УДК / UDC: 351.746:004.056:334.72
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364487

Сергій Анатолійович Красніков
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України
Київ, Україна
ORCID: https://orcid.org/0000-0001-6548-5457

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ДОСВІД ЕСТОНІЇ

Анотація. *Визначено завдання та напрями державно-приватного партнерства у сфері забезпечення кібербезпеки. Узагальнено законодавство Естонії, присвячене питанням розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки. Висвітлено концепти державної кібербезпекової політики Естонії. Визначено особливості та форми державно-приватного партнерства у сфері забезпечення кібербезпеки в Естонії. Розглянуто засади діяльності естонського кібертехнологічного кластеру, визначено проблемні питання забезпечення кадрового потенціалу фахівців у сфері кібербезпеки. Деталізовано механізми фінансування державно-приватного партнерства у сфері забезпечення кібербезпеки. Акцентовано, що успіх Естонії у питаннях розбудови державно-приватного партнерства заснований на залученні провідних технологічних компаній до цих процесів. Окреслено роль та значення міжнародних кібернавчань, які проводяться в Естонії під егідою Об'єднаного центру передових технологій з кібероборони НАТО. Визначено засади стратегічного партнерства між Естонією та Україною у сфері забезпечення кібербезпеки в контексті консолідації зусиль державного та приватного секторів. Визначено подальші шляхи удосконалення чинного законодавства у сфері співпраці між державою та приватним сектором з урахуванням кращих практик естонського досвіду у цій площині.*

Ключові слова: *державно-приватне партнерство, кіберзагроза, кіберінцидент, кіберризик, кіберзахист, кіберстійкість, кіберпростір, кібердомен, цифрові технології, приватний сектор, кібербезпека.*

Serhii A. Krasnikov
Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0001-6548-5457

PUBLIC-PRIVATE PARTNERSHIP IN CYBERSECURITY: ESTONIAN EXPERIENCE

Summary*. The tasks and directions of public-private partnership in the field of cybersecurity are determined. The legislation of Estonia devoted to the development of public-private partnership in the field of cybersecurity is summarized. The concepts of the state cybersecurity policy of Estonia are highlighted. The features and forms of public-private partnership in the field of cybersecurity in Estonia are determined. The principles of the Estonian cyber-technology cluster are considered, and the problematic issues of ensuring the human resource potential of specialists in the field of cybersecurity are identified. The mechanisms of financing public-private partnership in the field of*

© Красніков С.А. 2026

cybersecurity are detailed. It is emphasized that Estonia's success in the development of public-private partnership is based on the involvement of leading technology companies in these processes. The role and significance of international cyber exercises held in Estonia under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence are outlined. The principles of strategic partnership between Estonia and Ukraine in the field of cybersecurity in the context of consolidating the efforts of the public and private sectors have been defined. Further ways of improving the current legislation in the areas of strengthening cooperation between the state and the private sector as an important component of public-private partnership, taking into account the best practices of Estonian experience in this area, have been identified.

Keywords: *public-private partnership, cyber threat, cyber incident, cyber risk, cyber defense, cyber resilience, cyberspace, cyber domain, digital technologies, private sector, cybersecurity.*

Постановка проблеми. Кібербезпека була і залишається одним із ключових напрямів державної політики у сфері забезпечення національної безпеки. Адже у розвинених країнах світу застосування державно-приватного партнерства у сфері кібербезпеки є поширеною практикою, для чого створюються відповідні правові засади та належне інституційне забезпечення [1, с.48].

Україна, відчуваючи безпрецедентний тиск потужних кібератак, масштабування та збільшення чисельності кіберзагроз, переймається питаннями посилення кіберзахисту державних інформаційних ресурсів та об’єктів критичної інфраструктури. В умовах швидкого й динамічного розвитку цифрових 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. Це вимагає налагодження ефективної та комплексної співпраці між державою й приватним сектором, включаючи створення сучасної правової бази, підготовку експертів і фахівців, які зможуть протистояти будь-яким кіберзагрозам у сучасному кібердомені. Державно-приватне партнерство залишається одним із основних напрямів організації діяльності із забезпечення кібербезпеки як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. На фоні динамічного розвитку ландшафту кібербезпеки виникають нові кіберзагрози, які порушують надання критично важливих послуг, ставлять під загрозу конфіденційні дані та підривають довіру до державного та приватного секторів. Фактично, дослідження показують, що дефіцит навичок у сфері кібербезпеки створює додаткові кіберризики для 70% організацій [2].

