

В И С Н О В О К

до проекту Закону про державно-приватну взаємодію у сфері кібербезпеки

(реєстр. № 14150 від 24.10.2025)

Комітет Верховної Ради України з питань цифрової трансформації на своєму засіданні 16 грудня 2025 року (Протокол № 161) розглянув проект Закону про державно-приватну взаємодію у сфері кібербезпеки (реєстр. № 14150 від 24.10.2025), поданий народним депутатом України Федієнком О. П. та іншими народними депутатами України.

Законопроект розроблено з метою впорядкування та розвитку державно-приватної взаємодії у сфері кібербезпеки, побудови сталих комунікацій та координації дій між державними та приватними учасниками взаємодії, консолідації їх зусиль у забезпеченні кібербезпеки, посилення спроможностей національної системи кібербезпеки, забезпечення функціонування організаційно-технічної моделі кіберзахисту, стимулювання інновацій в сфері кібербезпеки та розвитку вітчизняного ринку товарів і послуг у сфері кібербезпеки.

В межах предметів відання Комітету щодо запропонованих законодавчих змін зазначаємо наступне.

Міністерство цифрової трансформації України у своєму висновку висловило, зокрема, такі зауваження та пропозиції.

1. У пункті четвертому частини першої статті 1 проекту Закону зазначено, що проект, що здійснюється на умовах державно-приватної взаємодії в сфері кібербезпеки (далі – проект) – сукупність послідовних заходів, спрямованих на підготовку та реалізацію державно-приватної взаємодії в сфері кібербезпеки за відповідним напрямом із залученням приватних учасників та третіх осіб відповідно до цього Закону.

Крім того, підпунктом третім пункту другого Прикінцевих та перехідних положень проекту Закону пропонується статтю 10 Закону України «Про основні засади забезпечення кібербезпеки України» (далі – Закон) викласти у новій редакції. У пункті 1 частини другої статті 10 запропонованої редакції до Закону також вживається формулювання «за відповідними напрямами».

Таким чином, з метою однозначного трактування норм проекту Закону та правильного застосування їх у майбутньому, формулювання «за відповідним напрямом» потребує уточнення із застосування відсильної норми.

2. Слід звернути увагу, що перелік основних напрямів державно-приватної взаємодії у кібербезпеці викладений у підпункті 3 пункту 2 Прикінцевих та перехідних положень проекту Закону (нова редакція статті 10 Закону) та безпосередньо у статті 4 проекту Закону, що фактично є дублюванням законодавчих норм.

Крім того, у частині другій статті 4 проекту Закону вказано, що державний учасник самостійно, спільно з іншими державними учасниками або спільно з приватними учасниками, має право визначити інший напрям державно-приватної взаємодії у сфері кібербезпеки, якщо це прямо не суперечить законодавству України та спрямовано на посилення.

Слід зазначити, що однією із основних конституційних засад в Україні є принцип верховенства права, що прямо закріплено у статті 8 Конституції України. Відповідно до частини першої статті 68 Конституції України, кожен зобов'язаний неухильно додержуватися Конституції та законів України.

Таким чином, норми закону мають найвищу юридичну силу, є обов'язковими до безумовного виконання і не можуть бути порушені ані прямо, ані опосередковано.

Будь-які положення, що можуть бути витлумачені як дозвіл чи заохочення до відступу від встановлених законом вимог, суперечать конституційним засадам правопорядку та є неприпустимими.

Аналіз запропонованих норм, які дозволяють учасникам вільно обирати напрями, не визначені законом, але спрямовані на «посилення», створює пряму загрозу виникнення колізій у законодавстві, зокрема, у високорегульованій та критично важливій сфері кібербезпеки.

Крім того, пропозиція щодо вільного обрання учасниками різних напрямів, які не визначено законом, за умови «спрямування на посилення» є юридично невизначеною, оскільки не зрозуміло, посилення якої саме сфери мається на увазі. Відсутність чітко визначеної, вимірюваної цілі в частині посилення унеможливорює об'єктивну оцінку відповідності дій учасників публічним інтересам та створює простір для суб'єктивного тлумачення.

Відтак, з метою уникнення корупційних ризиків, недопущення легалізації дій, що не мають прозорого правового обґрунтування, запобігання створенню умов для функціонування в тіньовому секторі, а загалом недопущення ухвалення рішень в інтересах окремих груп, що несе загрозу національним інтересам держави, пропонується частину другу статті 4 проекту Закону виключити та доопрацювати перелік основних напрямів та не дублювати зазначені норми у різних законах.

