

**Зауваження і пропозиції до проекту Закону України «Про внесення змін до деяких законів України щодо удосконалення процедур нагляду за кібербезпекою та запровадженням європейських схем сертифікації кібербезпеки», (реєстр. № 12207 від 14.11.2024) (далі – законопроект)**

1. Законопроектом передбачається утворення Кабінетом Міністрів України уповноваженого центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері кібербезпеки, як нового основного суб'єкта національної системи кібербезпеки.

Адміністрація Держспецзв'язку не підтримує обраний законопроектом механізм щодо визначення уповноваженого центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері кібербезпеки. Такий підхід створює значні ризики для функціонування національної системи кібербезпеки та підвищує ймовірність управлінської невизначеності.

Відповідно до частини першої розділу II законопроекту, він набирає чинності з дня, наступного за днем його опублікування, та вводиться в дію через два роки з дня набрання чинності.

Водночас з дня введення в дію законопроекту, Державна служба спеціального зв'язку та захисту інформації України позбавляється повноважень щодо формування та реалізації державної політики у сферах кіберзахисту, активної протидії агресії у кіберпросторі, здійснення державного контролю у цих сферах, координації діяльності інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту.

За таких обставин може виникнути ситуація, коли повноважень у Державної служби спеціального зв'язку та захисту інформації України у відповідній сфері вже не буде, а створення або визначення уповноваженого центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері кібербезпеки, у післявоєнний період, коли ресурси держави будуть обмеженими, потребуватиме значних фінансових, організаційних та часових витрат, що може послабити здатність держави оперативно реагувати на кіберзагрози.

Державна служба спеціального зв'язку та захисту інформації України на цей час ефективно забезпечує формування та реалізацію державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту та володіє необхідними компетенціями, кадровим потенціалом та технічним забезпеченням для ефективного виконання інших, пов'язаних із цими сферами завдань.

Враховуючи зазначене, пропонуємо у законопроекті визначити, що забезпечення формування та реалізації державної політики у сфері кібербезпеки здійснюється Державною службою спеціального зв'язку та захисту інформації України, що є найбільш раціональним рішенням у нинішніх умовах.

Обрання цього варіанту дозволить зберегти безперервність роботи національної системи кібербезпеки, посилити захист національних

електронних інформаційних ресурсів, ефективність реалізації державної політики у сфері кібербезпеки та управління кібербезпекою в державі.

У зв'язку з цим пропонуємо виключити із законопроекту норми, якими вносяться зміни до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» в частині позбавлення Держспецзв'язку відповідних повноважень, а саме пункт 4 розділу I законопроекту викласти у такій редакції:

«4. У Законі України “Про Державну службу спеціального зв'язку та захисту інформації України”:

1) абзац третій частини першої статті 1 виключити;

2) у частині першій статті 3:

у абзаці п'ятому слова “кіберзахисту об'єктів” замінити словами “кібербезпеки”;

у абзаці шостому слова “загальних вимог до кіберзахисту об'єктів критичної інфраструктури” замінити словами “вимог до кібербезпеки національних електронних інформаційних ресурсів”;

у абзаці десятому слова “забезпечення кібербезпеки та кіберзахисту” замінити словами “кібербезпеки”;

3) у частині першій статті 14:

у пункті 85 слова “захисту у кіберпросторі державних” замінити словами “кібербезпеки національних електронних ”;

у пункті 86 слова “щодо кіберзахисту” виключити;

4) у тексті Закону слова “державні інформаційні ресурси” замінити словами “національні електронні інформаційні ресурси”, а слово “кіберзахист” замінити словом “кібербезпека” у відповідних відмінках та формах числа.».

2. У підпункті 1 пункту 1 розділу I законопроекту пропонуємо.

1) абзац четвертий викласти у такій редакції:

«2) безпека електронних комунікаційних мереж та інформаційних, інформаційно-комунікаційних систем – здатність електронних комунікаційних мереж та інформаційних, інформаційно-комунікаційних систем забезпечувати захист від дій, що можуть поставити під загрозу доступність, аутентифікацію, цілісність, конфіденційність інформації, яка в них обробляється, а також послуг, що надаються з використанням зазначених мереж і систем;»;

2) абзац восьмий після слова «інформаційними» доповнити словами «та інформаційно-комунікаційними», а у абзаці дев'ятому слова «та інформаційні» замінити словами «, інформаційні та інформаційно-комунікаційні»;

3) абзацом одинадцятим частини першої статті 2 Закону України «Про хмарні послуги» визначено, що центр обробки даних – спеціалізований технічний комплекс, що складається з інженерної (системи безперебійного електроживлення, вентиляції, охолодження та регулювання вологості, пожежної безпеки, фізичної охорони), інформаційної, електронної

комунікаційної та програмно-апаратної інфраструктури, засоби якого забезпечують або реалізують надання послуг із зберігання та обробки даних, у тому числі, але не обмежуючи: надання хмарних послуг, резервного копіювання даних, передачі даних, оренди комунікаційних стійок, послуг хостингу.