Кібербезпека стала невід’ємною частиною бізнес-стратегії, визначаючи здатність організацій захищати свої цифрові активи та продовжувати діяльність навіть у кризових ситуаціях. Вирішуючи відповідні масштабні стратегічні завдання, держава відчуває потребу в залученні 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.

З метою забезпечення стримування агресивних дій у кіберпросторі проти України наша держава намагається посилити кібербезпеку в умовах правового режиму воєнного стану за рахунок технологічних, економічних, дипломатичних, розвідувальних заходів. Проте з огляду на обмежені ресурси держави, ефективне реагування на кіберзагрози потребує системного залучення потенціалу приватного сектору. В умовах воєнного стану, запровадженого у зв’язку з російською збройною агресією проти України,

кіберпростір перетворився на ключову площину сучасної війни. Масштабні кібератаки на критичну інфраструктуру вимагають залучення висококваліфікованих спеціалістів, зокрема й поза межами державного сектору, для спільного реагування на загрози та мінімізації їхніх наслідків, що зумовлює необхідність правового врегулювання такої взаємодії.

Підготовка відповідної законодавчої бази з питань розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки потребує адаптації до вимог актів ЄС, що підкреслює важливе значення інституцій громадянського суспільства та приватного сектору у питаннях забезпечення кібербезпеки. Основним нормативно-правовим актом ЄС, що визначає загальні засади здійснення державно-приватного партнерства у сфері кібербезпеки, є Директива (ЄС) 2022/2555 (NIS2) [3]. Зокрема, відповідно до пункту 55 цієї Директиви, державно-приватне партнерство у сфері кібербезпеки має забезпечити належну основу для обміну знаннями, передовим досвідом та встановлення спільного рівня розуміння між зацікавленими сторонами. Держави-члени ЄС на виконання її положень повинні сприяти реалізації політиці, яка є основою для створення й розвитку державно-приватного партнерства у сфері забезпечення кібербезпеки. У рамках державно-приватного партнерства держава може використовувати досвід приватних структур задля допомоги компетентним органам у розробці найсучасніших послуг та процесів, включаючи обмін інформацією, раннє попередження, навчання щодо кіберзагроз та кіберінцидентів, управління ризиками та планування кіберстійкості.

За таких умов, в контексті окресленої наукової проблеми для держави актуальними питаннями залишаються: створення ефективних організаційно-правових механізмів залучення представників приватного сектору до протидії деструктивній діяльності в кіберпросторі; налагодження паритетної взаємодії між державними органами, бізнесом і громадськістю у сфері кібербезпеки; підвищення рівня кіберстійкості на національному рівні завдяки консолідації зусиль держави та представників приватного сектору; зміцнення довіри між усіма учасниками шляхом підвищення прозорості та спільної відповідальності у питаннях забезпечення кібербезпеки; формування субкультури цифрової безпеки в суспільстві, що охоплює громадян, бізнес та державні інституції. З метою удосконалення вітчизняної моделі державно-приватного партнерства у сфері забезпечення кібербезпеки, доцільно висвітлити досвід деяких держав Європейського Союзу, зокрема Естонії – країні, де розшатований та функціонує Об'єднаний центр передових технологій з кібероборони НАТО [4].

Результати аналізу наукових публікацій. Державно-приватне партнерство у сфері забезпечення кібербезпеки та його розбудова перебували у фокусі уваги як вітчизняних, так і іноземних науковців. Кращі практики загальноєвропейського досвіду розбудови механізмів здійснення державно-приватного партнерства у сфері забезпечення кібербезпеки досліджували: В. Бойко [5], В. Григоренко [6], Г. Малахов [7], В. Матвієнко та Г. Петушкова [8], О. Поляков [9], К. Хоєцька [10]. Проте жоден із вказаних фахівців не здійснював огляд кращих практик європейського досвіду у сфері законодавчого забезпечення державно-приватного партнерства у сфері кібербезпеки на прикладі Естонії, яка є надійним та стратегічним партнером України у сфері кібербезпеки та цифрового розвитку, що посилює актуальність обраного наукового напряму.

