Інформаційна довідка
щодо проекту Закону України
«Про основи всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі»
*(реєстр. № 13592 від 01.08.2025)**

Анотація. *В інформаційній довідці досліджуються організаційно-правові засади залучення та участі представників приватного сектору і громадянського суспільства у спільній з державними органами протидії деструктивній діяльності в кіберпросторі. Зазначені питання досліджуються в контексті пропозицій, передбачених у проекті Закону України (реєстр. № 13592 від 01.08.2025) (далі – законопроект).*

Розглядається відповідність законопроекту нормам Конституції України, основоположним засадам правотворчої діяльності та техніки нормопроектування, актам права Європейського Союзу (далі – ЄС), положенням чинного законодавства України, що регулюють суспільні відносини у сфері забезпечення національної безпеки, зокрема здійснення державно-приватного партнерства з питань кібербезпеки.

За результатами дослідження виявлено ризики, які перешкоджатимуть належній реалізації законопроекту під час правозастосовної діяльності та досягненню проголошеної в ньому мети, спрямованої на законодавче забезпечення взаємодії між державними органами і громадськістю щодо реагування на загрози у кіберпросторі, запровадження на національному рівні ефективної системи кіберстійкості.

Ключові слова*: національна безпека; забезпечення кібербезпеки; інциденти з кібербезпеки; кіберпростір; державно-приватне партнерство; протидія кіберзагрозам, фахівці з кібербезпеки; стримування деструктивної діяльності у кіберпросторі.*

І. Вступна частина.

В умовах збройної агресії російської федерації відбуваються безпрецедентні за масштабом, технологічним рівнем та кількістю потужні кібератаки на об’єкти критичної інфраструктури та усі інформаційні ресурси України. Як наслідок, це вимагає від держави максимального посилення протидії таким кібератакам, забезпечення надійного та ефективного захисту кіберпростору України.

Російська військова агресія продемонструвала, що об’єктами масштабних кібератак можуть бути як державні підприємства чи установи, так і недержавні, приватні бізнес-структури. У багатьох випадках руйнівні наслідки таких атак взаємопов’язані між собою, оскільки несанкціоноване проникнення в систему даних приватних компаній може становити серйозну потенційну загрозу й для державних органів, установ та організацій, які використовують програмне забезпечення, розроблене приватними компаніями.

Окрім того, в умовах динамічної цифровізації усіх сфер життєдіяльності суспільства кожна громадська організація або бізнес-структура вимушена дбати не лише про захист персональних даних своїх членів, клієнтів чи комерційної

таємниці, але й гарантувати й забезпечувати всебічний кіберзахист усіх власних процесів та об'єктів критичної інфраструктури від потенційних ворожих посягань, особливо у кіберпросторі. Своєю чергою такий захист на сьогодні неможливий без співпраці недержавних установ з відповідними державними органами, наділеними спеціальною компетенцією та повноваженнями.

Вирішуючи стратегічні завдання щодо створення повноцінної системи кіберзахисту, держава має залучати для цього значну кількість висококваліфікованих експертів та фахівців, зокрема й поза межами державного сектору, які отримали спеціальну підготовку у сфері інформаційних технологій (аналітики, програмісти, хакери), мають необхідний спектр знань, навичок і вмінь у питаннях забезпечення кібербезпеки, зберігання й обробки цифрових даних та зможуть протистояти будь-яким загрозам у кіберпросторі.

Тобто державно-приватне партнерство у сфері запобігання та усунення кіберзагроз є важливою складовою національної безпеки в умовах відсічі збройної агресії. Воно дозволяє забезпечувати ефективну протидію сучасним кіберзагрозам, а також консолідувати спільні спроможності, зусилля і ресурси для здійснення кіберзахисту на національному рівні.

В умовах зростаючої кількості кіберінцидентів, стійкої тенденції збільшення масштабів кіберзагроз, які завдають значної шкоди інформаційно-телекомунікаційним системам, економіці й національній безпеці, головною метою залучення фахівців приватного сектору є спільне з державними установами реагування на вищевказані загрози та мінімізація їх наслідків.

