ДОСЛІДНИЦЬКА СЛУЖБА
ВЕРХОВНОЇ РАДИ УКРАЇНИ

Парламентське дослідження щодо особливостей законодавчого забезпечення державно-приватного партнерства у сфері забезпечення кібербезпеки на прикладі деяких європейських держав

2025

Парламентське дослідження щодо особливостей законодавчого забезпечення державно-приватного партнерства у сфері забезпечення кібербезпеки на прикладі деяких європейських держав*

Анотація. *У парламентському дослідженні висвітлено досвід деяких держав-членів Європейського Союзу щодо нормативного регулювання розвитку засад державно-приватного партнерства у сфері кібербезпеки, у зв'язку з чим проаналізовано законодавство п'яти держав Європейського Союзу: Німеччини, Естонії, Нідерландів, Франції, Швеції. На підставі проведеного аналізу розглянуто існуючі моделі державно-приватного партнерства у сфері кібербезпеки, узагальнено порядок, умови та особливості здійснення державно-приватного партнерства в цій галузі.*

Ключові слова: *державно-приватне партнерство, кібербезпека, кіберзагроза, кіберпростір, національна безпека, інформаційно-комунікаційні технології, критична інфраструктура, сектор безпеки і оборони, громадянське суспільство.*

Зміст

І. Вступна частина

Актуальність дослідження. Кібербезпека була і залишається одним із ключових напрямів державної політики у сфері забезпечення національної безпеки в усьому світі. Україна, відчуваючи безпрецедентний тиск потужних кібератак, масштабування та збільшення чисельності кіберзагроз, активно опікується питаннями посилення кіберзахисту державних інформаційних ресурсів та критичної інфраструктури. В умовах швидкого й динамічного розвитку інформаційно-комунікаційних технологій надзвичайно важливим є формування ефективних і виважених підходів, які мають забезпечити надійний кіберзахист та кіберстійкість як об'єктів критичної інфраструктури, так і всіх інформаційних систем, що вимагає налагодження ефективної та комплексної співпраці між державою й приватним сектором, включаючи створення сучасної нормативно-правової бази, підготовку експертів і фахівців, які зможуть протистояти будь-яким загрозам у кіберпросторі.

Саме державно-приватне партнерство є одним з основних напрямів організації діяльності із забезпечення кібербезпеки України як стану 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, хакери), мають необхідний спектр знань, навичок і вмінь у питаннях забезпечення кібербезпеки, зокрема розробки та впровадження комплексного ліцензійного програмного забезпечення, створення потужних дата-центрів для зберігання і обробки цифрових даних тощо.

Важливою складовою державної політики у сфері кібербезпеки є державно-приватне партнерство з метою посилення кіберстійкості в умовах війни, адже консолідація спроможностей, зусиль і ресурсів дозволяє організувати потужний кіберзахист на національному рівні, забезпечуючи ефективну протидію сучасним кіберзагрозам. Окрім того, в умовах стрімкої цифровізації усіх сфер життєдіяльності суспільства та держави кожна бізнес-структура має дбати не лише про захист персональних даних своїх клієнтів чи комерційної таємниці, але й гарантувати й забезпечувати всебічний кіберзахист усіх своїх процесів та об'єктів критичної інфраструктури від потенційних ворожих посягань, особливо у кіберпросторі. Залучення суб'єктів приватного сектору до побудови надійної та повноцінної системи кіберзахисту є спільним завданням держави та цивільного сектору кібербезпеки. Міжнародний досвід у цій площині переконливо засвідчує важливість значення ролі інституцій громадянського суспільства та приватного сектору у питаннях забезпечення кібербезпеки.

В умовах правового режиму воєнного стану, запровадженого у зв'язку з 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, зокрема й поза межами державного сектору, для спільного реагування на загрози та мінімізації їх наслідків, що зумовлює необхідність удосконалення правового врегулювання такої комплексної і паритетної взаємодії. Російська військова агресія також

продемонструвала, що влада й бізнес мають бути надійними партнерами та союзниками, співпрацювати одне з одним у питаннях забезпечення кібербезпеки і 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 програмне забезпечення, розроблене приватними компаніями. Таким чином, в Україні в рамках чинного законодавства поступово розвивається синергія між державою та приватним сектором у кібернетичній сфері: створюються інформаційно-аналітичні центри при підприємствах та організаціях критичної інфраструктури, запускаються платформи обміну інформацією про кіберзагрози тощо.

Загалом в Україні державно-приватне партнерство у сфері забезпечення кібербезпеки регулюється такими законодавчими актами: «Про національну безпеку», «Про державно-приватне партнерство», «Про основні засади забезпечення кібербезпеки», «Про критичну інфраструктуру», «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» тощо. Пунктом 14 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 07 березня 2025 р. № 204, передбачено розроблення дієвих механізмів залучення фахівців приватного сектору з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021, декларує, що стратегічним завданням України є створення необхідних передумов для забезпечення стримування агресивних дій у кіберпросторі шляхом застосування економічних, дипломатичних, розвідувальних заходів, а також залучення потенціалу приватного сектору.

Відповідно до статті 10 Закону України «Про основні засади забезпечення кібербезпеки» державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом: 1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій; 2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту; 3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів; 4) партнерства та координації команд реагування на комп'ютерні надзвичайні події; 5) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки; 6) надання консультативної та практичної допомоги з питань реагування на кібератаки; 7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет; 8) запровадження механізму громадського контролю ефективності заходів із забезпечення

кібербезпеки; 9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки; 10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки; 11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

Державно-приватне партнерство у сфері забезпечення кібербезпеки включає такі основні напрями: 1) кіберзахист державних і приватних інформаційних ресурсів, інформаційно-комунікаційних та ІТ-систем, обмін інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз, спрямованих на об'єкти критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів; 2) стимулювання розроблення вітчизняних програмних продуктів, зокрема програмного забезпечення з відкритим кодом, що пріоритетно використовуватимуться для обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури, спільна розробка ліцензованого програмного забезпечення, створення потужних дата-центрів для зберігання і обробки цифрових даних; 3) організація і проведення спільних науково-практичних заходів, присвячених тематиці забезпечення кібербезпеки, розробка та практична реалізація програм підвищення кваліфікації фахівців державних органів, що безпосередньо виконують функції із забезпечення кібербезпеки й кіберзахисту, шляхом залучення сертифікованих за міжнародними стандартами фахівців приватного сектору; 4) здійснення громадського контролю ефективності заходів у сфері забезпечення кібербезпеки. Таким чином, держава у взаємодії з приватним сектором ставить завдання щодо побудови ефективної моделі відносин у сфері кібербезпеки, яка заснована на довірчих стосунках. Державно-приватне партнерство надає змогу більш ефективно здійснювати розподіл ризиків між державним та приватним секторами.

Враховуючи сучасні виклики й загрози, забезпечення належного нормативно-правового підґрунтя задля організації та здійснення ефективної конструктивної співпраці між представниками приватного сектору, громадянського суспільства й органів 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 й державних інституцій – є важливим сучасним завданням держави і, зокрема, сектору безпеки і оборони України.

Також варто відмітити, що тематика розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки залишається доволі актуальною серед вітчизняних та іноземних практиків і науковців. Кращі закордонні практики розбудови державно-приватного партнерства у сфері кібербезпеки досліджували у

своїх наукових працях: В. Бойко[1], В. Григоренко[2], Д. Дубов[3], Г. Малахов[4], О. Фролова і О. Кучмій[5] та інші. Серед наукового доробку останніх років можна виділити роботи, які містять законотворчі ініціативи щодо удосконалення механізмів державно-приватного партнерства у сфері забезпечення кібербезпеки, у тому числі критичної та стратегічної інфраструктури України, зокрема: Г. Зубка[6], В. Круглова[7], С. Сєрєбряка[8], О. Шевчук та Є. Чорного[9]. Проблематику державно-приватного партнерства в секторі безпеки висвітлювали у своїх наукових працях: Ю. Заскока[10], Ю. Мех[11], Ю. Романюк та В. Паливода[12] та інші.

В умовах зростаючої кількості кіберінцидентів, тенденційного збільшення масштабів кіберзагроз, які завдають значної шкоди інформаційно-телекомунікаційним системам, економіці й національній безпеці, нормативно-правове регулювання організаційно-правових засад розбудови державно-приватного партнерства потребує удосконалення з метою розробки та впровадження комплексних заходів у сфері кібербезпеки.

Реалізація пріоритетних засад державної політики у цій сфері вимагає системного залучення потенціалу приватного сектору та громадянського суспільства з метою прогнозування та мінімізації кіберризиків, посилення кіберзахисту об'єктів критичної інфраструктури, протидії ворожій деструктивній діяльності в кіберпросторі, налагодження механізмів комплексної взаємодії й співпраці між державними органами, бізнесом і громадськістю у сфері кібербезпеки, формування культури цифрової безпеки в суспільстві, що охоплює громадян, бізнес-структури та уповноважені державні інституції. Вони мають бути адаптовані до сучасних

---

[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.

[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] 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

[6] 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

[7] 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.

[8] 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

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

[10] 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

[11] 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

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

тенденцій такої співпраці, а також кращих практик закордонного досвіду держав-членів ЄС у цій площині.

Наведене засвідчує актуальність поставлених питань і доцільність висвітлення кращих закордонних практик законодавчого забезпечення розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки.

Метою дослідження є узагальнення закордонного досвіду деяких держав-членів Європейського Союзу (далі – ЄС) (Німеччини, Естонії, Нідерландів, Франції та Швеції) щодо нормативного регулювання розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки, визначення його особливостей з метою запозичення окремих законодавчих підходів у національне законодавство.