Метою статті є узагальнення законодавчого забезпечення механізму державно-приватного партнерства у сфері забезпечення кібербезпеки в Естонії, визначення на підставі аналізу кращих практик естонського досвіду напрямків подальшого

удосконалення організаційно-правових засад розвитку державно-приватного партнерства у сфері забезпечення кібербезпеки України.

Виклад основного матеріалу. Геополітична ситуація підвищила рівень кіберзагроз для Естонії та всього західного світу, що вимагає консолідації зусиль з метою посилення кібербезпеки та її складових. Загалом сфера забезпечення кібербезпеки регулюється в Естонії такими законодавчими актами: про кібербезпеку [11], про захист персональних даних [12], про електронні комунікації [13]. У 2024 році була схвалена оновлена Стратегія кібербезпеки Естонії на 2024-2030 роки [14], пріоритетним завданням якої визначено прискорення імплементації у національне законодавство директив та регламентів ЄС і НАТО, побудова паритетного балансу інтересів між державою та приватним сектором, дотримання свободи цифрового підприємництва, вимог та стандартів у сфері кібербезпеки. Ключова увага стратегії приділяється зміцненню системи кібербезпеки Естонії у відповідь на глобальні загрози, що розвиваються, особливо в контексті зростання транснаціональної кіберзлочинності, геополітичного суперництва та 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 [15].

Естонія вважається одним із світових лідерів у сфері кібербезпеки, володіє високорозвинутою цифровою екосистемою саме завдяки гнучкій моделі державно-приватного партнерства, яка поєднує державні ресурси, приватні інновації та волонтерську діяльність. Естонія залишається європейським лідером у сфері технології блокчейн (KSI Blockchain) [16] і стала першою країною світу, яка використала блокчейн на державному рівні для забезпечення цілісності державних реєстрів та медичних метаданих. Естонія, як одна з найбільш цифровізованих країн світу, активно та ефективно залучає приватний сектор до співпраці з урядом, що дозволяє створювати інноваційні технологічні рішення, швидко реагувати на кіберзагрози та зміцнювати міжнародну позицію країни у сфері кібербезпеки. В Естонії цифрові рішення широко використовуються як у державному, так і в приватному секторах, а державно-приватне партнерство у сфері забезпечення кібербезпеки включає: розробку та надання рекомендацій для приватного сектору за наслідками виявлення та відстеження кіберінцидентів у кіберпросторі; проведення заходів, спрямованих на спільне вивчення та опанування здобутого сучасного позитивного досвіду запобігання кібератакам й 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 усіх рівнях.

Державно-приватне партнерство в Естонії є зразковим прикладом ефективної співпраці у сфері кібербезпеки, що базується на взаємній довірі, налагодженому обміну інформацією, спільних інноваційних рішеннях. Естонія є першою 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. Естонія, яка відома як “цифрова держава”, активно використовує концепцію “GR” для розвитку кібербезпеки, залучає міжнародних партнерів, здійснює просування своїх ініціатив на глобальному рівні.

Основним координатором у сфері державно-приватного партнерства у сфері забезпечення кібербезпеки Естонії визначено Національний центр кібербезпеки, який

функціонує з 2023 року [17]. Особливістю державно-приватного партнерства у сфері забезпечення кібербезпеки Естонії є активне залучення приватного сектору до розробки засад кібербезпекової політики на базі технологій штучного інтелекту. Так, Уряд Естонії співпрацює з приватними технологічними компаніями, ІТ-компаніями, такими як Guardtime" та "CybExer Technologies" з 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, у свою чергу, використовуються державними установами для тестування кіберстійкості об'єктів критичної інфраструктури. Приватні ІТ-компанії, на кшталт "CybExer Technologies", співпрацюють з державою з метою організації тренінгів для державних службовців та працівників критичної інфраструктури. Крім цього, Уряд Естонії створив платформи для оперативного обміну даними про кіберзагрози між державою та приватним сектором.