Досягнення цієї мети зумовлює необхідність запровадження всебічного нормативно-правового регулювання такого державно-приватного партнерства, насамперед встановлення організаційно-правових засад співробітництва, комплексної і рівноправної взаємодії держави з фахівцями у сфері інформаційних технологій та кібербезпеки. Результатом створення сучасної нормативно-правової бази має стати налагодження постійної та ефективної співпраці між державою й приватним сектором, забезпечення стабільного кіберзахисту та кіберстійкості всіх об'єктів критичної інфраструктури та інформаційних систем України.

Підготовка відповідної законодавчої бази передусім має бути адаптована до вимог актів права та досвіду держав-членів ЄС у досліджуваній сфері, що переконливо засвідчують важливість та ключове 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) 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 (далі – Директива NIS2)[1] (далі – Директива).

---

[1] 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

Зокрема, відповідно до пункту 55 Директиви державно-приватні партнерства (ДПП) у сфері кібербезпеки мають забезпечити належну основу для обміну знаннями, передовим досвідом та встановлення спільного рівня розуміння між зацікавленими сторонами. Держави-члени повинні сприяти політиці, що лежить в основі створення ДПП, які спеціалізуються на кібербезпеці. Ця політика повинна уточнювати, серед іншого, сферу застосування та залучені зацікавлені сторони, модель управління, доступні варіанти фінансування та взаємодію між зацікавленими сторонами щодо ДПП. ДПП можуть використовувати досвід приватних організацій для допомоги компетентним органам у розробці найсучасніших послуг та процесів, включаючи обмін інформацією, раннє попередження, навчання щодо кіберзагроз та інцидентів, управління кризами та планування стійкості.

В Україні на сьогодні державно-приватне партнерство у сфері забезпечення кібербезпеки регулюється насамперед такими законами: «Про національну безпеку», «Про державно-приватне партнерство», «Про основні засади забезпечення кібербезпеки», «Про критичну інфраструктуру», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» тощо.

Положення статті 10 та деяких інших норм Закону України «Про основні засади забезпечення кібербезпеки» визначають пріоритетні напрями та форми державно-приватної взаємодії у сфері кібербезпеки.

Серед них актуальними в умовах правового режиму воєнного стану, зокрема, є: створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, обмін інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, кібератак та кіберінцидентів; взаємодія з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі; кіберзахист державних і приватних інформаційних ресурсів, інформаційно-комунікаційних та ІТ-систем; стимулювання розроблення вітчизняних програмних продуктів; здійснення громадського контролю ефективності заходів у сфері забезпечення кібербезпеки.

Виходячи із визначених законом загальних засад державно-приватного партнерства у сфері кібербезпеки, у Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021 «Про «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», проголошується, 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.

На виконання вказаних стратегічних завдань пунктом 30 Плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України, затвердженого розпорядженням Кабінету Міністрів України від 19.12.2023 р. № 1163-р та

пунктом 14 Плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України, затверджених розпорядженням Кабінету Міністрів України від 07.032025 р. № 204-р, передбачено необхідність забезпечення розроблення законопроекту, спрямованого на врегулювання питань щодо всебічного залучення приватного сектору та громадянського суспільства до здійснення заходів із стримування деструктивної діяльності в кіберпросторі[2].

Основна частина.

Вищевикладене обумовило підготовку досліджуваного законопроекту, який визначає правові та організаційні засади залучення фахівців з реагування на інциденти кібербезпеки до здійснення компетентними державними установами заходів, спрямованих на усунення кіберзагроз, стримування деструктивної діяльності у кіберпросторі, загалом протидії збройній агресії проти України у цій сфері.

Законопроект містить 23 статті та складається з чотирьох розділів: «Загальні положення»; «Основні засади державного регулювання діяльності у сфері залучення фахівців з реагування на інциденти з кібербезпеки до участі у стримуванні та протидії агресії проти України в кіберпросторі»; «Правовий статус фахівців з реагування на інциденти з кібербезпеки при залученні їх до участі у стримуванні та протидії агресії проти України в кіберпросторі»; «Прикінцеві та перехідні положення».