Предметом дослідження є законодавство ЄС, що визначає загальні засади здійснення державно-приватного партнерства у сфері кібербезпеки, зокрема Директива (ЄС) 2022/2555 (NIS2)[13] (далі – Директива NIS2), законодавство держав ЄС (Німеччини, Естонії, Нідерландів, Франції та Швеції), що визначає напрями та зміст державно-приватного партнерства у сфері забезпечення кібербезпеки.

ІІ. Основна частина

1. Європейські стандарти державно-приватного партнерства у сфері кібербезпеки.

В Європейському Союзі державно-приватне партнерство у сфері кібербезпеки розвинено в більшості держав-членів, що надає сприятливу можливість консолідувати співпрацю між урядом, приватним сектором і громадянським суспільством. В умовах тривалої російської військової агресії для переважної більшості держав ЄС роль та значення кібербезпеки постійно зростає.

Ключову роль у розбудові державно-приватного партнерства у сфері забезпечення кібербезпеки відіграє Директива NIS2 від 14 грудня 2022 року (набула чинності 16 січня 2023 року), якою запроваджено системні заходи, спрямовані на досягнення високого загального рівня кібербезпеки на теренах ЄС з метою покращення функціонування внутрішнього цифрового ринку.

Директива NIS2 запроваджує комплексний та гармонізований підхід до питань забезпечення кібербезпеки, посилення захисту критичної інфраструктури, цифрових послуг і громадян ЄС від зростаючої загрози кіберінцидентів та кібератак.

Директива NIS2 встановлює 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 (CERT); запроваджує заходи з управління ризиками кібербезпеки та встановлює 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 відповідно до положень Директиви (ЄС) 2022/2557; встановлює правила та визначає зобов'язання щодо обміну інформацією про кібербезпеку; визначає наглядові та

[13] 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

примусові зобов'язання держав-членів ЄС[14], які поширюються як на операторів, так і на постачальників цифрових послуг, критично важливих технологій та органи державного управління.

Ключові завдання Директиви NIS2 передбачають: встановлення стандартного набору вимог щодо кібербезпеки для всіх держав-членів ЄС; розширення сфери її дії для охоплення більшої кількості секторів економіки та визначення відповідальних суб'єктів; запровадження більш суворих зобов'язань щодо процедур звітності про кіберінциденти та заходів правозастосування; сприяння кращій співпраці та обміну інформацією між державами-членами ЄС щодо кіберінцидентів та кіберзагроз; забезпечення високого рівня кіберстійкості як важливого стандарту на теренах ЄС.

Також документ спрямований на підвищення рівня безпеки мережевих та інформаційних систем у державах-членах ЄС, сприяючи співпраці між державним і приватним секторами. Здійснено розподіл усіх організацій на два види: «критично важливі» (Essential Entities) та «важливі» (Important Entities), що охоплює як великі, так і середні приватні компанії, які мають значний вплив на економіку й цифрову інфраструктуру. Це сприяє активній співпраці приватних компаній з державними органами для забезпечення вимог і критеріїв відповідності стандартам кібербезпеки.

Директива NIS2 заохочує створення міждержавних структур управління кіберкризами (наприклад, EU-CyCLONe)[15] та національних стратегій кібербезпеки, які визначають роль і місце приватного сектору в питаннях забезпечення кібербезпеки, запроваджує більш сувору відповідальність, що включає чималі штрафи й адміністративні стягнення для керівництва за невідповідність установленим стандартам та вимогам, із метою стимулювання приватних компаній активно співпрацювати з державними органами для уникнення санкцій, що сприяє формуванню посиленого формату такої співпраці.

Відповідно до частини четвертої статті 9 Директиви NIS2 кожна держава-член ЄС повинна схвалити Національний план реагування на масштабні кіберінциденти, який має визначати, зокрема: мету та цілі національних заходів; завдання і відповідальність органів управління; національні заходи кіберготовності, включаючи навчання та освітню діяльність; національні процедури між відповідними національними органами, заходи підтримки скоординованого управління великомасштабними інцидентами та кризами кібербезпеки на рівні ЄС.

У Директиві NIS2 акцентовано, що державно-приватне партнерство підвищує довіру до продуктів і послуг у сфері інформаційно-комунікаційних технологій, що є також вигідним для приватного сектору. 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. Встановлено, що

---

[14] Аналітична записка з питань порівняльного законодавства Європейського Союзу, держав-членів ЄС та інших держав щодо забезпечення кібербезпеки. URL: https://research.rada.gov.ua/documents/analyticRSmaterialsDocs/industry_policy/analytical_notes-indst/73998.html

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

напрями 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 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 CERT, EU-CyCLONe. Також приватні компанії зобов'язані ділитися інформацією про кіберінциденти, а держава надає підтримку у вигляді аналізу кіберзагроз і формує відповідні рекомендації, які поширюються на всю кіберспільноту (державний та приватний сектор). Важливою складовою є організація навчання й підвищення кваліфікації, що передбачає спільні тренінги та симуляції кібератак (наприклад, проєкт Cyber Europe)[16], де державні та приватні структури спільно відпрацьовують навички й уміння, реалізують заходи у сфері координації та екстреного реагування.

До недоліків у питаннях забезпечення кібербезпеки між державою та приватним сектором належать: фрагментація стандартів (попри єдині рамки, встановлені європейським законодавством, держави-члени ЄС тлумачать і впроваджують встановлені вимоги по-різному, що певним чином ускладнює співпрацю та її параметри); відсутність єдиного підходу щодо форм та методів побудови взаємодії між державним і приватним сектором; наявність системних помилок у процесі побудови взаємовідносин держави з бізнесом, що певним чином викликає недовіру; відсутність чітко визначених повноважень і компетенції у відповідальних державних органів, які виступають в якості сторони партнерських відносин із приватними бізнес-структурами.

На виконання закріплених вимог усі держави-члени ЄС мали до 17 жовтня 2024 року розробити та схвалити відповідний законопроект, який безпосередньо імплементує положення Директиви NIS2, одночасно визначити перелік заходів, спрямованих на забезпечення високого загального рівня кібербезпеки. Також відповідні національні закони повинні регулювати питання державно-приватного партнерства у сфері забезпечення кібербезпеки, визначати умови, порядок і моделі такої комплексної взаємодії, містити імперативну вимогу про те, що приватний сектор зобов'язаний не лише управляти кіберризиками та запобігати кіберінцидентам, але й вживати заходів з метою пом'якшення їх катастрофічних наслідків, співпрацюючи в цьому напрямі з державою.

Проте, не всі держави ЄС своєчасно виконали зазначені вимоги. Так, лише 14 із 27 держав ЄС імплементували Директиву NIS2 у національне законодавство (Бельгія, Данія, Греція, Італія, Литва, Латвія, Фінляндія, Румунія, Хорватія, Словаччина, Словенія, Угорщина, Кіпр, Люксембург). Враховуючи такий стан справ, Європейська Комісія у травні 2025 року офіційно звернулася до політичного

[16] Cyber Europe. URL: https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe

керівництва деяких держав-членів ЄС із жорстким попередженням та вимогою прискорити процедури імплементації Директиви NIS2 у національне законодавство[17]. У контексті практичної реалізації положень Директиви NIS2 державно-приватне партнерство є важливими аспектом для забезпечення мережевої безпеки та стійкості критичної інформаційної інфраструктури.

Важливе значення у сфері розбудови державно-приватного партнерства має закон ЄС про кіберсолідарність[18], який набув чинності 4 лютого 2025 року. Він спрямований на зміцнення спроможностей держав-членів ЄС попереджувати та виявляти кіберзагрози й кібератаки, передбачає створення Європейської системи оповіщення у сфері кібербезпеки, запровадження комплексного механізму подолання надзвичайних ситуацій для підвищення кіберстійкості на теренах ЄС. У структурі Європейської системи оповіщення у сфері кібербезпеки було створено об'єднані національні кіберцентри (транскордонні кіберцентри) з метою оперативного обміну інформацією. Загальною метою діяльності кіберцентрів є зміцнення кіберпотенціалу для аналізу, запобігання та виявлення будь-яких кіберзагроз. У рамках законодавчого регулювання транскордонні кіберцентри та команди реагування на надзвичайні ситуації (CERT) повинні тісно співпрацювати для забезпечення синергії, відповідно до протоколів співпраці здійснювати обмін інформацією про кіберзагрози та значні кіберінциденти. З огляду на важливу роль, яку відіграють представники приватного сектору, зокрема приватні підприємства, установи та організації, у контексті виявлення та реагування на кіберінциденти, кожна держава-член ЄС має залучати їх на довірчих засадах до процесів забезпечення кібербезпеки, зокрема у питаннях обробки конфіденційної інформації.

У рамках розбудови механізмів реагування на надзвичайні ситуації у сфері кібербезпеки було створено резерв кібербезпеки ЄС, який складається зі служб екстреного реагування, та який включає перелік довірених постачальників, уповноважених здійснювати заходи з метою відновлення пошкоджених або знищених інформаційно-комунікаційних систем за наслідками масштабних кіберінцидентів, що можуть негативно впливати на держави-члени, приватні установи, організації, офіси тощо. Резерв кібербезпеки ЄС має на меті підтримку національних органів влади у сфері надання допомоги постраждалим організаціям, що працюють у секторах з високою критичністю. Резерв кібербезпеки ЄС також забезпечуватиме підтримку приватного сектору – установ, організацій за аналогічних умов. Представники приватного сектору відіграють важливу роль у виявленні та реагуванні на масштабні кіберінциденти, така співпраця між ними та державою здійснюється на добровільних і паритетних засадах.

2. Законодавче забезпечення державно-приватного партнерства у сфері кібербезпеки в деяких державах ЄС.

