> (дата звернення: 07.03.2019).
12. Germano, Judith, H. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. Vol. 2. Issue 4. Pp. 179–187. URL: <http://www.sciencedirect.com/science/article/pii/S1874548209000274> (дата звернення: 07.03.2019).
13. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. URL: <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1478&context=jss> (дата звернення: 07.03.2019).
14. Public Private Partnership on Cybersecurity. URL: http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf (дата звернення: 07.03.2019).
15. ARNAUD Aurelie European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe. URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326 (дата звернення: 07.03.2019).
16. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0410> (дата звернення: 07.03.2019).

References

1. Goldsmith, S., & Eggers, W. D. (2009). *Governing by Network: The New Shape of the Public Sector*. Washington, DC: Brookings Institution Press. *www.brookings.edu*. Retrieved from: https://www.brookings.edu/wp-content/uploads/2016/07/governingbynetwork_chapter.pdf (viewed 07.03.2019) [in English].
2. The Directive on Security of Network and Information Systems (NIS Directive). (n. d.). *ec.europa.eu*. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive> (viewed 07.03.2019) [in English].
3. Digital single market. Bringing down barriers to unlock online opportunities. (n. d.). *ec.europa.eu*. Retrieved from: <https://ec.europa.eu/commission/priorities/digital-single-market/> (viewed 07.03.2019) [in English].
4. Strategic Research Agenda Final v0.96. (n. d.). *eur-lex.europa.eu*. Retrieved from: <http://eur-lex.europa.eu/procedure/EN/202369> (viewed 07.03.2019) [in English].

5. Directive (EU) 2016/1148 of the European Parliament and of the Council. (2016). *eur-lex.europa.eu*. Retrieved from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (viewed 07.03.2019) [in English].
6. Стійкість і безпека комунікаційної інфраструктури, мереж і послуг. (n. d.). *goo.gl*. Retrieved from: <https://goo.gl/mK4irQ> (viewed 07.03.2019) [in Ukrainian].
7. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. (2004). *eur-lex.europa.eu*. Retrieved from: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML> (viewed 07.03.2019) [in English].
8. REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL concerning the European Network and Information Security Agency (ENISA). (2010). *ec.europa.eu*. Retrieved from: http://ec.europa.eu/smart-regulation/impact/ia_carried_out/docs/ia_2010/sec_2010_1126_en.pdf (viewed 07.03.2019) [in English].
9. Council Directive 2008/114/EC as of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (2008). *eur-lex.europa.eu*. Retrieved from: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114> (viewed 07.03.2019) [in English].
10. Study on synergies between the civilian and the defence cybersecurity markets. (n. d.). *goo.gl*. Retrieved from: <https://goo.gl/uLXE43> (viewed 07.03.2019) [in English].
11. Cybersecurity Partnerships: A New Era of Public-Private Collaboration. (n. d.). *www.lawandsecurity.org*. Retrieved from: <http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf> (viewed 07.03.2019) [in English].
12. Germano, Judith H. (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. Vol. 2. Issue 4. (Pp. 179–187). *www.sciencedirect.com*. Retrieved from: <http://www.sciencedirect.com/science/article/pii/S1874548209000274> (viewed 07.03.2019) [in English].
13. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (n. d.). *scholarcommons.usf.edu*. Retrieved from: <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1478&context=jss> (viewed 07.03.2019) [in English].
14. Public Private Partnership on Cybersecurity. (2015). *ec.europa.eu*. Retrieved from: http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf (viewed 07.03.2019) [in English].
15. ARNAUD Aurelie European Cybersecurity Industry Leaders Recommendations on Cybersecurity for Europe. (n. d.). *ec.europa.eu*. Retrieved from: http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=13326 (viewed 07.03.2019) [in English].
16. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. (n. d.). *eur-lex.europa.eu*. Retrieved from: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016DC0410> (viewed 07.03.2019) [in English].