З метою узгодження з нормами інших законодавчих актів у названій сфері законопроект також передбачає внесення відповідних змін до Законів України «Про Службу безпеки України», «Про Національний банк України», «Про державно-приватне партнерство», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру».

За результатами проведеного дослідження, підтримуючи необхідність удосконалення чинного законодавства щодо державно-приватного партнерства при забезпеченні кібербезпеки та захисті національних інтересів України у кіберпросторі, з урахуванням передбачених у законопроекті пропозицій, вважаємо за доцільне відзначити таке.

Дослідницькою службою Верховної Ради України було підготовлено парламентське дослідження щодо особливостей законодавчого забезпечення державно-приватного партнерства у сфері забезпечення кібербезпеки на прикладі деяких європейських держав. У ньому висвітлено досвід певних держав-членів ЄС щодо нормативного регулювання підстав та порядку цього партнерства, його актуальні моделі, умови та особливості здійснення у різних країнах. За результатами дослідження надано пропозиції щодо можливостей використання такого досвіду для створення в України власної моделі державно-приватного партнерства у сфері забезпечення кібербезпеки, визначено основні напрямки та заходи його реалізації.

---

[2] Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України: розпорядження Кабінету Міністрів України від 19.12.2023 № 1163-р. URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text

Насамперед слід зазначити, що для належного застосування законопроекту та реалізації його мети щодо ефективного правового регулювання державно-приватного партнерства у сфері спільної протидії кіберзагрозам, вирішальне значення має якомога точне, чітке визначення термінів «приватний сектор» та «громадянське суспільство», які використовуються у назві та тексті законопроекту. Незважаючи на це, їх роз'яснення у статті 1 «Визначення основних термінів» або в інших статтях законопроекту відсутнє.

Водночас при їх формулюванні має бути враховано, що «приватний сектор», з огляду на його обов'язкові ознаки, може бути визначено як «сфера діяльності різноманітних недержавних, приватних підприємств, компаній, установ та організацій, функціонування яких не пов'язане з державною власністю чи державною службою».

Враховуючи конститутивні, невід'ємні ознаки «громадянського суспільства», його визначення має охоплювати «діяльність громадських об'єднань, спілок, товариств, інших організацій, функціонування політичних партій, засобів масової інформації та інших суспільних інститутів, інші форми взаємодії громадян та їхніх об'єднань поза державним сектором».

Передбачене у пункті 1 частини першої статті 1 законопроекту визначення «державно-приватного партнерства у сфері здійснення заходів зі стримування деструктивної діяльності в кіберпросторі» має доволі громіздку стилістичну структуру, перенасичене різними повторюваними та логічно не зв'язаними між собою термінами. Це утруднює його однозначне розуміння та, як наслідок, може суттєво ускладнити належну реалізацію законопроекту, зважаючи на ключове значення цього поняття для предмета його правового регулювання, а також його використання в інших нормах законопроекту.

Так, у запропонованій редакції це визначення фактично роз'яснює «само себе», оскільки «…партнерство у сфері здійснення заходів зі стримування деструктивної діяльності в кіберпросторі» передусім пояснюється через «співробітництво…у здійсненні заходів зі стримування деструктивної діяльності в кіберпросторі».

У кінцевому підсумку зазначені у ньому дії щодо «деструктивної діяльності в кіберпросторі», в тому числі «інциденти кібербезпеки та кібератаки», можуть тлумачитись як такі, що «здійснюються в порядку, встановленому цим Законом та іншими законодавчими актами».

Окрім того, наведений перелік дій у терміносистемі «… виявлення вразливостей, протидії, запобігання, виявлення, нейтралізації та відновлення після інцидентів кібербезпеки та кібератак …», що використовується у пропонованому визначенні та диспозиціях інших норм законопроекту, вочевидь не відповідає логічній та фактичній послідовності заходів, які мають бути вчинені з метою «протидії кіберзагрозам» та становлять складові компоненти змісту такої «протидії».