3. Пунктом 5 частини першої статті 1 проекту Закону пропонується новий термін «проект за нагальною потребою – проект, що здійснюється на умовах державно-приватної взаємодії у сфері кібербезпеки у разі виникнення нагальної потреби та який не передбачений у документах програмно-цільового характеру».

Однак, чітких критеріїв «нагальної потреби» не визначено, що несе ризик корупційної складової, зловживання владою та відсутності прозорості щодо такого проекту.

Крім того, норми, викладені у зазначеному терміні, а також у тексті проекту Закону в цілому (абзац третій пункту 1 частини першої, абзац третій пункту 1 частини другої статті 5, абзац третій пункту 1 частини першої статті 6 проекту Закону) свідчать про те, що проекти за нагальною потребою можуть реалізовуватися без складання документу програмно-цільового характеру та/або внесення змін до них та без застосування конкурентної процедури обрання приватних учасників.

З метою уникнення вищезазначених ризиків, пропонується чітко визначити вичерпний перелік випадків або критеріїв «нагальної потреби», щоб уникнути суб'єктивного застосування та встановити механізм поствиявлення або внутрішнього аудиту для проектів за нагальною потребою, щоб забезпечити їхню прозорість та обґрунтованість.

4. Пунктом 9 частини третьої статті 5 проекту Закону передбачається надання приватним учасникам інформації (даних), необхідної для реалізації відповідного проекту, у тому числі про кіберзагрози, кібератаки, кіберінциденти та заходи кіберзахисту; при цьому надання інформації з обмеженим доступом здійснюється відповідно до вимог законодавства України та умов, передбачених проектом.

Частиною п'ятою статті 11 проекту Закону передбачено, що державний учасник може надавати приватним учасникам службову інформацію, необхідну для реалізації відповідної державно-приватної взаємодії, та встановлювати умови обробки такої інформації. Порядок надання службової інформації, необхідної для реалізації державно-приватної взаємодії у сфері кібербезпеки затверджується Кабінетом Міністрів України.

Також, у частині четвертій зазначеної статті вказано, що якщо інформація за проектом належить до таємної або службової інформації, її надання та обробка здійснюється відповідно до спеціального законодавства, що врегульовує такі відносини.

Запропоновані проектом Закону норми свідчать про право доступу приватних учасників до службової та державної таємниці. При цьому проектом Закону пропонується врегулювати порядок доступу до неї на рівні підзаконного нормативно-правового акту.

Однак, така ініціатива створює загрози неконтрольованих каналів витоку службової та таємної інформації, порушення режиму секретності та підриває основи кіберзахисту національного рівня.

Згідно зі статтею 1 Закону України «Про державну таємницю» державна таємниця - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Зважаючи на норми Закону України «Про державну таємницю», доступ до державної таємниці надається лише громадянам, які пройшли спеціальну перевірку, отримали допуск і на яких покладено виконання обов'язків, пов'язаних із державною таємницею.

Так, приватні учасники державно-приватної взаємодії, за загальним правилом, не є суб'єктами, яким може бути надано доступ до цієї категорії інформації у рамках цивільно-правових відносин.

З урахуванням викладеного, було б доцільно виключити з тексту Закону будь-які положення, які можуть бути витлумачені як право приватного учасника на отримання державної таємниці, навіть із посиланням на спеціальне законодавство.

Крім того, закріпити основні норми регулювання доступу до службової інформації безпосередньо у Законі, зокрема визначити вичерпний перелік видів службової інформації, яка може бути передана приватному учаснику та чіткі цілі такої передачі (виключно для реалізації конкретних функцій проекту), критерії та умови для отримання такої інформації (наприклад, необхідність підписання додаткового договору про нерозголошення, наявність технічних засобів захисту), конкретні та вичерпні санкції за порушення режиму доступу та розголошення.

5. Частиною першою статті 6 проекту Закону визначено, що якщо відповідна державно-приватна взаємодія в сфері кібербезпеки передбачає залучення обмеженої кількості приватних учасників, застосовується конкурентна процедура їх обрання. Порядок проведення конкурентної процедури, а також підстави та порядок проведення неконкурентних процедур обрання приватного учасника для цілей державно-приватної взаємодії у сфері кібербезпеки, затверджується Кабінетом Міністрів України.