Наприклад, створена у 2006 році команда CERT-EE (Computer Emergency Response Team Estonia) [18] є відповідальною за управління інцидентами безпеки в комп'ютерних мережах домену "ee", одночасно є національним контактним пунктом у сфері міжнародного співробітництва в галузі ІТ-безпеки. Вона взаємодіє з національними телекомунікаційними компаніями, банківськими установами та ІТ-компаніями з метою раннього попередження, виявлення та реагування на будь-які кіберінциденти. Механізми розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки в Естонії спрямовані на створення висококібертехнологічного кластеру з метою обміну знаннями та навичками між державним та приватним секторами, зміст яких 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 [19]. Так, на постійній основі діяльність кібертехнологічного кластеру спрямована на підвищення компетенції та обізнаності у сфері кібербезпеки на всіх рівнях і сферах ІТ-середовища з метою пропагування необхідності забезпечення захисту інформаційних ресурсів від потенційних або реальних кіберзагроз. Надається методична допомога не лише суб'єктам господарювання у цій сфері, але й уповноваженим державним органам. Естонський кібертехнологічний кластер має на меті вирішити проблему нестачі фахівців з кібербезпеки шляхом розвитку ефективної та спільної мережі інкубаторів щодо опанування навичок кібербезпеки за участю усіх зацікавлених сторін. До пріоритетних завдань кібертехнологічного кластеру Естонії у рамках розбудови державно-приватного партнерства у сфері кібербезпеки відносяться: підвищення освітніх стандартів у сфері кібербезпеки; впровадження інновацій (сучасної методології та процедур виявлення загроз); побудова конструктивного діалогу та співпраці між державним та приватним секторами критичної інфраструктури; активізація процесу структурного розвитку архітектури та систем кібербезпеки; побудова найвищого ступеня довіри між державою та приватним сектором; активна взаємодія між учасниками кластера, бізнес-середовищем, представниками держави та академічною спільнотою; формування та розвиток професійного кадрового потенціалу у сфері кібербезпеки;

розвиток субкультури кібербезпеки, поширення знань про безпечну поведінку в цифровому просторі тощо.

Таким чином, Естонський кібертехнологічний кластер — платформа, яка об'єднує представників державного та приватного секторів, академічної спільноти, представників громадянського суспільства з метою посилення стану забезпечення кібербезпеки. Одночасно кібертехнологічний кластер має на меті сприяння розвитку національної кіберстійкості, впровадженню інноваційних рішень і технологій захисту інформації, адаптації національних стандартів до міжнародних практик, розвитку людського капіталу у сфері кібербезпеки, підтримку кіберзахисту критичної інфраструктури та налагодженню ефективної співпраці між ключовими стейкхолдерами, підвищення довіри між ними. Під егідою кібертехнологічного кластеру здійснюється розробка та практична реалізація заходів, спрямованих на посилення стану кібербезпеки, включаючи проведення, починаючи з 2022 року, щорічних національних конференцій з питань кібербезпеки, що є ще однією площадкою для дискусійних обговорень за участю державного та приватного сектору, представників академічної та експертної кіберспільноти тематичної проблематики. Метою таких науково-практичних заходів є обмін думками, вироблення єдиного підходу, посилення кооперації та співпраці у кібербезпекових питаннях, пошук оптимальних шляхів та розробка механізмів щодо реагування на сучасні та майбутні кіберзагрози, створення середовища, яке підтримує обмін знаннями та набутим досвідом [20].