Тобто у запропонованій редакції зазначена норма не повною мірою відповідає вимогам щодо змісту норми права, що міститься у нормативно-правовому акті, зокрема її ясності, точності, однозначності розуміння та

доступності для реалізації, встановленим статтею 34 Закону України «Про правотворчу діяльність» приписам.

З огляду на викладене, вважаємо за доцільне назване визначення з метою його оптимізації викласти у такій редакції: «Державно-приватне партнерство у сфері здійснення заходів зі стримування деструктивної діяльності в кіберпросторі – це співробітництво між державою Україна в особі компетентних державних органів (державних партнерів) та фахівцями з реагування на інциденти кібербезпеки, Лігою стримування деструктивної діяльності в кіберпросторі України та іншими представниками приватного сектора, що здійснюється в порядку, передбаченому цим Законом та іншими законодавчими актами, з метою запобігання, виявлення, нейтралізації та усунення наслідків кібератак та інцидентів кібербезпеки, протидії іншим проявам збройної агресії проти України в кіберпросторі».

Загальні ознаки державно-приватного партнерства, про що теж згадується у вказаному пункті, не визначаються «*цим Законом*», оскільки він має спеціальний, навіть вузькоспеціалізований характер. У разі необхідності у законопроекті може бути зроблене відповідне посилання на Закон України «Про державно-приватне партнерство», у якому надається загальне визначення цього поняття.

Виходячи зі змісту законопроекту, Ліга стримування деструктивної діяльності в кіберпросторі України, як «самоврядна професійна організація, що об’єднує фахівців з реагування на інциденти кібербезпеки», визначена як єдина громадська недержавна організація, що може представляти фахівців з реагування на інциденти кібербезпеки у питаннях партнерства з державними органами щодо протидії кіберзагрозам. На це вказують положення частини другої статті 7 законопроекту, згідно з якими професійне самоврядування фахівців з реагування на інциденти з кібербезпеки здійснюється виключно через зазначену Лігу.

Крім того, відповідно до частини першої статті 6, статті 8 законопроекту відомості про фахівців з реагування на інциденти кібербезпеки, які залучаються до здійснення заходів зі стримування деструктивної діяльності в кіберпросторі, мають бути в обов’язковому порядку внесені до спеціальної Бази даних. При цьому підставою для такого внесення має бути набуття вказаною фізичною особою членства у вищеназваній Лізі.

Водночас, ані Закон України «Про державно-приватне партнерство», що визначає організаційно-правові засади та принципи взаємодії державних та приватних партнерів, ані Закон України «Про основні засади забезпечення кібербезпеки України», що визначає правові та організаційні основи забезпечення кібербезпеки, засади координації такої діяльності, в т.ч. суб’єктів, які в межах своєї компетенції здійснюють заходи із забезпечення кібербезпеки та суб’єктів національної системи кібербезпеки (статті 5, 8 цього Закону), ані інші законодавчі акти у сфері захисту кіберпростору не містять будь-яких положень щодо участі у стримуванні деструктивної діяльності в кіберпросторі загалом однієї громадської організації чи недержавної установи, наявності у неї, внаслідок цього монопольного права представляти приватну сторону у відповідному державно-приватному партнерстві.

У законопроекті та доданих до нього документах не обґрунтовується, чому вказана «самоврядна професійна організація» матиме назву «Ліга». Виходячи з її мети та функціональної спрямованості, вбачаються більш слушними такі назви як «асоціація», «об'єднання», «спілка». Зазвичай назва «ліга» застосовується для найменування міжнародних чи спортивних організацій.

Наведений у статті 2 законопроекту «Законодавство про правові засади залучення та діяльності фахівців з реагування на інциденти з кібербезпеки щодо запобігання деструктивній діяльності в кіберпросторі» перелік відповідних законів є неповним і потребує доповнення. Окрім вказаних у цій статті зазначена сфера суспільних відносин регулюється також Законами України: «Про державно-приватне партнерство»; «Про критичну інфраструктуру»; «Про Державну службу спеціального зв'язку та захисту інформації України»; «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури».

