УДК 342.951

ПОЛЯКОВ О.М., начальник відділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0000-0002-8984-1476

ОСОБЛИВОСТІ ЗАЛУЧЕННЯ ПРИВАТНОГО СЕКТОРУ ДО ЗДІЙСНЕННЯ ЗАХОДІВ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, СТРИМУВАННЯ ДЕСТРУКТИВНОЇ ДІЯЛЬНОСТІ У КІБЕРПРОСТОРІ: КРАЩІ ПРАКТИКИ ЄВРОПЕЙСЬКОГО ДОСВІДУ

DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340524

Анотація. *Визначено тенденції, загрози та виклики у сфері кібербезпеки на теренах ЄС. Розкрито зміст та напрями державно-приватного партнерства у сфері забезпечення кібербезпеки. Деталізовано засади державної європейської політики у сфері забезпечення цифрової безпеки. Висвітлено деякі аспекти Директиви NIS 2, присвячені розбудові державно-приватного партнерства у сфері забезпечення кібербезпеки. Розкрито форми та моделі здійснення державно-приватного партнерства через призму загальноєвропейського законодавства. Проаналізовано загальноєвропейські засади розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки. Окреслено недоліки та виклики, які негативно впливають на стан державно-приватного партнерства у сфері забезпечення кібербезпеки в Європейському Союзі. Визначено основні принципи створення системи державно-приватного партнерства у сфері забезпечення кібербезпеки на теренах ЄС. Висвітлено прогалини у питаннях імплементації до національного законодавства Директиви NIS 2 більшістю держав ЄС, що провокує послаблення позицій державно-приватного партнерства у сфері забезпечення кібербезпеки. Визначено необхідність зміни такого підходу. Запропоновано подальші шляхи удосконалення чинного законодавства у частині посилення співпраці між державою, приватними компаніями і громадським суспільством як важливої складової державно-приватного партнерства з урахуванням кращих практик європейського досвіду.*

Ключові слова: *державно-приватне партнерство, кіберзагроза, кіберінцидент, кіберризик, кіберзахист, кіберстійкість, кіберпростір, інформаційно-комунікаційні технології, цивільний сектор кібербезпеки, імплементація, приватні компанії, громадянське суспільство, європейська цифрова політика, кризові ситуації, обмін досвідом та технологіями, взаємодія.*

Summary*. Trends, threats and challenges in the field of cybersecurity in the EU are identified. The content and directions of public-private partnership in the field of cybersecurity are disclosed. The principles of the state European policy in the field of digital security are detailed. Some aspects of the NIS 2 Directive, dedicated to the development of public-private partnership in the field of cybersecurity, are highlighted. The forms and models of implementing public-private partnership through the prism of pan-European legislation are disclosed. The pan-European principles of developing public-private partnership in the field of cybersecurity are analyzed. The shortcomings and challenges that negatively affect the state of public-private partnership in the field of cybersecurity in the European Union are outlined. The main principles of creating a system of public-private partnership in the field of cybersecurity in the EU are determined. The gaps in the implementation of the NIS 2 Directive into national legislation by most EU countries are detailed, which provokes a weakening of the positions of public-private partnerships in the field of cybersecurity, the need to change this approach. Further directions of improving the current legislation in terms of strengthening cooperation between the state and private companies and civil society as an important component of*

public-private partnerships, taking into account the best practices of European experience, are identified.

Keywords: *public-private partnership, cyber threat, cyber incident, cyber risk, cyber defense, cyber resilience, cyberspace, information and communication technologies, civilian cybersecurity sector, implementation, private companies, civil society, European digital policy, crisis situations, exchange of experience and technologies, interaction.*

Постановка проблеми. В умовах глобального геополітичного суперництва саме кібербезпека та її забезпечення стають ключовими напрямами державної безпекової політики, важливим фактором захисту національних інтересів у кіберпросторі. Україна, відчуваючи безпрецедентний тиск потужних російських кібератак, масштабування та збільшення чисельності кіберзагроз, активно опікується питаннями посилення кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури. В умовах швидкого та динамічного розвитку інформаційно-комунікаційних технологій надзвичайно важливим є формування ефективних та виважених підходів, які мають забезпечити надійний кіберзахист та кіберстійкість як об'єктів критичної інфраструктури, так і усіх інформаційно-комунікаційних систем, що вимагає налагодження ефективної співпраці між державою й приватним сектором, включаючи розробку та впровадження сучасної нормативно-правової бази, підготовку експертів, фахівців та навіть хакерів, які служитимуть в інтересах цивільного сектора кібербезпеки і зможуть протистояти будь-яким загрозам у кіберпросторі.

За таких умов саме державно-приватне партнерство є одним із основних принципів забезпечення кібербезпеки України в контексті захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. Вирішуючи відповідні масштабні стратегічні завдання, держава відчуває гостру потребу в залученні значної кількості кваліфікованих експертів та фахівців, які отримали спеціальну підготовку у сфері інформаційних технологій (аналітики, програмісти), мають необхідний спектр знань, навичок та вмінь у питаннях забезпечення кібербезпеки, зокрема, розробки та впровадження комплексного ліцензійного програмного забезпечення, створення потужних дата-центрів для зберігання і обробки цифрових даних тощо. В умовах стрімкої цифровізації кожна бізнес-структура має дбати не лише про захист персональних даних своїх клієнтів чи комерційних таємниць, але й забезпечувати всебічний захист усіх своїх процесів та критичної інфраструктури від потенційних ворожих дій, особливо у кіберпросторі. Залучення суб'єктів господарювання приватного сектора до побудови надійної та повноцінної системи кіберзахисту є спільним завданням держави та цивільного сектору кібербезпеки.