У оприлюдненому звіті "CyberHubs", який присвячений Естонії [21], підкреслюється, що ця держава зазнала значних змін у своєму ландшафті кібербезпеки, що пов'язано із зростаючою чисельністю кіберзагроз та масштабуванням російської агресії у кіберпросторі. Це вимагає посилення ініціатив, спрямованих на розбудову державно-приватного партнерства, включаючи посилення співпраці між урядом, навчальними закладами та приватним сектором, залучення цілеспрямованих інвестицій. Прогнозується, що попит Естонії на ІТ-фахівців зросте в 1,5 рази до 2027 року, що потребуватиме приблизно 2600 нових ІКТ-фахівців щорічно. При цьому посади у сфері кібербезпеки становитимуть 8–10% цієї потреби. Цей попит на кваліфікованих працівників у таких сферах, як управління кіберризиками, захист даних та реагування на кіберінциденти, перевищує поточні та прогнозовані показники підготовки фахівців, що призводить до суттєвої нестачі кваліфікованих кадрів. Щоб усунути цю прогалину, Естонія прагне покращити стан забезпечення кібербезпеки шляхом організації та проведення освітніх заходів та навчання, залучення до цих процесів багатопрофільних фахівців з приватного сектора, підвищити обізнаність громадськості про кіберзагрози, посилити захист бізнесу. Оскільки в Естонії не вистачає експертів у галузі кібербезпеки, створюються передумови задля залучення до цього сегменту представників приватного сектору, а покращення національних спроможностей у цій площині вимагає організації їхнього професійного навчання. Зростаюча залежність від цифрових систем у різних секторах економіки призводить до появи шаленого попиту на експертів у питаннях кібербезпеки як у державному, так і приватному секторах. Водночас, динамічний характер кіберзагроз означає, що фахівцям з кібербезпеки необхідно постійно оновлювати свої знання, практичні навички та вміння. Новітні технології, такі як штучний інтелект, квантові технології, блокчейн та хмарні обчислення, інтегруються в стратегії кібербезпеки. На цьому фоні як держава, так і приватний сектор стикаються із браком досвідченої робочої сили, яка має достатні знання у питаннях забезпечення ІТ-безпеки.

Як на національному, так і на рівні ЄС, фахівці з кібербезпеки повинні дотримуватися Кодексу етнічного поведінки у кіберпросторі [22], бути кваліфікованими, виконувати технічні та організаційно-правові вимоги у межах своїх службових повноважень. Щоб зберегти своє лідерство у сфері кібербезпеки, Естонія продовжує інвестувати в освіту та інновації, сприяючи консолідованій співпраці між урядом та бізнесом з метою розвитку кадрового потенціалу, здатного протистояти складним кіберзагрозам. Спільний підхід включає діяльність уряду, приватного сектору, академічної спільноти та представників промисловості. Співпраця між державним та приватним секторами сприяє формуванню штату досвідчених фахівців, що є важливим напрямком забезпечення кібербезпеки. Естонське законодавство навіть дозволяє цивільним фахівцям легально брати участь у військових операціях з метою посилення кіберзахисту під час кризових ситуацій.

Тому державно-приватне партнерство передбачає навчання та підвищення кваліфікації щодо навичок у сфері оцінки ризиків, управління кіберінцидентами та проведення аналізу кіберзагроз. Одночасно фахівці з кібербезпеки повинні мати аналітичні здібності, вміти виявляти та керувати кіберризиками, забезпечувати безперервність функціонування ІТ-бізнесу на рівні комерційних підприємств, установ та організацій. Щоб усунути наявні прогалини, Естонія вживає заходів з метою розробки та удосконалення програм освіти і навчання з питань кібербезпеки. Національні ініціативи, такі як підвищення кваліфікації фахівців державного та приватного ІТ-секторів, розробка академічних програм у галузі кібербезпеки активно впроваджуються на державному рівні.

Механізми фінансування державно-приватного партнерства у сфері забезпечення кібербезпеки включають: опанування грантової допомоги, стимулювання залучення інвестицій у дослідження та інновації, зокрема фінансування науково-дослідницьких та проектно-конструкторських робіт, сприяння інноваційному підприємництву в ІТ-сфері шляхом запровадження інституту дотацій й субсидій тощо. Державне фінансування передбачає формування з боку уряду платформи для реалізації R&D у сфері кібербезпеки, здійснення закупівель, залучення грантової допомоги, інвестицій, встановлення податкових пільг для телекомунікаційних компаній. З метою активізації інноваційної діяльності у сфері забезпечення кібербезпеки у рамках державно-приватного партнерства можуть використовуватися різні форми та інструменти державної підтримки проектів, спрямовані на підвищення їхньої ефективності, що включає такі її форми, як: фінансова, податкова, державні гарантії тощо. Таким чином, Естонія активно залучає приватний сектор до розробки та впровадження концептуальних засад політики кібербезпеки. Успіх Естонії у питаннях розбудови державно-приватного партнерства заснований на залученні провідних технологічних компаній до цих процесів. Для України досвід Естонії може бути цінним у створенні власної моделі ДПП, особливо в умовах посилення кіберзагроз.