У частині четвертій статті 3 законопроекту «Сфера застосування цього Закону» зазначено, що «особливості організаційних засад залучення фахівців з реагування на інциденти з кібербезпеки до участі у здійсненні заходів зі стримування деструктивної діяльності в кіберпросторі…у сферах національної безпеки, громадської безпеки, оборони чи правоохоронної діяльності, включаючи виявлення та розслідування кримінальних правопорушень, визначаються Службою безпеки України».

Однак така редакція не враховує, що відповідно до вимог статей 1, 2 Закону України «Про Національну поліцію» до завдань Національної поліції України також належить, серед іншого, забезпечення публічної безпеки і порядку, зокрема виявлення та розслідування відповідних кримінальних правопорушень.

Крім того, зазначені у цій статті сфери належать до компетенції не тільки Служби безпеки України, а й інших державних органів. Так, відповідно до положень пунктів 16 та 17 частини першої статті 1 Закону України «Про національну безпеку України» сектор безпеки і оборони та сили безпеки становлять систему органів державної влади, в т.ч. правоохоронних органів, державних органів спеціального призначення з правоохоронними функціями, діяльність яких перебуває під демократичним цивільним контролем і відповідно до Конституції та законів України за функціональним призначенням спрямована на захист національних інтересів України від загроз.

Перелік державних органів, що, окрім Служби безпеки України, входять до сектору безпеки і оборони, визначений у частині другій статті 12 цього Закону.

З огляду на викладене, частина четверта статті 3 законопроекту підлягає корегуванню. Зокрема, після слів «визначаються Службою безпеки України» вона має бути доповнена словами «а також Національною поліцією України, іншими правоохоронними органами, державними органами спеціального призначення з правоохоронними функціями, іншими державними органами, діяльність яких за функціональним призначенням, передбаченим законом, спрямована на захист національних інтересів України».

Окрім того, частину другу цієї статті доречно викласти у редакції: «Суспільні відносини у сфері залучення фахівців з реагування на інциденти кібербезпеки регулюються цим Законом, з урахуванням положень Законів України «Про національну безпеку України», «Про правовий режим воєнного стану», «Про правовий режим надзвичайного стану», «Про функціонування єдиної транспортної системи України в особливий період», «Про оборону України», «Про основні засади забезпечення кібербезпеки», «Про державно-приватне партнерство», «Про критичну інфраструктуру», «Про Державну службу спеціального зв'язку та захисту інформації України». Це також узгоджувалося би з положеннями статті 2 законопроекту щодо переліку законів, які регулюють досліджувану сферу суспільних відносин.

Актуальним у контексті досягнення мети законопроекту вважали би доповнення його нормами, які би конкретизували підстави та порядок взаємодії державних органів та залучених ними фахівців–представників приватного сектору під час протидії кіберзагрозам. Насамперед, це стосується обміну інформацією щодо можливих чи наявних кіберзагроз об'єктам критичної інфраструктури, кібератак та кіберінцидентів, а також обміну інформацією з фізичними особами, громадськими організаціями, ІТ-компаніями з метою виконання конкретних заходів запобігання, виявлення та нейтралізації кіберзагроз та усунення їх негативних наслідків. Законодавчою основою для цього можуть бути положення статті 9-1 «Національна система обміну інформацією про кіберінциденти, кібератаки, кіберзагрози» Закону України «Про основні засади забезпечення кібербезпеки».

Пропонована у законопроекті редакція частини першої статті 20 «Відповідальність за порушення законодавства у сфері кібербезпеки», незважаючи на свою громіздку структуру, є незавершеною, оскільки у ній не зазначено саме про *відповідальність* «фахівців з реагування на інциденти з кібербезпеки» за вчинення діянь, «що мають ознаки порушень законодавства».

Частина друга цієї статті, що фактично обмежує кримінальну чи адміністративну відповідальність вказаних фахівців лише діями, які містять «ознаки умисного порушення законодавства», не узгоджується з вимогами статей 24, 25 Кримінального кодексу України (далі – КК України) та статей 10, 11 Кодексу України про адміністративні правопорушення. Вони передбачають можливість притягнення до кримінальної або адміністративної відповідальності як за умисні, так і за необережні правопорушення. Підстави притягнення до відповідальності за вчинення конкретних діянь, зокрема у сфері державно-приватного партнерства з питань кібербезпеки, мають бути встановлені виключно вказаними Кодексами. При цьому, згідно із статтею 3 КК України кримінальна протиправність діяння, а також його караність та інші кримінально-правові наслідки визначаються тільки цим Кодексом.