Забезпечення кібербезпеки, удосконалення захисту інформації у кіберпросторі залишаються актуальними завданнями інституцій громадянського суспільства, підприємств, установ та організацій усіх форм власності в умовах стрімкого розвитку інформаційно-комунікаційних технологій. Інформаційна сфера також зачіпає важливі проблеми, що становлять інтерес для окремих осіб, асоціацій, що діють у приватному секторі. Міжнародний досвід у цій площині переконливо засвідчує, що значну роль у питаннях забезпечення кібербезпеки та кіберзахисту, підтримання кіберстійкості, відіграють інституції громадянського суспільства та приватний ІТ-сектор. Саме тому у громадянському суспільстві особливо важливе значення мають також відносини між державою і комерційними структурами у сфері забезпечення кібербезпеки.

В умовах правового режиму воєнного стану, запровадженого у зв'язку зі російською збройною агресією проти України, кіберпростір став однією з ключових

площин сучасної війни. Масштабні кібератаки на об'єкти критичної інфраструктури вимагають максимального залучення висококваліфікованих фахівців та спеціалістів, зокрема й поза межами державного сектору, для спільного реагування на загрози та мінімізації їхніх наслідків, що зумовлює необхідність удосконалення правового врегулювання такої комплексної та паритетної взаємодії. Російська військова агресія також переконливо продемонструвала, що політична влада та бізнес мають бути надійними партнерами й плідно співпрацювати у питаннях забезпечення кібербезпеки та посилення кіберзахисту, оскільки будь-які кібератаки на державні ресурси можуть поширюватися й на бізнес-структури, а несанкціоноване проникнення в системи даних приватних компаній може становити серйозну потенційну загрозу, у тому числі й для державних органів, установ та організацій, які використовують навіть ліцензійне програмне забезпечення, розроблене як вітчизняними, так і зарубіжними приватними компаніями.

Таким чином, Україна поступово і динамічно розвиває партнерство з приватним сектором у кібернетичній сфері: створюються та функціонують інформаційно-аналітичні центри на комерційних підприємствах, які відносяться до об'єктів критичної інфраструктури, запускаються платформи обміну інформацією про кіберзагрози, проводяться тренінги та навчання, науково-практичні заходи за участю представників держави та приватного сектору.

Виходячи із сучасних загрозливих тенденцій та викликів, створення і удосконалення нормативно-правового підґрунтя для організації та побудови ефективної конструктивної співпраці і взаємодії між представниками приватного сектору й органами державної влади з метою виявлення, запобігання, профілактики та нейтралізації деструктивної діяльності в кіберпросторі, розбудови спільної кіберстійкості національного рівня, підвищення рівня прозорості, довіри та відповідальності у сфері кібербезпеки, формування культури цифрової безпеки серед громадян, бізнесу та державних інституцій є важливим і актуальним завданням держави та заслуговує на увагу, особливо через призму кращих практик європейського досвіду.

Результати аналізу наукових публікацій. Проблематика державно-приватного партнерства у сфері забезпечення кібербезпеки залишається доволі актуальною серед вітчизняних та іноземних практиків і науковців. Кращі практики зарубіжного досвіду розбудови механізмів державно-приватного партнерства у сфері кібербезпеки досліджували у своїх наукових працях: В. Бойко [1], В. Григоренко [2], Д. Дубов [3], Г. Малахов [4] та інші. Серед наукових праць останніх років можна виділити роботи, які містять законотворчі ініціативи, спрямовані на удосконалення механізмів розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки. Це, зокрема, роботи: Г. Зубка [5], В. Круглова [6], О. Шевчук та Є. Чорного [7]. Проблематику державно-приватного партнерства в секторі безпеки висвітлювали у своїх наукових працях: Ю. Заскока [8], Ю. Мех [9], Ю. Романюк та В. Паливода [10]. Проте жоден із вказаних фахівців не здійснював огляд кращих практик європейського досвіду у сфері законодавчого забезпечення державно-приватного партнерства у сфері кібербезпеки у зв'язку із набуттям чинності Директивою ЄС 2022/2555 "Про мережі та інформаційні системи" (NIS 2).

Метою статті є визначення на підставі узагальнення концептуальних основ загальноєвропейського законодавства у сфері кібернетичного державно-приватного партнерства подальших шляхів удосконалення організаційно-правових засад розвитку державно-приватного партнерства у сфері забезпечення кібербезпеки України з урахуванням кращих практик європейського досвіду у цій площині.