Форми державно-приватного партнерства у сфері забезпечення кібербезпеки передбачають: розробку та надання урядом рекомендацій для приватного сектору за наслідками виявлення та відстеження кіберінцидентів у кіберпросторі; проведення заходів, спрямованих на спільне вивчення та опанування сучасного досвіду запобігання кібератакам та кіберзагрозам з урахуванням динамічної зміни їхнього ландшафту; постійне удосконалення політики “Government Relations” у сфері забезпечення кібербезпеки Естонії, яка базується на інтеграції державного та приватного секторів, що дозволяє ефективно протистояти кіберзагрозам і просувати цифрову кіберстійкість; щорічне проведення конференцій та інших науково-практичних заходів з метою обміну

досвідом і технологіями. Державно-приватне партнерство у сфері кібербезпеки Естонії є ключовим елементом її стратегії захисту цифрової інфраструктури та забезпечення стійкості до кіберзагроз. Формат залучення приватного сектору у питаннях забезпечення кібербезпеки передбачає їхнє миттєве реагування на кіберзагрози, що засвідчує відсутність бюрократичних обмежень, що Естонія використовує як важливу перевагу. Естонія, як одна з найбільш цифрових країн світу, ефективно залучає та стимулює приватний сектор до співпраці з державою, що дозволяє створювати інноваційні рішення, швидко реагувати на будь-які кіберзагрози та зміцнювати міжнародну позицію Естонії у сфері кібербезпеки.

Державно-приватне партнерство в Естонії є зразковим прикладом ефективної співпраці у сфері кібербезпеки, що базується на взаємній довірі, обміні інформацією та спільних інноваціях. У рамках розбудови державно-приватного партнерства у сфері забезпечення кібербезпеки розроблено алгоритми щодо швидкої мобілізації цивільних фахівців у разі масштабних кібератак, в рамках якого держава отримує доступ до новітніх розробок приватних ІТ-гігантів. На цьому фоні важливою проблемою залишається нестача професійного кадрового потенціалу приватного сектору.

З цього приводу слушно зазначає К. Хоєцька, що державно-приватне партнерство у сфері кібербезпеки в умовах цифрової трансформації є формою залучення представників приватного сектору для організації комплексної співпраці з метою захисту державних інтересів у кібердомені [10, с.52].

Слід вказати, що щорічно Естонія організовує та проводить міжнародні кібернавчання з активної кібероборони під егідою Об'єднаного центру передових технологій з кібероборони НАТО, що надає змогу державі та приватному сектору відпрацьовувати спільну відповідь на кібератаки на об'єкти критичної інфраструктури в умовах, максимально наближених до реальних. У травні 2025 року в Естонії відбулися міжнародні навчання із кібероборони – Locked Shields, які організував Центр співробітництва НАТО у сфері кібероборони, що базується в Таллінні, за участю 4 тис. експертів із 41 держав-член і партнерів НАТО [23]. Естонія активно експортує свою модель державно-приватного партнерства у сфері кібербезпеки, допомагаючи іншим державам ЄС та світу, зокрема Україні у питаннях сприяння розбудові національної системи кібербезпеки, з використанням Таллінського механізму – міжнародної ініціативи, через яку Естонія разом з партнерами координує підтримку кіберстійкості України шляхом залучення у тому числі й приватних компаній для реалізації проєктів у сфері кіберзахисту [24]. Талліннський механізм було запущено у грудні 2023 році як міжнародну відповідь на зростання кіберзагроз та постійну російську агресію, у тому числі й у кібердомені з метою посилення кіберзахисту України шляхом підвищення ефективності та скоординованості міжнародної допомоги між країнами-партнерами. Він став платформою, яка об'єднує зусилля багатьох країн-партнерів у спільній боротьбі з кіберзагрозами та захисті цифрової інфраструктури України.

25-26 вересня 2025 року в рамках Талліннського механізму, відбувся дводенний технічний тренінг з кібербезпеки "UA-EE Cyber Shield", організований Національним координаційним центром кібербезпеки при РНБО України спільно з естонськими партнерами – Estonian Centre for International Development (ESTDEV), CybExer Technologies та e-Governance Academy з метою об'єднання українських фахівців державних органів та установ задля отримання практичних навичок у сфері виявлення та протидії кіберзагрозам, розбудови державно-приватного партнерства [25].