Важливим компонентом посилення спроможностей держави у сфері забезпечення кібербезпеки є побудова конструктивного діалогу у форматі державно-

[17] 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
[18] EU Cyber Solidarity Act. URL: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

приватного партнерства, без якого неможливо налагодити ефективну та надійну співпрацю, запровадити комплексний механізм швидкого й оперативного реагування на кіберзагрози та інші виклики в кіберпросторі.

Кожна держава ЄС за власної ініціативи створює інституційні механізми, розробляє організаційно-правові засади розбудови державно-приватного партнерства у сфері кібербезпеки, впроваджує власну модель державно-приватного партнерства, при цьому має власний унікальний досвід налагодження паритетної співпраці з приватним сектором. Розглянемо кращі закордонні практики деяких держав-членів ЄС (Німеччини, Естонії, Нідерландів, Франції та Швеції) щодо законодавчого забезпечення розвитку державно-приватного у сфері забезпечення кібербезпеки.

Німеччина. Правовою основою розбудови державно-приватного партнерства в досліджуваній сфері став Національний план захисту інформаційної інфраструктури, який у 2011 році було трансформовано в Національну стратегію кібербезпеки Німеччини[19]. Подальший розвиток пріоритетів державно-приватного партнерства у сфері кібербезпеки було закладено в положеннях Стратегії кіберзахисту Німеччини 2016 року[20]. Відповідальним за координацію у сфері забезпечення кібербезпеки Німеччини є Федеральне відомство з питань інформаційної безпеки. Заходи у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури Німеччини визначено в таких федеральних законах: «Про Федеральне відомство з питань інформаційної безпеки» (BSIG)[21], «Про постачання електроенергії та газу» (EnWG)[22], «Про телекомунікації» (TKG)[23]. Захист критичної інфраструктури в Німеччині на стратегічному та операційному рівнях здійснюється в рамках реалізації Національної стратегії захисту критичної інфраструктури[24]. Німеччина приділяє особливу увагу безпеці промислових систем. Зокрема, це завдання реалізується через ініціативи на кшталт Альянсу для кібербезпеки (Allianz für Cybersicherheit), який координується Федеральним відомством з інформаційної безпеки та об'єднує органи державної влади, приватні компанії і наукові установи для захисту критичної інфраструктури (KRITIS), а також для обміну інформацією. У цьому контексті провідні компанії, такі як «Siemens», надають технологічні рішення для державних потреб, сприяючи реалізації проєктів у сфері цифрової безпеки та захисту критичної інфраструктури. Водночас захист критичної інфраструктури вимагає комплексної співпраці на рівні федеральних відомств у межах їх компетенції та органів влади федеральних земель у межах розподілу повноважень.

---

[19] Cyber Security Strategy for Germany. 2011. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Germany_2011_Cyber_Security_Strategy_for_Germany.pdf

[20] Cyber-Sicherheitsstrategie für Deutschland 2016. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2016.pdf?__blob=publicationFile&v=3

[21] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG). URL: https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html

[22] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG). URL: HTTPS://WWW.GESETZE-IM-INTERNET.DE/ENWG_2005/BJNR197010005.HTML

[23] Telekommunikationsgesetz. URL: https://www.gesetze-im-internet.de/tkg_2021/

[24] Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3

Сфера державно-приватного партнерства у сфері кібербезпеки між операторами критично важливої інфраструктури та державними органами безпосередньо врегульовується Планом реалізації KRITIS (Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen)[25], що є складовою частиною Національного плану захисту інформаційної інфраструктури[26]. План реалізації KRITIS поширюється на приватних операторів і постачальників критичної інфраструктури, зокрема підприємства й організації, які спеціалізуються на транспортних перевезеннях, енергетиці, інформаційних технологіях та телекомунікаціях тощо[27]. Важливу роль у забезпеченні державно-приватного партнерства відіграє створений у 2018 році Кластер кібербезпеки міста Бонн (Cyber Security Cluster Bonn), який об'єднує понад 100 компаній, федеральних і земельних установ, а також університетів, таких як Боннський університет і Університет прикладних наук Бонн-Рейн-Зіг. Тісна співпраця надає унікальну платформу для пошуку оптимальних шляхів попередження і протидії кіберзагрозам, підвищення кваліфікації та підготовки IT-фахівців. У зв'язку з обмеженими кадровими можливостями цього кластеру, місто Бонн (колишня столиця ФРН до 1990 року) планує надати додаткову фінансову підтримку в обсязі 40 тис. євро на 2025/2026 роки[28]. Також слід відзначити, що в Німеччині стартапи в галузі кібербезпеки отримують значну підтримку завдяки державним грантам і програмам партнерства з великими IT-компаніями.

Важлива роль відводиться команді реагування на комп'ютерні інциденти CERT-Bund, яка в межах функціонування сервісу Bürger-CERT інформує приватних користувачів (фізичних осіб, бізнес) шляхом надання безкоштовної та незалежної інформації щодо актуальних кіберзагроз, включаючи шкідливе програмне забезпечення і вразливості інформаційно-комунікаційних систем[29]. Цей сервіс функціонує як модель комунікації та побудови довіри між державними структурами і приватним сектором у контексті розбудови державно-приватного партнерства. Німецький національний центр кіберреагування (Nationales Cyber-Abwehrzentrum, NCAZ) здійснює координацію дій з реагування на кіберінциденти та забезпечує обмін інформацією в цій сфері[30]. Дієвим інструментом для розвитку інноваційних рішень у сфері кібербезпеки, а також для налагодження тісної співпраці між технічною спільнотою, приватним сектором і державними інституціями виступають хакатони –

---

[25] Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/umsetzungsplan-kritis.pdf?__blob=publicationFile&v=4

[26] Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). URL: https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/05-12-09/05-12-09-anlage-nr-16.pdf?__blob=publicationFile&v=2

[27] Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/umsetzungsplan-kritis.pdf?__blob=publicationFile&v=4

[28] Фінансова підтримка проекту «Кібер-кампус Бонн». URL: https://www.bonn.de/pressemitteilungen/april/finanzielle-unterstuetzung-fuer-projekt-cyber-campus-bonn.php?loc=uk

[29] CERT-Bund. URL: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

[30] Державно-приватне партнерство у сфері кібербезпеки: Міжнародний досвід та можливості для України. Аналітична доповідь. 2018. URL: https://niss.gov.ua/publikacii/analitichni-dopovidi/derzhavno-privatne-partnerstvo-u-sferi-kiberbezpeki-mizhnarodniy-0

форуми для розробників програмного забезпечення та інших фахівців (програмістів, системних адміністраторів, дизайнерів).

Модель державно-приватного партнерства у сфері кібербезпеки, що реалізується Німеччиною, базується на пріоритеті посиленого захисту критичної інфраструктури, створенні сучасних платформ для взаємодії, налагодженні оперативного обміну інформацією, впровадженні сервісного підходу в питаннях кіберзахисту, розробці освітніх програм і забезпечення виконання європейських стандартів. Особливістю державно-приватного партнерства у сфері забезпечення кібербезпеки Німеччини є функціонування інституціональних платформ взаємодії між державними органами влади та підприємствами, до яких належать координаційні групи з питань захисту критичної інфраструктури (KRITIS) на трьох адміністративних рівнях: федеральному, на рівні федеральних земель та органів місцевого самоврядування.

Водночас одним із викликів, що впливає на ефективність державно-привтаного партнерства у сфері кібербезпеки залишається кадрова нестача в окремих структурах, відповідальних за координацію взаємодії. Також Німеччина все ще не гармонізувала своє національне законодавство відповідно до вимог Директиви NIS2, а відповідний законопроект щодо її імплементації[31] перебуває на стадії розгляду в парламентських комітетах та очікувано може бути схвалений тільки у 2026 році[32].

Естонія. Сфера забезпечення кібербезпеки регулюється в Естонії такими законодавчими актами: «Про кібербезпеку»[33], «Про захист персональних даних»[34], «Про електронні комунікації»[35]. У 2024 році була схвалена оновлена Стратегія кібербезпеки Естонії на 2024–2030 роки[36], пріоритетним завданням якої визначено прискорення імплементації в національне законодавство директив та регламентів ЄС і НАТО, побудова паритетного балансу інтересів між державою і приватним сектором, дотримання свободи цифрового підприємництва, вимог та стандартів у сфері кібербезпеки. Ключова увага стратегії приділяється зміцненню системи кібербезпеки Естонії у відповідь на глобальні кіберзагрози, що розвиваються, особливо в контексті зростання транснаціональної кіберзлочинності, геополітичного суперництва й протиборства, які виникають внаслідок війни Росії проти України. На рівні Стратегії важливою складовою забезпечення кібербезпеки визначено саме державно-приватне партнерство, яке спрямовано на захист цифрової інфраструктури, забезпечення національної кіберстійкості.

---

[31] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz). URL: https://dip.bundestag.de/vorgang/gesetz-zur-umsetzung-der-nis-2-richtlinie-und-zur-regelung-wesentlicher-grundz%C3%BCge/314976?f.wahlperiode=20&f.typ=Vorgang&start=25&rows=25&sort=datum_ab&pos=38&ctx=d

[32] Understanding the implications and technical standards of NIS 2 for German entities. URL: https://cyberupgrade.net/blog/compliance-regulations/understanding-the-implications-and-technical-standards-of-nis-2-for-german-entities/?utm_source=chatgpt.com

[33] Küberturvalisuse seadus 09.05.2018. URL: https://www.riigiteataja.ee/akt/122052018001

[34] Isikuandmete kaitse seadus 12.12.2018. URL: https://www.riigiteataja.ee/en/eli/523012019001/consolide

[35] Elektroonilise side seadus 08.12.2004. URL: https://www.riigiteataja.ee/akt/127022022003

[36] Cybersecurity Strategy 2024-2030 «Cyber-Conscious Estonia». URL: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

Національним координатором у сфері забезпечення кібербезпеки визначено Державне управління інформаційних систем Естонії[37], діяльність якого спрямована на виявлення загрозливих тенденцій, розвиток цифрових послуг та підвищення загальної цифрової обізнаності в рамках розбудови державно-приватного партнерства.