Виклад основного матеріалу. В сучасних умовах для України актуалізуються питання законодавчого забезпечення розбудови державно-приватного партнерства з метою розробки та впровадження комплексних заходів у сфері забезпечення кібербезпеки в умовах зростаючої малопрогнозованості кіберінцидентів, збільшення кількості та масштабів кіберзагроз, які завдають значної шкоди інформаційно-телекомунікаційним системам, економіці та національній безпеці. Реалізація пріоритетних засад державної політики у цій площині вимагає системного залучення потенціалу приватного сектору та громадського суспільства з метою прогнозування та мінімізації кіберризиків, посилення кіберзахисту об'єктів критичної інфраструктури, протидії деструктивній діяльності в кіберпросторі, налагодження механізмів комплексної взаємодії між державними органами, бізнесом і громадськістю у сфері кібербезпеки, формування культури цифрової безпеки в суспільстві, зміст якої охоплює громадян, бізнес-структури та уповноважені державні інституції. Вони мають бути адаптовані до сучасних тенденцій такої співпраці, а також кращих практик зарубіжного досвіду держав-членів ЄС у цій царині. 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 [1, с.34].

Для більшості держав ЄС в умовах російської військової агресії роль та значення кібербезпеки постійно та динамічно зростає, а кіберландшафт швидко розвивається, завдяки цифровізації розширюється діапазон кіберзагроз і вразливостей. У зв'язку з цим держави-члени ЄС розробляють дієві механізми з метою координації спроможностей у сфері розбудови державно-приватного партнерства шляхом прийняття загальноєвропейських актів законодавства, одним з яких є Директива NIS2 (2022) [11]. Так, Директива NIS2 (2022/2555) була ухвалена Європейським Союзом 14 грудня 2022 року і набула чинності 16 січня 2023 року. Вона відіграє ключову роль у розбудові державно-приватного партнерства у сфері забезпечення кібербезпеки. Директива NIS2 замінює попередню Директиву NIS та має на меті усунути недоліки та фрагментацію, що спостерігалися під час її впровадження на теренах ЄС. Вона запроваджує більш комплексний та гармонізований підхід до питань забезпечення кібербезпеки, посилення захисту критичної інфраструктури, цифрових послуг та громадян ЄС від зростаючої загрози кіберінцидентів та кібератак. Загалом Директива NIS2 – це звід правил та вимог щодо кібербезпеки, що застосовуються до широкого кола організацій та суб'єктів господарювання в масштабах ЄС. Вона поширюється на операторів та постачальників цифрових послуг, критично важливих технологій та органи державного управління. Ключові цілі NIS2 включають: встановлення стандартних вимог щодо кібербезпеки для всіх держав-членів ЄС; розширення сфери дії директиви для охоплення більшої кількості секторів та відповідальних суб'єктів господарювання; запровадження більш суворіших зобов'язань щодо звітності про кіберінциденти та заходів правозастосування; сприяння кращій співпраці та обміну інформацією між державами-членами ЄС; забезпечення високого рівня кіберстійкості як важливого стандарту в Європейському Союзі.

Також Директива NIS 2 спрямована на підвищення рівня безпеки мережевих та інформаційних систем у державах-членах ЄС, сприяючи співпраці між державним і приватним секторами. Порівняно з попередньою Директивою NIS (2016/1148) Директива NIS2 значно розширює сферу застосування, зміст якої включає більше секторів економіки, таких як енергетика, транспорт, охорона здоров'я, фінанси, цифрова

інфраструктура, промисловість та державне управління. Вона поділяє організації на "критично важливі" (Essential Entities) та "важливі" (Important Entities), що охоплює як великі, так і середні приватні компанії, які мають значний вплив на економіку та цифрову інфраструктуру. Це змушує приватні компанії активно співпрацювати з державними органами для забезпечення відповідності вимогам кібербезпеки. Директива встановлює чіткі вимоги та критерії щодо повідомлення про кіберінциденти: приватні структури повинні інформувати компетентні органи протягом 24 годин після виявлення інциденту та надавати повний звіт протягом 72 годин. Це сприяє створенню підґрунтя задля обміну інформацією між приватними компаніями та державними органами, що є основою державно-приватного партнерства. Такий обмін даними допомагає виявляти реальні та потенційні кіберзагрози, ділитися передовим досвідом та координувати заходи, спрямовані на реагування на кібератаки. Також положення директиви акцентують увагу на моніторингу ланцюгів постачання, вимагаючи від приватних компаній перевіряти своїх контрагентів на відповідність стандартам NIS2. Це має стимулювати приватні компанії та ІТ-суб'єктів господарювання плідно співпрацювати з державними органами для розробки спільних стандартів безпеки, які зміцнюють партнерство через посилення відповідальності в контексті захисту критичної інфраструктури та цифрових сервісів. Директива встановлює мінімальні вимоги для приватних компаній щодо проведення регулярних тренінгів з кібербезпеки як для керівництва, так і для працівників.

Держави-члени можуть підтримувати ці ініціативи шляхом розробки спільних навчальних програм, що сприяє формуванню культури кібербезпеки в рамках розбудови державно-приватного партнерства. Директива заохочує створення міждержавних структур управління кіберкризою (наприклад, EU-CyCLONe) та національних стратегій кібербезпеки, які визначають роль та місце приватного сектору у питаннях забезпечення кібербезпеки, запроваджує суворішу відповідальність, включаючи штрафи та адміністративну відповідальність керівництва за невідповідність встановленим вимогам з метою стимулювання приватних компаній активно співпрацювати з державними органами для уникнення санкцій, що сприяє формуванню посиленого формату співпраці.