У пояснювальній записці до законопроекту зазначається, що «проект не містить правил і процедур, що можуть становити ризики вчинення корупційних правопорушень». Проте, положення частини першої статті 6 законопроекту передбачають можливість компенсації фактичних та ресурсних витрат, понесених фахівцями з реагування на інциденти з кібербезпеки, у зв'язку з

виконанням ними завдань під час заходів стримування деструктивної діяльності у кіберпросторі. У пункті 4 частини першої статті 12 та у статті 21 законопроекту чітко зазначено, що розмір та порядок компенсації таких витрат визначаються Кабінетом Міністрів України, а їх джерела фінансування становлять, передусім, кошти державного бюджету.

Вбачається, що такий порядок фінансування діяльності представників приватного сектору, залучених до участі у забезпеченні кібербезпеки та протидії загрозам у кіберпросторі, передбачений у законопроекті, об'єктивно містить значні ризики вчинення корупційних правопорушень та правопорушень, пов'язаних із корупцією. Внаслідок цього законопроект потребує проведення відповідної антикорупційної експертизи.

У переліку законодавчих актів, передбачених у «Прикінцевих та перехідних положеннях» законопроекту, до яких пропонується внести відповідні зміни, відсутні Закони України «Про Кабінет Міністрів України», «Про центральні органи виконавчої влади» та «Про оборону України». Це не узгоджується з викладеними у статті 12 пропозиціями щодо наділення додатковими повноваженнями Кабінету Міністрів України, Міністерства оборони України, інших центральних органів виконавчої влади у зв'язку із залученням представників приватного сектору для реалізації державної політики з протидії агресії проти України в кіберпросторі. Своєю чергою їх відсутність не відповідає встановленим Законом України «Про правотворчу діяльність» вимогам до змісту нормативно-правового акту, норми якого мають узгоджуватися з нормами інших законодавчих актів, що регулюють аналогічну сферу суспільних відносин.

Отже, вищеозначені пропозиції досліджуваного законопроекту не повною мірою узгоджуються із встановленими Законом України «Про правотворчу діяльність» вимогами щодо повноти, правової визначеності та системності змісту нормативно-правового акта, відповідності його положень іншим законам та нормам, передбаченим у законопроекті. У подальшому це ускладнить реалізацію законопроекту під час правозастосовної діяльності та досягнення проголошеної в ньому мети щодо законодавчого забезпечення ефективної взаємодії між державними органами та представниками приватного сектору і громадянського суспільства у протидії кібератакам та іншим загрозам кіберпростору України.

Пояснювальна записка до законопроекту містить описання фінансово-економічного обґрунтування фінансових витрат, необхідних для здійснення передбачених у законопроекті заходів. Проте відповідні розрахунки до такого обґрунтування, як того вимагає частина першій статті 27 Бюджетного кодексу України та частина третя статті 91 Регламенту Верховної Ради України, не додаються.

Висновок.

Попри актуальне значення законопроекту, він містить деякі ризики запропонованих у ньому положень, що не повною мірою узгоджуються з усталеними вимогами законодавчої техніки щодо повноти, правової визначеності й системності змісту нормативно-правового акта, його

узгодженості з іншими законами та нормами самого законопроекту. Зазначені ризики в подальшому перешкоджатимуть належній реалізації законопроекту. З огляду на це, вищезазначені положення законопроекту підлягають корегуванню.

Дослідницька служба
Верховної Ради України

** Цей документ підготовлений Дослідницькою службою Верховної Ради України як довідковий інформаційно-аналітичний матеріал. Інформація та позиції, викладені в документі, не є офіційною позицією Верховної Ради України, її органів або посадових осіб. Цей документ може бути цитований, відтворений та перекладений для некомерційних цілей за умови відповідного посилання на джерело.*