Державно-приватне партнерство у сфері забезпечення кібербезпеки включає: розробку та надання рекомендацій для приватного сектору за наслідками виявлення й відстеження кіберінцидентів у кіберпросторі; проведення заходів, спрямованих на спільне вивчення та опанування здобутого сучасного позитивного досвіду запобігання кібератакам і кіберзагрозам; постійне удосконалення політики «Government Relations» у сфері забезпечення кібербезпеки, яка базується на інтеграції державного та приватного секторів, що дозволяє ефективно протистояти кіберзагрозам і гарантувати цифрову кіберстійкість на всіх рівнях.

Естонія є першої державою ЄС, яка впровадила концепцію політики «Government Relations» (GR) у сфері кібербезпеки, що зумовлено високим рівнем цифровізації, набутим позитивним досвідом протистояння кібератакам та реалізацією стратегічного підходу до міжнародної кібербезпекової співпраці. Особливістю державно-приватного партнерства у сфері забезпечення кібербезпеки Естонії є активне залучення приватного сектору до розробки засад кібербезпекової політики. Так, уряд Естонії співпрацює з приватними технологічними компаніями, IT-компаніями, такими як «Guardtime» та «CybExer Technologies», із метою розробки стратегічних рішень у сфері посилення кіберзахисту як державних, так і приватних інформаційних ресурсів, активно використовує при цьому блокчейн технології. Наприклад, компанія «Guardtime», яка спеціалізується на блокчейн-технологіях, співпрацює з урядом Естонії з метою захисту державних інформаційних даних, зокрема електронних медичних записів (e-Health), системи електронного врядування. Технологічний гігант «CybExer Technologies» розробляє рішення для організації та проведення кібернавчань, які, своєю чергою, використовуються державними установами для тестування кіберстійкості об'єктів критичної інфраструктури. Приватні IT-компанії співпрацюють із державою з метою організації тренінгів для державних службовців і працівників критичної інфраструктури. Уряд Естонії створив платформи для оперативного обміну даними про кіберзагрози між державою та приватним сектором.

Механізми розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки в Естонії передбачають створення кібертехнологічного кластера з метою обміну знаннями й навичками між державним і приватним секторами, який об'єднує провідні компетенції та набутий передовий досвід у сфері кібербезпеки. Естонський кібертехнологічний кластер передбачає організацію навчання для підвищення освітніх стандартів та обізнаності серед представників бізнес-структур у сфері кібербезпеки[38]. До пріоритетних завдань кібертехнологічного кластера Естонії у рамках розбудови державно-приватного партнерства у сфері кібербезпеки відносяться: підвищення освітніх стандартів у сфері кібербезпеки; впровадження

[37] Riigi Infosüsteemi Amet (RIA). URL: https://www.ria.ee/en

[38] Eesti CyberTech klaster. URL: https://itl.ee/cybertech

інновацій (сучасної методології та процедур виявлення загроз); побудова конструктивного діалогу й співпраці між державним і приватним секторами критичної інфраструктури; активізація процесу структурного розвитку архітектури та систем кібербезпезпеки; побудова найвищого ступеня довіри між державою і приватним сектором; активна взаємодія між учасниками кластера, бізнес-середовищем, представниками держави й академічною спільнотою; формування та розвиток професійного кадрового потенціалу у сфері кібербезпеки; розвиток субкультури кібербезпеки, поширення знань про безпечну поведінку в цифровому просторі тощо.

Тому державно-приватне партнерство передбачає професійні освітні заходи, навчання та підвищення кваліфікації з метою отримання навичок у сфері оцінки ризиків, управління кіберінцидентами та проведення аналізу кіберзагроз. Спільний підхід включає діяльність уряду, приватного сектору, академічної спільноти й представників суб'єктів господарювання і цифрової індустрії. Щорічно в Естонії проводиться Північно-балтійський саміт із безпеки[39], під час якого питання забезпечення кібербезпеки і, зокрема, управління уразливостями в кіберпросторі обговорюються на рівні держави, бізнесу та кіберспільноти.

Естонія як одна з найбільш цифровізованих держав світу ефективно залучає до співпраці приватний сектор, що дозволяє створювати інноваційні рішення, швидко реагувати на кіберзагрози, зміцнювати міжнародну позицію країни у сфері глобальної кібербезпеки.

Нідерланди. Законодавство у сфері забезпечення кібербезпеки включає Стратегію кібербезпеки на 2022–2028 роки[40] та закон «Про безпеку мереж та інформаційних систем».[41] Законодавство Нідерландів у сфері кібербезпеки є комплексним, частково імплементує директиву NIS 2, тобто базується на європейських стандартах з акцентом на посилений захист об'єктів критичної інфраструктури та розбудову державно-приватного партнерства, спрямоване на підвищення цифрової стійкості Нідерландів. Основна концепція законодавства у сфері забезпечення кібербезпеки із залученням державно-приватного партнерства в Нідерландах передбачає спільне формування кіберстійкості уряду, бізнесу та організацій громадянського суспільства, що включає розробку та вжиття комплексу заходів, спрямованих на запобігання кіберінцидентам, мінімізацію збитків від кібератак та сприяння швидкому й оперативному відновленню IT-систем і критичної інфраструктури, при цьому громадянське суспільство відіграє важливу роль у розвитку цифрових навичок – від базових знань і вмінь до високого рівня експертизи.

Уряд Нідерландів активно працює над імплементацією Директиви ЄС NIS2 у національне законодавство, що має завершитися до кінця 2025 року. Очікується, що оновлений закон має посилити вимоги до стратегічних засад розбудови державно-

---

[39] CYBERS on nüüd NEVERHACK Estonia. URL: https://neverhack.ee/?gad_source=1&gad_campaignid=21726399961&gbraid=0AAAAAC75nmCnbaWKMJbrqm2GwrFJGJywy&gclid=EAIaIQobChMIudHK3PSYjwMVskGRBR3QwAMAEAAYASAAEgIoYfD_BwE

[40] Netherlands Cybersecurity Strategy 2022-2028. (NLCS). URL: https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/netherlands-cybersecurity-strategy-2022-2028

[41] Wet beveiliging netwerk- en informatiesystemen (Wbni). 09.11.2018. URL: https://wetten.overheid.nl/BWBR0041515/2024-10-01

приватного партнерства та кіберстійкості[42]. Державно-приватне партнерство у сфері кібербезпеки в Нідерландах є прикладом ефективної співпраці між урядом, приватним сектором і науковими академічними установами для захисту національного сегмента кіберпростору.

Національним координатором у сфері забезпечення кібербезпеки в Нідерланадах визначено міністра юстиції та безпеки[43], який у рамках повноважень курирує діяльність Національного центру кібербезпеки[44] – установи, яка об'єднує тактичні та оперативні знання, набутий досвід співпраці державного й приватного секторів. Відповідно до компетенції Національний центр кібербезпеки сприяє постачальникам цифрових послуг та уряду Нідерландів у питаннях взаємодії; інформує з питань кіберзагроз і кіберінцидентів для мережевих й інформаційних систем постачальників цифрових послуг та уряду; проводить аналіз і технічні дослідження кіберзагроз або ознак їх виникнення; сприяє обміну інформацією між державою, уповноваженими підприємствами й організаціями, громадськістю. Національний центр кібербезпеки активно співпрацює з приватними компаніями для захисту критичних секторів, особливо портів Роттердама, національних банківських і фінансових установ.

Нідерланди активно розвивають механізми державно-приватного партнерства, що ґрунтуються на взаємній довірі, обміні інформацією та спільному реагуванні на кіберзагрози, що засвідчує сервісну модель такої співпраці, яка здійснюється під егідою центрів обміну та аналізу інформації ISAC[45], завдяки яким компанії з різних секторів (енергетика, фінанси, телекомунікації) обмінюються даними про кіберзагрози в режимі реального часу. Метою їх діяльності є підвищення цифрової стійкості шляхом обміну інформацією про кіберзагрози, вразливості та кіберінциденти, що включає обмін інформацією про кібератаки, виявлені нові типи шкідливого програмного забезпечення або вразливості щодо програмного забезпечення. Учасниками ISAC є приватні компанії, державні установи та інші зацікавлені сторони, які спільно забезпечують безпечний обмін інформацією. У рамках ISAC аналізується інформація про кіберзагрози й кіберінциденти, а результатом цього аналізу є звіти, які допомагають формулювати рекомендації та плани дій для всієї кіберспільноти. Співпраця у рамках державно-приватного партнерства включає організацію та проведення спільних кібернавчань, діяльність інноваційних хабів тощо.