EU-CyCLONe – Європейська мережа організацій зв'язку з питань кібернетичних криз – це мережа співпраці для національних органів держав-членів, відповідальних за управління кіберризиками [12]. Ця мережа була запущена у 2020 році та офіційно оформлена 16 січня 2023 року одночасно з набуттям чинності стаття 16 Директиви NIS2. Основними завданнями EU CyCLONe є:

- підтримувати скоординоване управління масштабними кіберінцидентами на операційному рівні та забезпечувати регулярний обмін відповідною інформацією між державами-членами та установами, органами, службами та агентствами ЄС;
- постійно підвищувати рівень готовності до управління масштабними кіберінцидентами та кризами у сфері кібербезпеки;
- розвивати спільну ситуаційну обізнаність щодо масштабних кіберінцидентів та криз у сфері кібербезпеки;
- періодично проводити оцінку відповідних масштабних кіберінцидентів та криз у сфері кібербезпеки, формувати пропозиції з метою уникнення негативних наслідків;
- здійснювати координацію управління масштабними кіберінцидентами та кризами у сфері кібербезпеки, ініціювати схвалення рішень на політичному рівні щодо таких кіберінцидентів;

- проводити обговорення національних планів реагування на масштабні кіберінциденти та будь-які кризові ситуації.

Таким чином, Директива NIS2 запровадила такі інновації у сфері розвитку державно-приватного партнерства у сфері кібербезпеки: розширила сфери дії та встановила умови залучення приватного сектору; запровадила обов'язкову звітність та обмін інформацією про будь-які кіберінциденти; встановила обов'язковість проведення навчання та підвищення обізнаності приватного сектору у питаннях забезпечення кібербезпеки; збільшила розміри штрафів та запровадила адміністративну відповідальність керівників підприємств, установ та організацій приватного сектору за невиконання встановлених вимог з метою стимулювання приватних компаній активно співпрацювати та обмінюватися інформацією з державними й правоохоронними органами. Таким чином, Директива NIS2 створює законодавчі рамки для розвитку ефективного державно-приватного партнерства у сфері кібербезпеки, сприяючи обміну інформацією, спільному управлінню кіберризиками, кіберінцидентами, вразливостями, забезпечує підвищення стійкості критичної інфраструктури на теренах ЄС [13].

Важливо зазначити, що NIS2 також може застосовуватися до суб'єктів господарювання поза межами ЄС, які надають важливі або необхідні цифрові послуги на європейському ринку, навіть якщо вони фізично не розташовані в кордонах ЄС. Крім того, суб'єкт господарювання все ще може бути класифікований як "важливий" навіть якщо він не відповідає загальним критеріям розміру, наприклад, у випадках, коли він є єдиним постачальником критично важливої цифрової послуги, життєво важливої для суспільної або економічної діяльності в державі-члені ЄС Директива NIS 2 охоплює не лише великі організації, але й менші суб'єкти господарювання, які відіграють ключову роль у підтримці критично важливої інфраструктури або цифрових послуг в межах ЄС.

Директива 2022/2555 запроваджує заходи, спрямовані на досягнення високого загального рівня кібербезпеки на теренах ЄС з метою покращення функціонування внутрішнього цифрового ринку. Для досягнення цієї мети відповідно до Директиви: встановлено зобов'язання, які вимагають від держав-членів прийняття національних стратегій кібербезпеки та призначення або створення компетентних органів, органів управління кіберкризами, єдиних контактних пунктів з питань кібербезпеки (єдиних контактних пунктів) і груп реагування на інциденти комп'ютерної безпеки (CSIRT); запроваджено заходи з управління ризиками кібербезпеки та встановлено зобов'язання щодо звітності для суб'єктів господарювання, чия діяльність не пов'язана з управлінням критичною інфраструктурою, а також для суб'єктів, визначених як критично важливі за Директивою (ЄС) 2022/2557; встановлено правила та визначено зобов'язання щодо обміну інформацією про кібербезпеку; визначено наглядові та примусові зобов'язання держав-членів ЄС. Директивою NIS 2 також визначені зобов'язання для держав-членів ЄС щодо розробки національних стратегій кібербезпеки. За Директивою ці нормативно-правові акти повинні надаватися для опрацювання Агентству ЄС не пізніше трьох місяців із дати їх схвалення державами-членами та переглядатися кожних п'ять років з урахуванням рівня системних кіберзагроз.

Відповідно до статті 7 Директиви NIS 2 національна стратегія кібербезпеки, серед іншого, має включати положення щодо: основних напрямів та засобів забезпечення кібербезпеки; заходів з управління ризиками, стандартизації і сертифікації продуктів та рішень, які впливають на кібербезпеку; правового статусу уповноважених органів; умов реалізації проєктів публічно-приватного партнерства у відповідній сфері; механізмів інформування уповноважених органів та Агентства ЄС про істотні кіберінциденти тощо. Невід'ємною складовою національних стратегій політики є забезпечення кібербезпеки в

окремих сферах суспільних відносин. Саме цими нормативно-правовими актами закладаються правові засади управління кіберризиками на галузевому рівні, визначаються спеціальні засоби протидії кіберзагрозам та завдання суб'єктів владних повноважень із забезпечення кібербезпеки з урахуванням галузевих особливостей.