Однак спостерігається невизначеність чітких, об'єктивних та вичерпних критеріїв для застосування конкурентної процедури саме на рівні Закону.

Така нормативна недосконалість може надавати державному учаснику дискреційні повноваження щодо суб'єктивного визначення кількості приватних учасників, що, в свою чергу, несе високий ризик необґрунтованого уникнення конкурентних процедур і, як наслідок, корупційних зловживань та порушення принципу рівних можливостей.

6. Статтею 9 проекту Закону визначено основні правові засади ініціювання державно-приватної взаємодії в сфері кібербезпеки приватним учасником, зокрема передбачено подання пропозиції та терміни її розгляду.

Однак, не встановлено обов'язку проведення конкурсу/відбору (конкурентної процедури), якщо пропозицію визнано доцільною, а проект передбачає залучення обмеженої кількості учасників.

Відсутність необхідності проведення конкурсу/відбору приватних учасників може призвести до «ручного» обрання ініціатора без конкурентної процедури, що в свою чергу потребує доповнення проекту Закону відповідними нормами.

7. Частиною третьою статті 9 проекту Закону передбачається, що у разі прийняття рішення про доцільність реалізації державно-приватної взаємодії у сфері кібербезпеки відповідно до отриманої пропозиції, державний учасник розробляє та приймає документ програмно-цільового характеру відповідно до пункту 1 частини третьої статті 6 цього Закону.

Однак, у статті 6 проекту Закону відсутня третя частина, а зміст зазначеної статті стосується обрання приватних учасників, а не документів програмно-цільового характеру, що свідчить про некоректне відсилання та потребує доопрацювання статті 7 проекту Закону, у якій визначені форми та методи державно-приватної взаємодії в сфері кібербезпеки.

8. Згідно з частиною третьою статті 10 проекту Закону інформація, одержана державним учасником від приватного учасника згідно з умовами державно-приватної взаємодії, не може бути використана для ініціювання заходів державного нагляду (контролю) щодо такого приватного учасника, встановлення порушення законодавства таким приватним учасником (його працівниками) або застосування адміністративно господарських санкцій до такого приватного учасника.

Зазначена норма потребує перегляду, оскільки її зміст несе ризик створення маніпуляцій з боку недоброчесних учасників, які можуть намагатися приховати власні порушення під приводом участі у проекті.

9. Варто зазначити, що проектом Закону не визначено центрального органу виконавчої влади, відповідального за формування та реалізацію державної політики саме у сфері державно-приватної взаємодії у сфері кібербезпеки.

Зокрема така визначеність необхідна для координації діяльності державних учасників, методологічного забезпечення (розробки типових форм документів, рекомендацій), узагальнення практики та моніторингу ефективності.

10. Відповідно до пункту 2 пояснювальної записки, метою проекту Закону визначено впорядкування та розвиток державно-приватної взаємодії у сфері кібербезпеки, зміцнення довіри, побудова сталих комунікацій та координації дій між державними та приватними учасниками взаємодії, консолідація їх зусиль у забезпеченні кібербезпеки, посилення спроможностей національної системи кібербезпеки, забезпечення функціонування організаційно-технічної моделі кіберзахисту, стимулювання інновацій в сфері кібербезпеки та розвиток вітчизняного ринку товарів і послуг у сфері кібербезпеки.

Однак, комплексний аналіз аргументів свідчить, що наявні проблеми пов'язані не стільки з відсутністю окремого Закону, скільки із недосконалістю чинного механізму державно-приватного партнерства та декларативним характером норм про державно-приватну взаємодію, встановлених чинним законодавством.

Враховуючи вищезазначене, проект Закону потребує ґрунтовного доопрацювання.

Народні депутати України – члени Комітету при обговоренні законопроекту зазначили, що він покликаний, зокрема, створити необхідні передумови для розвитку співпраці державного і приватного секторів у сфері кібербезпеки в Україні, разом з тим вищезазначені зауваження та пропозиції потребують відповідного опрацювання та врахування.

Враховуючи зазначене, за результатами обговорення Комітет ухвалив:

1. Рекомендувати Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки врахувати висловлені зауваження та пропозиції під час підготовки та розгляду проекту Закону про державно-приватну взаємодію у сфері кібербезпеки (реєстр. № 14150 від 24.10.2025), поданого народним депутатом України Федієнком О. П. та іншими народними депутатами України.

2. Направити Висновок про розгляд зазначеного законопроекту до Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки.

Голова Комітету

М. КРЯЧКО