Щорічно в Нідерландах проводяться навчання «Exercise ISIDOOR»[46], під час яких здійснюється моделювання кіберінцидентів, формування плану дій на випадок несанкціонованого витоку даних або виявлення вразливості в ІТ-системах. У рамках навчання уряд співпрацює з приватним сектором з метою схвалення рішень щодо

---

[42]Cyberbeveiligingswet. URL: https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel%3A36764#wetgevingsproces

[43] Ministerie van Justitie en Veiligheid. URL: https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid

[44] Nationaal Cyber Security Centrum (NCSC). URL: https://www.nctv.nl/onderwerpen/nationaal-cyber-security-centrum

[45] Information Sharing and Analysis Centers (ISAC). URL: https://www.digitaltrustcenter.nl/wat-is-een-isac

[46] Cyber Exercise with Public and Private Partners. URL: https://securitydelta.nl/news/overview/cyber-exercise-with-pubic-and-private-partners

оперативного реагування на інциденти. Паритетна співпраця між державним та приватним секторами є важливою складовою, оскільки більшість IT-інфраструктур у Нідерландах перебувають у зоні відповідальності саме приватного сектору. У Гаазі створено та діє Нідерландський кластер кібербезпеки[47], який об'єднує уряд, бізнес-структури та дослідницькі інституції з метою розробки інноваційних рішень у сфері кібербезпеки, сприяння стартапам, які створюють нові технології у сфері кіберзахисту. У рамках цього кластера понад 300 компаній, урядових організацій та наукових установ співпрацюють разом, починаючи з 2013 року з метою ,зміни ландшафту кібербезпеки. Сфера діяльності включає обмін знаннями й навичками, тісну співпрацю над інноваційними рішеннями кібербезпеки, які можна масштабувати в Нідерландах і на міжнародному рівні. Важливу роль у питаннях забезпечення кібербезпеки виконує саме приватний сектор, зокрема великі телекомунікаційні компанії на кшалт «Philips», «KPN», «Fox-IT», які активно інвестують у захист власних інформаційно-комунікаційних мереж, співпрацюють з урядом у питаннях забезпечення безпеки національної критичної інфраструктури. При цьому викликом у сфері державно-приватного партнерства залишається проблема побудови довіри, оскільки приватні компанії іноді побоюються відкривати чутливу інформацію через ризики її витоку. У зв'язку з постійним зростанням кіберзагроз та ускладненості кібератак державно-приватне партнерство в Нідерландах адаптується шляхом постійного удосконалення формату співпраці та ініціювання залучення стартапів до навчальних програм.

Франція. Сфера кібербезпеки у Франції врегульована Законом про захист даних 1978 року[48], Законом про комп'ютерне шахрайство 1988 року[49], Законом про цифрову республіку 2016 року[50], Законом про військове програмування 2023 року[51], Законом про безпеку цифрового простору 2024 року[52]. Державним органом, відповідальним за координацію у сфері кібербезпеки, є Національне агентство безпеки інформаційних систем, що надає технічну підтримку операторам критичної інфраструктури у процесі впровадження положень законодавства. Основні засади державної кібербезпекової політики викладені в Національній стратегії кібербезпеки[53], яка є частиною плану «Франція – 2030» і доповнює попередні ініціативи, зокрема Стратегічний огляд кібероборони 2018 року[54] та Національну стратегію цифрової безпеки 2015 року[55] . Форми державно-приватного партнерства у

[47] The Dutch Security Cluster. URL: https://securitydelta.nl

[48] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

[49] Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000875419

[50] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746

[51] Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la defense. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047914986

[52] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique. URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368

[53] Доступ закритий.

[54] Revue stratégique de cyberdéfense. 2018. URL: https://www.sgdsn.gouv.fr/files/files/Publications/20180206-np-revue-cyber-public-v3.3-publication.pdf

[55] Stratégie nationale pour la sécurité du numérique. URL: https://www.cybermalveillance.gouv.fr/medias/2019/11/strategie_nationale_securite_numerique.pdf

сфері кібербезпеки передбачають: надання урядом технічних рекомендацій, безпекових стандартів і експертної підтримки для приватного сектору з метою реагування на кіберінциденти, запобігання загрозам та підвищення загального рівня цифрової стійкості[56]; сприяння розвитку науково-дослідного потенціалу та трансферу інновацій у сфері кіберзахисту до приватного сектору, зокрема через підтримку проєктів, спрямованих на технологічні розробки у сфері кібербезпеки[57]; організацію спільних заходів, присвячених аналізу та впровадженню передового досвіду протидії кібератакам і кіберзагрозам.

Державно-приватне партнерство у сфері кібербезпеки у Франції в освітньому та кадровому вимірах включає: інтеграцію модулів із кібербезпеки до освітніх програм вищої освіти, адаптованих до специфіки кожного напряму підготовки, з метою формування цифрової грамотності та підвищення рівня обізнаності серед майбутніх фахівців; включення навчальних курсів із кіберзахисту до системи безперервної професійної освіти, з урахуванням галузевих потреб і кваліфікаційних вимог, що сприяє оновленню компетенцій працюючих фахівців[58]; запровадження змістовних компонентів із кібербезпеки до програм підготовки кадрів державної служби; врахування аспектів кіберзахисту під час конкурсного відбору та у професійній підготовці спеціалістів, які працюють у сфері інформаційних і комунікаційних технологій.

Стратегічний план діяльності Національного агентства безпеки інформаційних систем на 2025–2027 роки[59], підготовлений у рамках реалізації Національної стратегії кібербезпеки, визначає ключові завдання щодо розвитку національної системи кіберзахисту. Задекларовано, що важливим аспектом є формування сталої мережі взаємодії і координації між основними суб'єктами у сфері кібербезпеки, зокрема структурами державного сектору, суб'єктами реагування на кіберінциденти, представниками приватного сектору та іншими заінтересованими сторонами. У цьому контексті важливу координаційну функцію виконує CERT-FR – національна команда реагування на комп'ютерні інциденти, діяльність якої здійснюється у тісній взаємодії з партнерськими структурами.

За ініціативи Президента Франції було засновано Національний хаб кібербезпеки «Кіберкампус» (Campus Cyber), який функціонує як міжсекторальна платформа співпраці між представниками великого бізнесу, малих і середніх підприємств, стартапів, державного сектору, освітніх і науково-дослідних установ, а також професійних асоціацій. Основною метою діяльності цього кластера є розвиток національного потенціалу у сфері кібербезпеки шляхом консолідації зусиль державних, приватних та академічних суб'єктів.

Важливу роль у розбудові національної інфраструктури кібербезпеки відіграє Кластер передового досвіду в галузі кібертехнологій (Pôle d'Excellence Cyber) – міжгалузева організація, що об'єднує заклади освіти, науково-дослідні установи та

---

[56] Agence nationale de la sécurité des systèmes d'information. URL: https://www.sgdsn.gouv.fr/notre-organisation/composantes/agence-nationale-de-la-securite-des-systemes-dinformation

[57] Dispositifs d'accompagnement nationaux. URL: https://cyber.gouv.fr/dispositifs-daccompagnement-nationaux

[58] Stratégie nationale pour la sécurité du numérique. URL: https://www.cybermalveillance.gouv.fr/medias/2019/11/strategie_nationale_securite_numerique.pdf

[59] Plan stratégique 2025-2027 de l'ANSSI. URL: https://cyber.gouv.fr/publications/plan-strategique-2025-2027-de-lanssi

інноваційні підприємства задля стимулювання синергії у сфері кіберзахисту. Основним завданням кластера є розвиток системного підходу до забезпечення кібербезпеки шляхом координації інноваційної діяльності та просування технологічних рішень. У 2025 році Франція ініціювала створення об'єднаної галузевої платформи «Team France Digital Confidence – Cybersecurity», до якої увійшли державні та приватні учасники. Метою цієї ініціативи визначено консолідацію національного потенціалу у сфері кібербезпеки. У Франції державні установи та об'єкти критичної інфраструктури користуються послугами з кіберзахисту від приватних компаній, таких як «Thales» та «Orange Cyberdefense».

Для стимулювання міжсекторальної співпраці у сфері кібербезпеки у Франції активно застосовуються формати відкритої співпраці – хакатони. Такі заходи об'єднують представників державного сектору, бізнесу, академічної спільноти з метою розробки інноваційних рішень у галузі. Зокрема, серед прикладів таких ініціатив – хакатон «HackX», організований Вищою політехнічною школою, який щорічно збирає понад 500 учасників. Серед ключових напрямів, які розробляються у рамках цього заходу, – штучний інтелект, кібербезпека та принципи сталого цифрового розвитку[60].

Особливостями державно-приватного партнерства у сфері кібербезпеки Франції є: розбудова кадрового потенціалу та підготовка фахівців у сфері кіберзахисту шляхом впровадження державою модулів із кібербезпеки до освітніх програм вищої освіти, сприяння безперервному професійному розвитку фахівців у сфері кібербезпеки; розвиток інноваційної екосистеми у сфері кіберзахисту, де ключовими платформами для міжсекторальної співпраці є Кіберкампус та Кластер, які об'єднують органи державної влади, заклади освіти, науково-дослідні установи та бізнес з метою стимулювання технологічного розвитку та інновацій.

Попри те, що державно-приватне партнерство у сфері кібербезпеки у Франції є ключовим елементом національної стратегії забезпечення безпеки кіберпростору, на практичному рівні зберігається переважання державних інституцій у сфері кібербезпеки, тоді як участь приватного сектору залишається обмеженою.

Основні напрями державно-приватного партнерства у сфері кібербезпеки у Франції включають: обмін інформацією та оперативне реагування; технологічний розвиток через спільні проєкти між державою та приватними компаніями, зокрема в рамках діяльності Кіберкампусу та Кластера; організацію навчання та підвищення кваліфікації, формування кадрового резерву IT-фахівців. Імплементація Директиви NIS2 розпочалася з етапу підготовки законопроекту про підвищення стійкості критичної інфраструктури та посилення кібербезпеки[61], який було представлено на засіданні Ради міністрів у жовтні 2024 року та подано на розгляд парламенту з метою його ухвалення впродовж наступних місяців[62].