Висновки. Державно-приватне партнерство у сфері кібербезпеки в Естонії є одним із ключових елементів моделі цифрової стійкості країни. Естонія не має окремого закону

про державно-приватне партнерство, проте активно залучає стартапи та приватні ІТ-компанії (Cybernetica, Guardtime, Bitdefender Estonia тощо) для співпраці. Одночасно законодавство Естонії стимулює залучення приватних структур до захисту критичної інформаційної інфраструктури, забезпечуючи високий рівень довіри між державою та приватним сектором та демонструє усунення будь-яких бюрократичних перепон у цьому процесі. Заслуговує на увагу успішна діяльність естонського кібертехнологічного кластеру. Загалом, державно-приватне партнерство у сфері забезпечення кібербезпеки Естонії — це субкультура співпраці та довіри між державою та приватним сектором, які підкріплені законодавством про критичну інфраструктуру та функціонуванням спільних сервісів. Невипадково ця модель вважається однією з найефективніших в ЄС та активно опановується іншими країнами (включаючи Україну).

Естонія залишається важливим стратегічним партнером України, який послідовно підтримує Україну в її прагненні зміцнити кіберстійкість і динамічно розвивати власний високотехнологічний бізнес. На постійній основі Естонія підтримує та реалізує низку проектів та ініціатив, спрямованих на розвиток кібербезпекових спроможностей України. Консолідація зусиль державного та приватного секторів Естонії та України дозволить не лише ефективно протидіяти кіберзагрозам, але й створити нові можливості для розвитку інноваційних продуктів, які матимуть вагоме значення для всієї Європи. Також для України досвід Естонії у сфері державно-приватного партнерства може бути досить корисним під час удосконалення власної моделі державно-приватного партнерства, особливо в умовах посилення кіберзагроз в умовах російської військової агресії, подальшої розбудови стратегічного партнерства між Україною та Естонією, спрямованого на зміцнення кіберстійкості та перспективного розвитку спільних ініціатив у сфері кібербезпеки.

Виходячи із викладеного, держава спільно з приватним сектором має розробити та запровадити засновану на довірі ефективну модель взаємодії у сфері забезпечення кібербезпеки, що передбачає: врегулювання цього питання на законодавчому рівні, визначивши форми і методи здійснення такого партнерства з метою зміцнення взаємної довіри; запровадження пілотних менторських програм підвищення кваліфікації фахівців державних органів, що безпосередньо виконують функції із забезпечення кібербезпеки та кіберзахисту шляхом залучення сертифікованих за міжнародними стандартами фахівців приватного сектору; впровадження на підприємствах, в установах і організаціях незалежно від форми власності субкультури кібербезпеки, що полягає у постійному підвищенні кіберобізнаності їх керівників та працівників.

У зв’язку з цим потребує прискорення схвалення законопроекту “Про основи всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі” від 01.08.2025 р. № 13592 [26], що надасть змогу: активно залучати представників приватного сектору до протидії деструктивній діяльності в кіберпросторі; налагодити взаємодію між державними органами, бізнесом і громадськістю у сфері кібербезпеки; підвищити рівень кіберстійкості на національному рівні.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Маркєєва О.Д., Розвадовський Б.Л. Теоретичні підходи до державно-приватного партнерства у сфері національної безпеки. *Стратегічна панорама.* 2022. №1. С. 42-50. DOI https://doi.org/10.53679/2616-9460.1.2022.04.

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.

3. The NATO Cooperative Cyber Defence Centre. URL: https://ccdcoe.org.

4. Growing Cyber Talent Through Public–Private Partnerships. URL: https://reports.weforum.org/docs/WEF_Growing_Cyber_Talent_Through_Public_Private_Partnerships_2025.pdf.

5. 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.

6. 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.

7. 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.

8. Матвієнко В.М., Петушкова Г.Є. Європейський досвід державно-приватного партнерства у сфері кібербезпеки: можливості для України. *Актуальні проблеми міжнародних відносин.* 2022. Том. 1. С.10-18. DOI https://doi.org/10.17721/apmv.2022.152.1.10-18.