Відповідно до частини четвертої статті 9 Директиви NIS 2 кожна держава-член ЄС повинна схвалити Національний план реагування на масштабні кіберінциденти та кризи у сфері кібербезпеки, який має визначати, зокрема: мету та цілі національних заходів; завдання та відповідальність органів управління кіберкризою; процедури управління кіберкризою, включаючи їх інтеграцію в загальну національну структуру управління кризою та канали обміну інформацією; національні заходи готовності, включаючи навчання та навчальну діяльність; відповідні державні та приватні зацікавлені сторони та залучену інфраструктуру; національні процедури та домовленості між відповідними національними органами та органами для забезпечення ефективної участі держави-члена, підтримки скоординованого управління великомасштабними інцидентами та кризами кібербезпеки на рівні ЄС.

У рамках Директиви NIS 2 акцентовано, що державно-приватне партнерство підвищує довіру до продуктів і послуг у сфері інформаційно-комунікаційних технологій, що є вигідним для приватного сектору, оскільки це полегшує доступ йому до цифрових ринків ЄС. Водночас, держави-члени за допомогою приватного сектору отримують інструмент для забезпечення як кібербезпеки, так і безпеки об'єктів критичної інфраструктури. Ця взаємна вигода стимулює державно-приватне партнерство, оскільки приватні структури зацікавлені у співпраці з державними органами для отримання сертифікатів відповідності і створення сприятливих передумов задля доступу до цифрових ринків ЄС. Напрямки інноваційного розвитку у сфері кібербезпеки передбачають залучення приватних компаній до процесу створення та запуску новітніх технологій, ноу-хау, які мають відповідати стандартам ЄС.

Таким чином, європейська політика державно-приватного партнерства у сфері забезпечення кібербезпеки спрямована на створення стійкої, скоординованої та ефективної системи захисту цифрової інфраструктури через співпрацю між державними органами та приватним сектором. Механізми співпраці передбачають обмін інформацією, організацію навчання, фінансування з метою створення стійкої екосистеми та архітектури кібербезпеки, де держава та приватний сектор спільно протидіють будь-яким кіберзагрозам.

Так, обмін інформацією про кіберзагрози включає створення відповідних мереж для спільного використання, таких як CSIRTs, Network та EU-CyCLONe. Також приватні компанії зобов'язані ділитися інформацією про кіберінциденти, а держава надає підтримку у вигляді аналізу кіберзагроз і формує відповідні рекомендації. Важливою складовою є навчання та підвищення кваліфікації, що передбачає спільні тренінги та симуляції кібератак (наприклад, проєкт Cyber Europe), де державні та приватні структури спільно відпрацьовують навички та вміння, впроваджують заходи координації та екстренного реагування. Такий важливий напрямок, як фінансування державно-приватного партнерства передбачає залучення інвестицій під проєкти кібербезпеки, коли приватні компанії можуть отримувати гранти за умови своєї зацікавленості у консолідованій співпраці з державними органами. Наприклад, фінансуються проєкти з розробки безпечного програмного забезпечення або побудови інноваційного захисту об'єктів критичної інфраструктури.

Одночасно викликами у цій сфері залишаються: різниця у існуючих пріоритетах, оскільки держава фокусується, у першу чергу, на питаннях забезпечення національної

безпеки, а приватний сектор – на прибутковості та конкурентоспроможності; ступінь довіри між державою та приватним сектором, оскільки обмін чутливою або конфіденційною інформацією вимагає високого рівня довіри, що іноді є проблемою через комерційні інтереси. Також недоліком у питаннях забезпечення кібербезпеки між державою та приватним сектором є фрагментація стандартів, оскільки навіть попри єдині рамки, встановлені загальноєвропейським законодавством, держави-члени ЄС впроваджують встановлені вимоги по-різному, що певним чином ускладнює співпрацю. Загалом приватний сектор відіграє важливу та ключову роль у європейській політиці забезпечення кібербезпеки, оскільки: він допомагає впроваджувати технології, які відповідають стандартам сертифікації; бере участь у тестуванні безпеки цифрових продуктів і ланцюгів постачання; надає інформацію та дані про кіберзагрози і кіберінциденти з метою спільного аналізу та реагування. Окрім того, завдання, які вирішує державно-приватне партнерство у сфері забезпечення кібербезпеки, включають: спільне технічне регулювання обробки даних; обмін інформацією про загрози та вразливості; надання методичної допомоги у питаннях боротьби з незаконним або протиправним контентом тощо. За таких умов для кожної держави-члена ЄС імплементація загальноєвропейських підходів у національне законодавство є критично важливою для посилення стану національної кібербезпеки у рамках розбудови державно-приватного партнерства.

Основними принципами створення екосистеми державно-приватного партнерства у сфері забезпечення кібербезпеки на теренах ЄС є: забезпечення технологічних рішень; використання достатніх людських ресурсів; розробка відповідної нормативно-правової бази як основи такої співпраці. При цьому важливо забезпечити відкриту комунікацію між державним та приватним секторами. Залучення саме малих та середніх ІТ-компаній до процесу побудови державно-приватного партнерства у сфері кібербезпеки також має вирішальне значення, оскільки вони є основою європейської економіки, у тому числі й цифрової. Серед рекомендацій ЄС щодо покращення державно-приватного партнерства виділяється розробка заходів, спрямованих на підвищення мотивації приватного сектору до участі у процесах забезпечення кібербезпеки. При цьому саме державні органи кожної держави ЄС мають розробляти та впроваджувати національний план дій щодо державно-приватного партнерства.