---

[60] Hackathons en France : Guide Complet des Événements Incontournables en 2025. URL: https://appairium.com/fr/blog/hackatons

[61] Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. URL: https://www.legifrance.gouv.fr/contenu/Media/files/autour-de-la-loi/legislatif-et-reglementaire/actualite-legislative/2024/pjl_prmd2412608l_cm_15.10.2024.pdf

[62] Directive NIS 2 - MonEspaceNIS2. URL: https://monespacenis2.cyber.gouv.fr/directive/

Швеція. Досліджувана сфера врегульована такими законами: «Про дані пацієнтів»[63], «Про безпеку»[64], «Про інформаційну безпеку для важливих для суспільства та цифрових послуг»[65], «Про електронні комунікації»[66]. Ухвалена урядом у березні 2025 року Національна стратегія кібербезпеки на 2025–2029 роки закріплює напрями державної політики у сфері кібербезпеки[67] і визначає, що державний та приватний сектори є відповідальними суб'єктами забезпечення кібербезпеки на державному рівні. Таким чином, кожна організація несе відповідальність за захист інформації, мережевих та інформаційних систем, які використовуються для операційної діяльності або надання послуг. Також у положеннях Стратегії окреслено існуючі проблеми забезпечення кібербезпеки, які негативно впливають на стан та ефективність реалізації державно-приватного партнерства, до яких відносяться: низький рівень компетентності та обізнаності з питань кібербезпеки; відсутність належної правової регламентації у питаннях управління ризиками, пов'язаними з кіберзагрозами; недостатній обмін інформацією між державним і приватним секторами, відсутність довіри.

Національним координатором у сфері кібербезпеки визначено Агентство з питань цивільного захисту і надзвичайних ситуацій. Взаємодія з приватним сектором передбачає розробку й використання симуляційних платформ (Cyber Range) задля відпрацювання навичок реагування на кіберзагрози. Відповідно до компетенції та в межах повноважень Національний центр кібербезпеки здійснює такі основні функції: координацію попередження, виявлення та реагування на кіберзагрози та кіберінциденти; слугує національною платформою для співпраці та обміну інформацією між державними і приватними акторами у сфері кібербезпеки[68]. Національна команда реагування на комп'ютерні інциденти Швеції «CERT-SE» надає методичну допомогу і проводить консультування для державного сектору, приватних компаній з питань протидії кіберзагрозам та реагування на кіберінциденти. Кластери й ініціативи, що функціонують у Швеції, роблять значний внесок у розвиток національної екосистеми кібербезпеки. Серед провідних кластерів слід виділити «Cyberly», що діє в межах Наукового парку Лінчепінг. Цей кластер об'єднує організації, які працюють над посиленням цифрової стійкості через спільні проєкти, мережі та робочі групи, сприяючи координації заходів і обміну досвідом[69]. Безпековий технологічний хаб Швеції (Sweden Secure Tech Hub) охоплює шість

[63]Patientdatalag (2008:355). URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355/

[64]Säkerhetsskyddslag (2018:585). URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585/

[65]Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174/

[66] Lag (2022:482) om elektronisk kommunikation. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/

[67]Nationell strategi för cybersäkerhet 2025-2029. URL: https://www.regeringen.se/contentassets/a35c523611834fa1997d1ff5b2297338/nationell-strategi-for-cybersakerhet-20252029-skr.-202425121.pdf

[68] Government sets up a national cybersecurity center. URL: https://techsverige.se/en/2020/12/regeringen-inrattar-ett-nationellt-cybersakerhetscenter/?utm_source=chatgpt.com

[69] Cyberly continues to grow – welcoming Knowit and Stadium. URL: https://swedensecuretechhub.se/news/cyberly-continues-to-grow-welcoming-knowit-and-stadium/

провідних наукових парків і зосереджений на підтримці цифрової трансформації з фокусом на навчання, розвиток і масштабування кібербезпекових рішень для малого та середнього бізнесу[70].

У Швеції регулярно проводяться хакатони, які спрямовані на розвиток інновацій у кібербезпеці, цифровій трансформації та управлінні даними, де учасники опановують нові знання й навички за участю провідних технологічних і телекомунікаційних компаній, відомих стартапів[71]. «Hackaping – 2025» є найбільшим хакатоном, він організований університетом Лінчепінга та приватними компаніями. Таким чином, форми державно-приватного партнерства у сфері кібербезпеки передбачають: обмін інформацією про кіберризики; надання консультаційної підтримки з питань кіберзахисту; підготовка рекомендацій з метою сприяння розвитку цифрової інфраструктури та зміцненню кіберстійкості; спільну розробку технологій кіберзахисту (приватні компанії, наприклад Ericsson, беруть участь у розробці безпечних телекомунікаційних мереж (зокрема 5-G)); реалізацію освітніх ініціатив і тренінгів тощо. Отже, державно-приватне партнерство у сфері кібербезпеки передбачає тісну координацію між органами державної влади, приватними компаніями, навчально-науковими інституціями та громадянським суспільством. Участь держави, зокрема через Національний центр кібербезпеки і національну команду реагування на комп'ютерні інциденти Швеції (CERT-SE) створюють сприятливі умови для системної підтримки компаній приватного сектору в питаннях управління кіберризиками, захисту критичної інфраструктури та підвищення кіберстійкості. Ефективність державно-приватного партнерства певним чином стримують деякі виклики, зокрема дефіцит кваліфікованих кадрів, недостатній рівень довіри під час обміну інформацією. Незважаючи на зазначені проблеми, сервісна модель державно-приватного партнерства у сфері кібербезпеки, яка поєднує державні інституції, приватні компанії та науково-дослідні структури, створює передумови для ефективного реагування на сучасні кіберзагрози і підвищення рівня національної кібербезпеки Швеції.

3. Узагальнення форм та видів здійснення державно-приватного партнерства у сфері кібербезпеки в деяких державах ЄС.

Пріоритети національної політики державно-приватного партнерства у сфері забезпечення кібербезпеки в досліджуваних європейських державах закріплені у спеціальних законодавчих актах, присвячених правовій регламентації та визначенню особливостей кібербезпекової галузі, зокрема з питань: кібербезпеки, захисту персональних даних, електронних комунікацій, захисту критичної інфраструктури тощо. Важливе значення мають схвалені на державному рівні Стратегії кібербезпеки, у положеннях яких питанням державно-приватного партнерства у сфері забезпечення кібербезпеки приділяється значна увага, визначаються засади, передумови й особливості його розвитку, напрями конструктивної співпраці між державою, бізнесом та громадськістю *(Табл. 1)*.

---

[70]Sweden Secure Tech Hub - a national cybersecurity innovation hub. URL: https://www.swedenict.se/sweden_secure_tech_hub/

[71] Welcome To Sweden's Largest AI Hackathon! URL: https://cillers.com/hackathons/google-ai-hackathon-tekniska-museet-2025?utm_source=chatgpt.com

Таблиця 1

Назва держави	**Національний координатор у сфері забезпечення кібербезпеки**	**Національний кластер кібербезпеки**	**Модель державно-приватного партнерства**	**Наявність команди реагування на комп'ютерні надзвичайні події (CERT)**
Естонія	Державне управління інформаційних систем	Естонський кібертехнологічний кластер	Сервісна	+
Нідерланди	Національний центр кібербезпеки	Нідерландський кластер кібербезпеки	Сервісна	+
Німеччина	Федеральне відомство з питань інформаційної безпеки	Кластер кібербезпеки міста Бонн	Сервісна	+
Франція	Національне агентство безпеки інформаційних систем	Кластери: Національний хаб кібербезпеки «Кіберкампус», Кластер передового досвіду в галузі кібертехнологій	Сервісна	+
Швеція	Агентство з питань цивільного захисту та надзвичайних ситуацій	Кластери: Cyberly, Безпековий технологічний хаб Швеції, Національний кібербезпековий вузол	Сервісна	+

У проаналізованих державах функціонує сервісна модель державно-приватного партнерства у сфері забезпечення кібербезпеки, яка має певні особливості і передбачає тісну співпрацю між державними органами та приватними компаніями, де приватний сектор виступає постачальником спеціалізованих послуг, у тому числі й цифрових послуг, технологій або експертиз, а держава, своєю чергою, забезпечує регуляторну підтримку, координацію та фінансування. Сервісна модель демонструє, що держава сприймається не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки. Тобто сервісну модель державно-приватного партнерства можна охарактеризувати як платформу задля динамічної взаємодії між державними

та приватними секторами, які здійснюють спільну реалізацію функцій з метою забезпечення безпеки у кіберпросторі. У рамках цієї моделі держава визначає стратегічні цілі, регуляторні вимоги та здійснює координацію, а приватний сектор, своєю чергою, надає технологічні рішення, інновації та оперативне реагування на будь-які кіберінциденти або кіберзагрози. Ця модель орієнтована на надання конкретних сервісів для підвищення кіберстійкості, захисту критичної інфраструктури та швидкого реагування на кіберзагрози. Створення чіткої моделі побудови взаємодії на кшталт сервісної спрямовано на заміну регуляторного підходу, адаптацію кращих закордонних практик для посилення національної кіберстійкості на загальнодержавному рівні. Приватний сектор надає державі та її органам відповідні сервіси у сфері кіберзахисту. При цьому саме держава визначає критерії, яким мають відповідати ті чи інші послуги. За результатами розгляду сервісної моделі державно-приватного партнерства у кожній досліджуваній державі ЄС визначено, що завдяки їй відбувається чіткий розподіл функціональних повноважень між державою та приватним сектором, оскільки саме уряд визначає мету, завдання, стратегічні цілі такої співпраці, а приватний сектор надає допомогу та сприяння, вирішує технологічні інноваційні завдання, залучає інвестиції, організовує постачання певних сервісів і цифрових послуг для державних органів.

Особливостями сервісної моделі державно-приватного партнерства *(Табл. 2)* є: 1) економічна ефективність, що означає діяльність держави з метою оптимізації витрат шляхом залучення приватних компаній замість створення власних коштовних систем чи підготовки кадрів «з нуля»; 2) фокус на критичну інфраструктуру, що передбачає, що в рамках сервісної моделі приватні компанії надають послуги захисту об’єктів критичної інфраструктури (енергетика, фінанси, транспорт), що є пріоритетом для держави; 3) швидке впровадження сучасних технологій, у тому числі й пілотних проєктів, що означає, що приватний сектор має доступ до передових технологій, таких як штучний інтелект, блокчейн, це дозволяє оперативно впроваджувати сучасні рішення; 4) стимулювання приватного сектору з боку держави означає, що означає, що остання надає податкові пільги чи гранти для приватних компаній, які беруть участь або залучені до механізмів державно-приватного партнерства.