9. Поляков О.М. Особливості залучення приватного сектору до здійснення заходів у сфері забезпечення кібербезпеки, стримування деструктивної діяльності у кіберпросторі: кращі практики європейського досвіду. *Інформація і право.* 2025. № 3 (54). С. 157-168. DOI https://doi.org/10.37750/2616-6798.2025.3(54).340524

10. Chojecka K. Cybersecurity, Resilience and Sustainability: Evaluating The Role of Public-Private Partnerships. *YEARBOOK OF ANTITRUST AND REGULATORY STUDIES.* 2025. №18. PP. 39-55. DOI: 10.7172/1689-9024.YARS.2025.18.32.9. URL: https://press.wz.uw.edu.pl/cgi/viewcontent.cgi?article=1487&context=yars.

11. Küberturvalisuse seadus 09.05.2018. URL: https://www.riigiteataja.ee/akt/122052018001.

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

13. Elektroonilise side seadus 08.12.2004. URL: https://www.riigiteataja.ee/akt/127022022003.

14. Cybersecurity Strategy 2024-2030. URL: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf.

15. Küberjulgeolek 2025: Väljakutsed ja strateegiad. URL: https://neverhack.ee/blogi/kuberjulgeolek-2025-valjakutsed-ja-strateegiad

16. KSI Blockchain. URL: https://e-estonia.com/solutions/cyber-security/ksi-blockchain.

17. National Cyber Security Centre — NCSC-EE. URL: https://www.ria.ee/en/cyber-security/national-cyber-security-centre-ncsc-ee

18. Computer Emergency Response Team Estonia. URL: https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee.

19. Eesti CyberTech klaster. URL: https://itl.ee/cybertech.

20.Riikliku Küberturvalisuse aastakonverents 2025. URL: https://onlineexpo.com/ee/kuberturvalisus-2025.

21. CyberHubs. Cybersecurity Skills Needs Analysis report Estonia. URL: https://cyberhubs.eu/wp-content/uploads/2024/10/Estonia_Cybersecurity-skills-needs-analysis-report-1.pdf.

22. Ühisavaldus riikide vastutustundliku käitumise edendamise kohta küberruumis. URL: https://www.vm.ee/uudised/uhisavaldus-riikide-vastutustundliku-kaitumise-edendamise-kohta-kuberruumis.

23. В Естонії пройдуть масштабні навчання з кібероборони Locked Shields. URL: https://www.eurointegration.com.ua/news/2025/05/3/7210832.

24. Tallinn Mechanism. URL: https://www.cdto-campus.com/en/faculties/tallinn-cybersecurity-mechanism.

25. Україна та Естонія посилюють взаємодію у сфері кібербезпеки. URL: https://www.rnbo.gov.ua/ua/Diialnist/7296.html.

26. Про основи всебічного залучення приватного сектору та громадянського суспільства до здійсмнення заходів зі стримування деструктивної діяльності в кіберпросторі: проект Закону України від 01.08.2025 р. №13592. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/56929.

Сергій Анатолійович Красніков
провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
03113, вул. Миколи Василенко, 3, Київ, Україна
email: sergkrasnikov@ukr.net

Serhii A. Krasnikov
Leading Researcher, Ukrainian Scientific and research Institute of special equipment and forensic expertise of the Security Service of Ukraine
03113 Kyiv, Ukraine, M. Vasylenka Str. 3
email: sergkrasnikov@ukr.net

Рекомендоване цитування: Красніков С.А. Державно-приватне партнерство у сфері забезпечення кібербезпеки: досвід Естонії. *Інформація і право.* № 2(57)/2026. 2026. С. 227-237. https://doi.org/10.37750/2616-6798.2026.2(57).364487

Suggested Citation: Krasnikov S. (2026) Public-Private Partnership in Cybersecurity: Estonian Experience. *Information and Law*. 2(57)/2026. 227-237. https://doi.org/10.37750/2616-6798.2026.2(57).364487

Дата надходження статті до редакції: 15.04.2026 р.
Дата прийняття статті до друку після рецензування: 05.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

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