Створення системи державно-приватного партнерства у сфері забезпечення кібербезпеки на теренах ЄС має дозволити обмінюватися знаннями, передовим досвідом та досягти спільного рівня розуміння між усіма зацікавленими сторонами (держава та приватний сектор). Рамкові угоди про державно-приватне партнерство на рівні кожної держави-члена ЄС спрямовані на покращення комунікацій, планування, оцінку кіберризиків, операційну діяльність, включаючи розробку механізмів з метою реагування на кіберінциденти та кіберзагрози. Таке партнерство допомагає впроваджувати заходи у сфері забезпечення кібербезпеки та кіберстійкості.

Приватні компанії активно ініціюють проведення науково-практичних заходів, форумів з метою постійного обміну інформацією та досвідом, що надає можливість формувати розуміння ризиків кібербезпеки як загальну умову ведення бізнесу.

У цьому контексті С. Сєрєбряк слушно вказує, що основною метою державно-приватного партнерства у сфері забезпечення кібербезпеки є побудова конструктивного діалогу та плідної співпраці, реальної довіри між приватним сектором та державними установами; заохочення співпраці між державними та приватними організаціями на ранніх етапах дослідницького та інноваційного процесу. На його переконання, перспективні спільні заходи у сфері кібербезпеки включають: залучення стартапів та

науковців до проведення комп'ютерно-технічної експертизи; розробку та впровадження сучасного програмного забезпечення з метою виявлення та запобігання кіберзагрозам на ранніх стадіях; постійний моніторинг кіберпростору; навчання галузевих спеціалістів, розробку та просування онлайн-освітніх платформ тощо [14, с.335].

Інші дослідники О. Фролова та О. Кучмій, дослідивши переваги та виклики державно-приватного партнерства у сфері кібербезпеки, дійшли висновку, що причинами спільної вигоди державного і приватного сектору за результатами співпраці можуть бути: прагнення усунути реальні та потенційні вразливості; еволюція кіберзагроз від національних до міжнародних; налагодження постійного обміну знаннями та передовим досвідом; досягнення стабільності кіберсистеми; встановлення прямих та надійних контактів з іншими організаціями тощо [15, с. 205].

Представник датської школи науковців К. Крістенсен у своїй публікації на підставі проведеного аналізу вказує, що у стратегічних документах ЄС з питань кібербезпеки неодноразово підкреслюється важливість ролі держави у питаннях побудови співпраці з приватним сектором у боротьбі з кібератаками та кіберзлочинцями. Тому, на переконання автора, в контексті розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки, необхідно враховувати національні відмінності на рівні кожної держави ЄС окремо, проте мотивацією такого співробітнитцва завжди виступає спільний інтерес та економічна вигода, а приватний сектор у своїй діяльності має керуватися концепцією корпоративного ризику та безпеки. Адже у рамках побудови діалогу у європейському цифровому просторі трапляються суперечки між державою та приватним сектором, які пов'язані із запровадженням державою розподілу та категоризацією кіберризиків на основі такого критерію, як визначення виконавців. Це вимагає впроваджувати персоналізований підхід для проведення оцінки кіберзагроз, провокуючи, певним чином, втрату часу та можливостей своєчасного вжиття попереджувальних заходів, розпізнавання та блокування посягань і кібератак [16, с.1444].

В. Матвієнко та Г. Петушкова, здійснивши вивчення європейського досвіду державно-приватного партнерства у сфері кібербезпеки, дійшли висновку, що воно є взаємовигідною формою партнерства для обох сторін – державного та приватного секторів. При цьому на європейському просторі існує фрагментація підходів до розвитку та функціонування його змісту. Передумовами для цього стала унікальність ситуації, яка склалася на європейському цифровому просторі, адже як державний, так і приватний сектор об'єднує загальна ідея про те, що державно-приватне партнерство є базовим елементом для підвищення кіберстійкості та розвитку кіберзахисту усіх суб'єктів національної системи кібербезпки. На цьому фоні питання довіри та контролю є найважливішими проблемами, як і постійна дилема щодо того, чи будуть ці структури ефективними у разі масованих кібератак, оскільки немає жодної європейської країни, яка мала би унікальний досвід протистояння кібератакам у поєднанні з класичними методами залучення громадянського суспільства до цих процесів [17, с.17]. Із викладеними позиціями як вітчизняних, так і зарубіжних науковців не можна не погодитися.