Таблиця 2

Сервісна модель державно-приватного партнерства у сфері кібербезпеки

№	Складові компоненти	Зміст
1.	**Повноваження**	Держава визначає стратегічні цілі, регуляторні вимоги та координує діяльність. Приватний сектор надає технологічні рішення, експертизу, інновації та оперативне реагування.
2.	**Цілі та завдання**	Модель зосереджена на наданні конкретних сервісів, таких як моніторинг кіберзагроз, реагування на інциденти, аудит кібербезпеки, навчання персоналу.
3.	**Контрактна основа**	Укладаються договори, які чітко визначають обсяг послуг, строки, відповідальність сторін та механізми оцінки ефективності.

4.	**Гнучкість та адаптивність**	Модель дозволяє швидко адаптуватися до нових кіберзагроз завдяки залученню інноваційних рішень приватного сектору.
5.	**Обмін інформацією**	Забезпечується оперативний обмін даними про кіберзагрози між державою та приватними партнерами для швидкого реагування.
6.	**Фокус на спеціалізацію**	Приватні компанії надають високоспеціалізовані послуги (наприклад, захист хмарних систем, аналіз ШІ-базованих загроз), які держава самостійно не може ефективно реалізувати.

Типовою рисою державно-приватного партнерства у сфері кібербезпеки в провідних європейських державах – Німеччині, Естонії, Нідерландах, Франції та Швеції – є визначення на законодавчому рівні Національного координатора у сфері забезпечення кібербезпеки. Так, наприклад, у Німеччині – це Федеральне відомство з питань інформаційної безпеки, в Естонії – Державне управління інформаційних систем, яке контролює міністр юстиції та безпеки, у Нідерландах – Національний центр кібербезпеки, у Франції – Національне агентство безпеки інформаційних систем, у Швеції – Агентство з питань цивільного захисту та надзвичайних ситуацій. Національний координатор у межах компетенції та відповідно до функціональності визначає формат такої співпраці: на добровільних засадах або в обов'язковому (імперативному) порядку. Як демонструє позитивний закордонний досвід, державно-приватне партнерство у сфері кібербезпеки передбачає такі форми налагодження взаємодії: побудова конструктивного діалогу та визначення шляхів співпраці; формування довіри між приватним сектором і державними інституціями; заохочення співпраці між державними й приватними організаціями на всіх етапах дослідницького та інноваційного процесу тощо.

Повноваження та компетенція цих структур у сфері державно-приватного партнерства, як правило, є тотожними і передбачають: забезпечення виконання функції координації в питаннях кібербезпеки на національному рівні, забезпечення надійного кіберзахисту критичної інфраструктури, підвищення обізнаності суспільства та громадськості щодо кіберзагроз; об'єднання тактичних й оперативних знань, умінь та навичок із метою налагодження співпраці державного та приватного секторів; сприяння у питаннях взаємодії постачальників цифрових послуг і уряду; налагодження спільного інформування постачальників цифрових послуг та держави з питань кіберзагроз та кіберінцидентів для мережевих й інформаційних систем; проведення аналізу і технічних досліджень кіберзагроз і кіберінцидентів або ознак їх виникнення; сприяння обміну інформацією між державою, уповноваженими підприємствами і організаціями, громадськістю про кіберзагрози та кіберінциденти, шляхи посилення кіберстійкості. Під егідою Національного координатора у сфері забезпечення кібербезпеки створюються національні команди реагування на комп'ютерні інциденти (CERT), які сприяють взаємодії між державним та приватним секторами, координують їх спільні дії.

Також у вказаних державах спільною рисою є створення й функціонування Національного кластера кібербезпеки – координаційної платформи, яка об'єднує

ресурси, можливості, спроможності та компетенції державних органів, урядових організацій, представників приватного сектору. Основним завданням Національного кластера кібербезпеки є підвищення рівня стратегічного потенціалу національної кібербезпеки, розвиток професійної кіберспільноти та забезпечення безпечного кіберпростору в контексті розбудови державно-приватного партнерства. Діяльність Національного кластера кібербезпеки спрямована на зміцнення спроможностей, сталий розвиток сектору національної кібербезпеки та організацію регулярних подій: координаційних зустрічей, обговорень, форумів, самітів, освітніх науково-практичних заходів, зокрема конференцій тощо. Національний кластер кібербезпеки сприяє ефективному втіленню довгострокових цілей та реалізації стратегічних напрямів розвитку системи національної кібербезпеки, координує, надає підтримку та експертизу для виконання актуальних завдань, у тому числі й через механізми державно-приватного партнерства. Останнім часом на теренах ЄС набуває поширення тенденція активної участі представників приватного сектору та громадськості в засіданнях урядових робочих груп під час розробки законодавчих норм у сфері забезпечення кібербезпеки, підготовки стратегічних документів у цій галузі, при цьому особлива увага приділяється розвитку культури кібербезпеки та поширенню знань громадськості та спільноти про безпечну поведінку в цифровому просторі.

Більш досконалий механізм державно-приватного партнерства у сфері кібербезпеки демонструють Німеччина та Естонія. Ці держави ЄС мають низку спільних рис, які свідчать про комплексний підхід до налагодження та розбудови співпраці між державним і приватним секторами з урахуванням сучасних тенденцій загальнодержавного технологічного розвитку, передових технологій і залучення інновацій у цій галузі. Спільними ознаками для цих європейських держав є концентрація уваги державної політики у сфері державно-приватного партнерства саме на необхідності посилення кіберзахисту критичної інфраструктури (енергетика, транспорт, фінанси, телекомунікації). У Німеччині це реалізується через таку ініціативу, як Альянс для кібербезпеки (Allianz für Cybersicherheit), який координується Федеральним відомством з інформаційної безпеки та об'єднує державні органи і приватні компанії для захисту критичної інфраструктури (KRITIS). Ця платформа поєднує бізнес, державу і науковців для обміну інформацією та розробки стандартів у сфері кібербезпеки.

Своєю чергою, в Естонії державно-приватне партнерство зосереджено на необхідності захисту цифрових сервісів, таких як e-Governance, на основі співпраці з приватними IT-компаніями, які надають послуги та сервіси для державних платформ. Естонія використовує такі платформи, як Cyber Security Council та CERT-EE (Computer Emergency Response Team Estonia), де приватні компанії беруть участь у реагуванні на кіберінциденти та в розробці технологій.

Обидві держави мають Центри реагування на кіберінциденти (CERT), які діють як зв'язуюча ланка між державою та бізнесом. Також у Німеччині та Естонії активно розвивається оперативний обмін даними про кіберзагрози між державними органами та приватним сектором. У Німеччині це відбувається через платформи, створені Федеральним відомством з інформаційної безпеки, які забезпечують швидке

інформування про нові реальні й потенційні кіберзагрози. В Естонії, завдяки високому рівню цифровізації, обмін інформацією є ключовим елементом державно-приватного партнерства, зокрема через співпрацю з приватними ІТ-компаніями, які надають аналітику та інструменти для моніторингу кіберпростору. Обидві держави використовують сервісну модель державно-приватного партнерства, де приватний сектор надає спеціалізовані послуги, такі як моніторинг, аналіз кіберзагроз, розробка ліцензованого програмного забезпечення, послуги з аудиту кібербезпеки. У Німеччині технологічні приватні компанії («Siemens», «SAP») надають технологічні рішення для забезпечення державних потреб.

В Естонії приватні компанії («Cybernetica» та «Nortal») беруть участь у розробці й підтримці державних цифрових сервісів, зокрема системи електронного голосування, здійснюють розробку і впровадження стандартів ІТ-безпеки, вимог щодо конфіденційності, проводять аудит кібербезпеки, аналізують ризики складних криптографічних, цифрових або фізичних систем, включаючи їх економічні та соціальні аспекти, здійснюють комплексні прикладні дослідження щодо застосування машинного навчання, забезпечення квантової безпеки тощо.

Як Німеччина, так і Естонія активно залучають приватний сектор до організації навчання фахівців із кібербезпеки. У Німеччині це реалізується через спільні програми за участю університетів та бізнес-структур, а також через започатковані ініціативи Альянсу для кібербезпеки. В Естонії приватні компанії співпрацюють із державою для створення навчальних програм, зокрема за участю Талліннського технічного університету, де проводяться тренінги з кіберзахисту для всіх бажаючих із залученням академічної спільноти та фахівців-практиків.

Як Німеччина, так і Естонія демонструють підхід, який пов’язаний з активним залученням стартапів через державні гранти та програми співпраці з великими ІТ-корпораціями. У Німеччині активно підтримуються стартапи у сфері кібербезпеки через державні гранти та програми співпраці з великими корпораціями. Естонія, відома своєю стартап-екосистемою, залучає інноваційні компанії до розробки технологічних рішень для кібербезпеки, що сприяє швидкому впровадженню нових технологій. Основою державно-приватного партнерства у сфері кібербезпеки є взаємна довіра, адже Естонія має більш тісні зв’язки між державою та бізнесом, що пов’язано з масштабною цифровізацією на загальнодержавному рівні, це дозволяє створювати інноваційні рішення, швидко реагувати на загрози та зміцнювати міжнародну позицію держави у сфері кібербезпеки. Таким чином, Німеччина та Естонія демонструють однаковий виважений підхід у питаннях державно-приватного партнерства у сфері кібербезпеки, який ґрунтується на необхідності координації і консолідації зусиль та спроможностей на захисті критичної інфраструктури, створенні платформ для співпраці, оперативному обміні інформацією, освітніх ініціативах та відповідності стандартам ЄС.

У Німеччині та Естонії кіберспільнота підтримує формат державно-приватного партнерства на основі взаємної довіри, що забезпечується реалізацією спільних заходів, постійною комунікацією переважно на імперативних засадах. Конфігурація співпраці в рамках державно-приватного партнерства у сфері кібербезпеки включає

обмін думками та позиціями, тематичне обговорення під час проведення науково-практичних заходів, зокрема конференцій, симпозиумів, семінарів тощо.

Таким чином, найбільш розвинене державно-приватне партнерство у сфері кібербезпеки спостерігається у таких державах ЄС, як Німеччина та Естонія, завдяки ефективному законодавству, розвиненому технологічному сектору та активним платформам співпраці. Спільним недоліком є тривалий процес та зволікання щодо імплементації Директиви NIS2, яка вимагає удосконалення співпраці між державою та приватним сектором у сфері забезпечення кібербезпеки з метою гармонізації стандартів і процедур ЄС у національне законодавство. Ці європейські держави демонструють ефективну інтеграцію потужностей та ресурсів держави й приватного сектору, що може бути корисним прикладом для України при розробці власної моделі державно-приватного партнерства.

У решті проаналізованих держав ЄС прискіплива увага приділяється захисту об'єктів критичної інфраструктури (енергетика, транспорт, фінанси, телекомунікації, охорона здоров'я), що є пріоритетом державно-приватного партнерства. У Нідерландах Національний центр кібербезпеки активно співпрацює з приватними компаніями для захисту критичних секторів, особливо щодо портів Роттердама, національних банківських та фінансових установ. У Швеції Агентство з питань цивільного захисту та надзвичайних ситуацій координує захист критичної інфраструктури через співпрацю з приватними операторами. У Франції Агентство з питань кібербезпеки співпрацює з приватним сектором для забезпечення безпеки стратегічних галузей, зокрема енергетики та авіації. У вказаних державах ЄС державно-приватне партнерство базується на сервісній моделі, де приватний сектор надає спеціалізовані послуги, такі як моніторинг кіберзагроз, аудит кібербезпеки, розробка ліцензованого програмного забезпечення, спільне реагування на кіберінциденти. Так, у Нідерландах великі ІТ-компанії (такі як «Philips», «KPN») спрямовують власні технологічні рішення для захисту державних систем, а у Швеції приватні компанії (як-от «Ericsson») беруть участь у розробці безпечних телекомунікаційних мереж, зокрема 5-G. У Франції приватні компанії (такі як «Thales» чи «Orange Cyberdefense») надають послуги сервісного обслуговування у сфері кіберзахисту для державних підприємств критичної інфраструктури.

У Нідерландах, Швеції та Франції активно залучають приватний сектор до освітніх програм і тренінгів із кібербезпеки: проводять спільні ініціативи з університетами та приватними компаніями для підготовки фахівців у сфері кіберзахисту; співпрацюють з приватними компаніями для створення симуляційних платформ (Cyber Range) з метою організації та проведення кібертренувань; підтримують програми підвищення кваліфікації через комплексну співпрацю з приватними компаніями та академічними навчальними закладами.

Важливим аспектом розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки у цих державах ЄС є залучення інновацій та стартапів. Так, наприклад, у Нідерландах діють програми, які об'єднують стартапи, великі компанії та уряд. У Швеції стартапи у сфері кібербезпеки отримують підтримку через державні гранти та співпрацю з Агентством з питань цивільного захисту і надзвичайних

ситуацій. У Франції такі ініціативи, як «Campus Cyber», сприяють інтеграції стартапів і великих компаній для розробки новітніх технологічних рішень.

Особливості, пов'язані з державно-приватним партнерством у сфері забезпечення кібербезпеки, включають: формат прозорості й довіри; гнучкість реагування на кіберзагрози та кіберінциденти; фокус на превентивність заходів посилення кібербезпеки. Так, зокрема, Нідерланди, Швеція та Франція прагнуть будувати державно-приватне партнерство на основі взаємної довіри, що забезпечується прозорими процедурами та регулярною комунікацією переважно на добровільних засадах, використовують інститут державно-приватного партнерства з метою адаптації до нових кіберзагроз, таких як кібератаки на ланцюги постачання чи гібридні кіберзагрози. Усі ці держави ЄС наголошують на необхідності проактивних заходів, таких як проведення регулярних незалежних аудитів стану кібербезпеки з метою виявлення вразливостей, спільне моделювання кіберзагроз, аналіз кіберінцидентів тощо.

Фінансово-економічні аспекти розбудови державно-приватного партнерства передбачають залучення інвестицій, які, своєю чергою, спрямовуються на впровадження пілотних менторських програм підвищення кваліфікації фахівців державних органів, які виконують функції із забезпечення кібербезпеки та кіберзахисту, шляхом залучення сертифікованих за міжнародними стандартами фахівців приватного сектору, у тому числі й дослідницьких програм; розробку вітчизняних програмних продуктів, зокрема ліцензованого програмного забезпечення з відкритим кодом, які використовуються з метою обробки та захисту державних інформаційних ресурсів, а також на об'єктах критичної інформаційної інфраструктури; розробку дієвого алгоритму посилення кіберзахисту тощо.

На підставі проведеного аналізу перспективними заходами у сфері посилення кібербезпеки в контексті розбудови державно-приватного партнерства вбачаються: залучення стартапів, представників академічної та наукової спільноти в якості фахівців для проведення навчання, виконання комп'ютерно-технічних та інших видів спеціальних комплексних експертиз; залучення представників експертного й наукового середовища, громадських об'єднань до дискусій та обговорення проблематики, спільне розроблення нормативно-правових актів, нормативних документів і стандартів у сфері забезпечення кібербезпеки; сприяння співпраці з приватними організаціями для підвищення стійкості критичної інфраструктури; спільний моніторинг та аналіз стану кіберпростору з метою виявлення і запобігання кіберзагрозам на ранніх стадіях, їх попередження; підготовка галузевих спеціалістів і фахівців, розробка та сприяння реалізації освітніх онлайн-платформ тощо. 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 і гарантуючи надійний кіберзахист критичної інфраструктури. Таким чином, приватний сектор глибоко інтегрований у різні аспекти національної кібербезпеки, активно залучається тією чи іншою державою ЄС для боротьби з кібератаками, підтримання кіберстійкості та кіберзахисту критичної інфраструктури.

Для всіх проаналізованих держав ЄС загрозливою тенденцією та викликом для успішної реалізації державно-приватного партнерства є нестача кваліфікованих кадрів у сфері кібербезпеки, а надмірна залежність від приватних компаній може створювати певні вразливості для державних органів, провокувати ризики витоку конфіденційної інформації. Окрім того, недоліками співпраці в рамках державно-приватного партнерства визначено проблеми побудови довірчих відносин, також брак або відсутність у більшості приватних компаній належних підходів до управління кіберінцидентами значно підвищує уразливість ІТ-систем, які перебувають у розпорядженні приватного сектору, непоодинокі випадки недостатнього обміну інформацією між державним і приватним секторами. Також проблемним аспектом у сфері державно-приватного партнерства для всіх проаналізованих європейських держав залишаються повільні темпи імплементації Директиви NIS2 у національне законодавство, обмеженість фінансових ресурсів, певна бюрократизація процесів побудови співпраці, недостатнє закріплення чітких юридичних форм взаємодії на законодавчому рівні.

ІІІ. Висновки

У проаналізованих європейських державах (Німеччина, Естонія, Нідерланди, Франція, Швеція) функціонують розвинені механізми державно-приватного партнерства у сфері кібербезпеки, засновані на сервісній моделі, що включає створення платформ, альянсів та ініціатив, з урахуванням національних особливостей інституційно-правового забезпечення такої співпраці. Європейський досвід у рамках національних юрисдикцій вказаних держав демонструє успішні приклади об’єднання технічних та людських ресурсів, спроможностей і потужностей держави й бізнесу з метою захисту критичної інфраструктури, посилення кіберзахисту та забезпечення кібербезпеки на загальнодержавному рівні.

Державно-приватне партнерство передбачає комплексну взаємодію та співпрацю між державними органами і приватним сектором для вирішення суспільно важливих завдань, зокрема забезпечення посиленого кіберзахисту критичної інфраструктури та її об’єктів, обміну інформацією, реагування на кіберінциденти, розробки стандартів, навчання кадрів та впровадження сучасних технологічних рішень. У рамках державно-приватного партнерства приватні компанії надають високоспеціалізовані послуги та сервіси, які держава самостійно не може ефективно реалізувати без зайвих фінансових витрат. Значна роль відводиться регулярним освітнім заходам за участю представників приватного сектору.

Для України досвід держав ЄС, зокрема Естонії та Німеччини, може бути цінним у справі створення власної моделі державно-приватного партнерства у сфері забезпечення кібербезпеки. Пропозиції удосконалення державно-приватного партнерства у сфері забезпечення кібербезпеки мають передбачати: розробку законодавчих основ такої співпраці, підготовку та надання урядом України рекомендацій для приватного сектору за наслідками виявлення та відстеження кіберінцидентів у кіберпросторі; проведення науково-практичних заходів (конференцій, хакатонів, самітів), спрямованих на спільне вивчення й опанування сучасним досвідом протидії та запобігання кібератакам і кіберзагрозам з урахуванням динамічної зміни їх ландшафту; впровадження кращого досвіду політики ЄС

«Government Relations», що дозволяє ефективно протистояти кіберзагрозам і просувати цифрову кіберстійкість; розвиток Національного кластера кібербезпеки.

Важливим кроком на шляху реалізації євроінтеграційних прагнень України є імплементація Директиви NIS2 у національне законодавство та створення власної моделі державно-приватного партнерства.

Дослідницька служба
Верховної Ради України