Слід вказати, що на виконання загальноєвропейських вимог усі держави-члени ЄС мали до 17 жовтня 2024 року внести зміни до свого національного законодавства з метою імплементації положень Директиви NIS 2 для посилення кібербезпеки об'єктів критичної інфраструктури, покращення цифрових послуг та сервісів в ЄС. Тобто кожна держава ЄС повинна розробити та схвалити відповідний законопроект, який безпосередньо імплементує положення Директиви NIS2, одночасно визначивши перелік

заходів, спрямованих на забезпечення високого загального рівня кібербезпеки. Також відповідні національні закони повинні певним чином регулювати питання державно-приватного партнерства у сфері забезпечення кібербезпеки, визначати умови, порядок та моделі такої комплексної взаємодії, визначати імперативну вимогу про те, що приватний сектор зобов'язаний не лише управляти кіберризиками та запобігати кіберінцидентам, але й вживати заходів з метою пом'якшення їхніх катастрофічних наслідків, співпрацюючи у цьому напрямку з державою.

Так, наприклад, лише 14 з 27 держав ЄС імплементували Директиву NIS2 у національне законодавство (Бельгія, Данія, Греція, Італія, Литва, Латвія, Фінляндія, Румунія, Хорватія, Словаччина, Словенія, Угорщина, Кіпр, Люксембург). У Бельгії підготовлено сучасний закон про кібербезпеку мереж та інформаційних систем, який набув чинності 18 жовтня 2024 року [18], а у Німеччині – Федеральний закон щодо посилення кібербезпеки лише має бути остаточно схвалений в 2026 році [19]. Нідерланди планують прийняти новий закон про кібербезпеку наприкінці 2025 року, а Данія, Франція, Ірландія та Іспанія й інші держави ЄС досить повільно ставляться до необхідності прискорення схвалення відповідних законів, що негативно впливає на загальний стан забезпечення кібербезпеки на національному рівні кожної окремо узятої держави. Таким чином, не усі держави ЄС імплементували Директиву NIS 2 у національне законодавство. Враховуючи такий стан справ, Європейська комісія у травні 2025 року офіційно звернулася до політикумів держав-членів ЄС із жорстким попередженням про необхідність прискорити процедури імплементації Директиви NIS 2 у національне законодавство [20].

Таким чином, приватний сектор глибоко інтегрований у різні аспекти національної кібербезпеки, активно залучається тією чи іншою країною для боротьби з кібератаками, підтримання кіберстійкості та кіберзахисту критичної інфраструктури. У державах ЄС приватні компанії в середньому витрачають біля 30 відсотків свого бюджету на постійне удосконалення технологій у сфері забезпечення кібербезпеки, з метою придбання сучасного програмного забезпечення. Приватні компанії є учасниками переважної більшості заходів, організованих державою та присвячених обміну набутим досвідом, пошуку оптимальних шляхів посилення стану забезпечення кіберзахисту критичної інфраструктури, гарантування цифрової безпеки на теренах ЄС тощо. Європейські корпорації виробляють більшу частину програмного та апаратного забезпечення, яке використовують уряди держав Союзу, при цьому найбільш типовою формою співпраці є договірні зобов'язання між урядом та представниками приватного сектору. Одночасно скоординовані засади партнерства між державою та приватними структурами можуть забезпечити надходження додаткових ресурсів, необхідних для посилення кібербезпеки.

Висновки. Директива NIS2 є ключовим законодавчим актом Європейського Союзу, який має на меті підвищити рівень кібербезпеки в країнах-членах. Її впровадження посилює вимоги до приватних компаній, що працюють з критичними інфраструктурами, мережевими та інформаційними системами. Важливою складовою процесів забезпечення кібербезпеки на теренах ЄС визначено державно-приватне партнерство. Ця директива не лише підвищує вимоги до кібербезпеки, а й ставить перед постачальниками ІТ-послуг та цифрових сервісів серйозні завдання: розробка чіткої стратегії управління кіберризиками, впровадження ефективних засобів захисту та формування спеціалізованих команд, які відповідатимуть за забезпечення безпеки інформаційних систем тощо. При цьому успішна діяльність на європейському цифровому ринку неможлива без належного рівня захисту даних як важливого спільного завдання держави та приватного сектора. Таким чином, важливим

пріоритетом європейської політики державно-приватного партнерства у сфері забезпечення кібербезпеки є створення стійкої, скоординованої та ефективної системи захисту цифрової критичної інфраструктури через паритетну співпрацю між державними органами та приватним сектором. Механізми співпраці передбачають обмін інформацією, організацію навчання, підвищення кваліфікації, пошук додаткових каналів фінансування з метою створення стійкої екосистеми та архітектури кібербезпеки, де держава та приватний сектор спільно протидіють будь-яким кіберзагрозам, підтримуючи кіберстійкість та гарантуючи надійний кіберзахист критичної інфраструктури.

Директива NIS2 була адаптована не усіма країнами Європейського Союзу. Це означає, що компанії, які працюють на цих ринках або з партнерами з цих країн, зобов'язані виконувати вимоги кібербезпеки, встановлені на національному рівні. Тому загальним недоліком є гальмування більшістю держав ЄС імплементації положень Директиви NIS 2 у національне законодавство, що, у свою чергу, засвідчує повільність процесів розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки як на загальноєвропейському рівні, так і на державному.

Україна, в контексті здійснення кроків на шляху до євроінтеграції, має адаптувати свою політику у сфері кібербезпеки відповідно до стандартів ЄС, що передбачає у рамках розбудови державно-приватного партнерства: гармонізацію вітчизняного законодавства з Директивою NIS2; реалізацію спільних проектів за участю держави та приватних компаній, у тому числі й в IT-сфері; вільний доступ до цифрових ринків ЄС; підвищення кіберстійкості, особливо в умовах війни; сприяння співпраці між державою та приватними структрами з метою посилення кіберзахисту критичної інфраструктури тощо.

Виходячи із викладеного, потребує прискорення схвалення парламентом законопроекту "Про основи всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі" (реєстр. № 13592 від 01.08.2025 р.) [21], що надасть змогу: створити ефективні організаційно-правові механізми залучення представників приватного сектору та громадянського суспільства до протидії деструктивній діяльності в кіберпросторі; налагодити взаємодію між державними органами, бізнесом і громадськістю у сфері кібербезпеки; підвищити рівень кіберстійкості на національному рівні завдяки консолідації зусиль держави та недержавних суб'єктів; зміцнити довіру між усіма учасниками кіберсфери шляхом підвищення прозорості та спільної відповідальності; сформувати культуру цифрової безпеки в суспільстві, що охоплює громадян, бізнес структури та державні інституції.

Використана література

1. Бойко В.О. Європейський досвід державно-приватного партнерства у сфері кібербезпеки: підходи до формування нормативно-правових засад. *Стратегічні пріоритети.* 2019. № 1. С. 28-36. URL: https://niss-priority.com/index.php/journal/article/view/235/223.

2. Григоренко В.А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки. *Інформація і право.* 2021. № 2(37). С. 155-161. DOI https://doi.org/10.37750/2616-6798.2021.2(37).238405.

3. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. Доп. / за заг. Ред. Д. Дубова. Київ : НІСД, 2018. 84 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberbezpeka.pdf

4. Малахов Г.Б. Шляхи удосконалення державно-приватного партнерства у сфері кібербезпеки України. *Інформація і право.* 2023. № 4 (47). С. 197-206. DOI https://doi.org/10.37750/2616-6798.2023.4(47).291666

5. Зубко Г.Ю. Публічно-приватне партнерство у сфері безпеки стратегічної інфраструктури України. *Юридичний науковий електронний журнал.* 2020. № 2. Том.2. С. 13-17. URL: http://www.lsej.org.ua/2-2_2020/5.pdf.

6. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія. Державне управління.* 2018. Т.29 (68). № 3. С. 57-61.

7. Шевчук О.Р., Чорний Є.М. Правове регулювання державно-приватного партнерства у сфері інформаційної безпеки. *Юридичний бюлетень*. 2021. Випуск 19. С. 127-133.

8. Заскока Ю.В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. *Наукові перспективи.* 2021. № 9 (15). С. 85-98. URL: http://perspectives.pp.ua/index.php/np/article/view/467/470.

9. Мех Ю.В. Юридичний погляд на концепції оптимальних моделей державно-приватного партнерства в секторі безпеки України. *Науковий вісник Ужгородського національного університету. Серія Право.* 2023. №80. Том 1. С. 507-512. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/297170/290088.

10. Романюк Ю.П., Паливода В.О. Роль недержавних інституцій у зміцнені сектору безпеки і оборони держави. *Стратегічна панорама.* 2020. № 1-2. С. 21-28.

11. Директива (ЄС) 2022/2555 про заходи для високого загального рівня кібербезпеки в Союзі, внесення змін до Регламенту (ЄС) № 910/2014 і Директиви (ЄС) 2018/1972, а також про скасування Директиви (ЄС) 2016/1148. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.

12. EU-CyCLONe. - European cyber crisis liaison organisation network. URL: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone.

13. NIS2 Directive Transposition Tracker. URL: https://ecs-org.eu/activities/nis2-directive-transposition-tracker.

14. Сєрєбряк С.В. Державно-приватне партнерство у сфері забезпечення кібербезпеки. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2024. №6. С. 351-356. URL: http://journal-app.uzhnu.edu.ua/article/view/317022

15. Фролова О., Кучмій О. Public-private partnership in sphere of cybersecurity as an important factor of european stability. *Міжнародні та політичні дослідження.* 2021 № 34. С. 194–211. https://doi.org/10.18524/2707-5206.2021.34.237903. URL: http://heraldiss.onu.edu.ua/article/view/237903.

16. Kristoffer Kjærgaard Christensen. Public-private partnerships on cyber security: A practice of loyalty. *International Affairs.* 2017. Vol. 93. № 6. pp. 1435-1452. URL: https://www.jstor.org/stable/48570028.

17. Матвієнко В.М., Петушкова Г.Є. Європейський досвід державно-приватного партнерства у сфері кібербезпеки: можливості для України. *Актуальні проблеми міжнародних відносин.* 2022. № 152. Том 1. С. 10-18. http://apir.iir.edu.ua/index.php/apmv/article/view/3827/3487

18. La loi NIS2. URL: https://atwork.safeonweb.be/fr/nis2.

19. NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz. URL: https://www.bundestag.de/presse/hib/kurzmeldungen-1022586.

20. Commission calls on 19 Member states to fully transpose the NIS2 Directive. URL: https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive.

21. Про основи всебічного залучення приватного сектору та громадянського суспільства до здійсмнення заходів зі стримування деструктивної діяльності в кіберпросторі: проект Закону України від 01 серпня 2025 р. №13592. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/56929.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~