Водночас об'єктами Національного центру резервування державних інформаційних ресурсів є технологічно облаштовані майданчики, будівлі, приміщення, взаємоз'єднані електронними комунікаційними мережами для забезпечення роботи єдиних основних і резервних захищених центрів обробки даних (дата-центрів), у тому числі спеціальних мобільних та пересувних рухомих комплексів, призначених для обробки та збереження національних електронних інформаційних ресурсів (абзац третій пункту 2 Порядку функціонування Національного центру резервування державних інформаційних ресурсів, затвердженого постановою Кабінету Міністрів України від 07.04.2023 № 311).

Враховуючи зазначене пропонуємо абзац двадцять дев'ятий викласти в такій редакції:

«27) Національний центр резервування національних електронних інформаційних ресурсів – організована сукупність інформаційно-комунікаційних систем, центрів обробки даних, розміщених на визначених об'єктах, створених з метою забезпечення стану захищеності та безперервності обробки національних електронних інформаційних ресурсів, кібербезпеки, резервування, та зберігання резервних копій національних електронних інформаційних ресурсів державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів, підприємств, установ та організацій;»;

4) Верховною Радою України прийнятий та переданий на підпис Президента України Закон України «Про внесення змін до деяких законів України щодо функціонування Національної системи конфіденційного зв'язку та Національної електронної комунікаційної мережі» (реєстр. № 10273 від 20.11.2023). Цим Законом передбачається внесення змін, зокрема, до Закону України «Про основні засади забезпечення кібербезпеки України» якими змінюється назва «Національної телекомунікаційної мережі» на «Національну електронно комунікаційну мережу» та надано визначення цього терміну.

Враховуючи зазначене пропонуємо абзац тридцятий виключити, а у тексті законопроекту слова «Національна комунікаційна мережа» у всіх відмінках замінити словами «Національна електронна комунікаційна мережа» у відповідному відмінку;

5) в законопроекті термін «державні інформаційні ресурси» пропонується замінити терміном «національні електронні інформаційні ресурси» в якому під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій

нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів.

Враховуючи зазначене, пропонуємо в абзаці сороковому слова «Перелік національних інформаційних ресурсів» замінити словами «Перелік видів національних інформаційних ресурсів», а у тексті Законів України «Про основні засади забезпечення кібербезпеки України» та «Про національну безпеку України» слова «державні інформаційні ресурси» замінити словами «національні електронні інформаційні ресурси»;

б) абзац сорок третій після слів «надавачі кваліфікованих електронних довірчих послуг» доповнити словами «та послуг електронної ідентифікації з високим рівнем довіри», що забезпечить узгодженість норм із вимогами законодавства у сферах електронної ідентифікації та електронних довірчих послуг.

3. Законопроектом передбачена втрата чинності Закону України «Про захист інформації в інформаційно-комунікаційних системах».

Відповідно до статті 9 цього Закону, власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, зобов'язаний утворювати службу захисту інформації або призначати відповідальних осіб для забезпечення захисту інформації та здійснення контролю за цим процесом. На практиці зазначені служби чи відповідальні особи, що діють в органах державної влади, фактично виконують функції з організації та впроваджені заходів з кіберзахисту.

З урахуванням зазначеного пропонуємо статтю 5<sup>4</sup>, викладену в підпункті 5 пункту 1 розділу I законопроекту, доповнити новою частиною такого змісту:

«10. Суб'єкти виконання вимог з кібербезпеки для вжиття заходів, спрямованих на захист електронної комунікаційної мережі, інформаційних та інформаційно-комунікаційних систем і фізичного середовища цих систем від кіберінцидентів утворюють служби кібербезпеки або призначають осіб, на яких покладається забезпечення кібербезпеки та контролю за ним.

В суб'єктах виконання вимог з кібербезпеки, що є органами державної влади, призначаються керівники із кібербезпеки, яким безпосередньо підпорядковуються служби кібербезпеки.»

4. У підпункті 7 пункту 1 розділу I законопроекту останній абзац викласти у такій редакції:

«5. Впровадження організаційно-технічної моделі кібербезпеки, як складової національної системи кібербезпеки та її періодичний перегляд здійснюється, зокрема, Державним центром кібербезпеки, який забезпечує функціонування та розвиток системи захищеного доступу державних органів до мережі Інтернет, центру антивірусного захисту національних електронних інформаційних ресурсів, тренінгового кіберцентру, аудиту інформаційної безпеки та стану кібербезпеки суб'єктів виконання вимог з кібербезпеки, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, оцінки стану захищеності національних електронних інформаційних ресурсів,

а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, кіберінциденти та кібератаки, заходи щодо протидії ним, програм та методик проведення навчань.».

5. У підпункті 8 пункту 1 розділу I законопроекту абзаци другий - сьомий викласти в такій редакції:

«В рамках роботи Національного центру резервування національних електронних інформаційних ресурсів забезпечується:

1) безперервність обробки відповідного національного електронного інформаційного ресурсу, резервування національних електронних інформаційних ресурсів, зберігання резервних копій національних електронних інформаційних ресурсів шляхом надання послуг, визначених в Порядку надання послуг Національного центру резервування національних електронних інформаційних ресурсів;

2) надійне функціонування серверного обладнання, системи зберігання даних, архітектурно-технічних рішень щодо резервного копіювання й дублювання інформаційних систем, постійно працюючої інженерної інфраструктури;

3) здійснення обов'язкового контролю за статистичними даними роботи системи управління та моніторингу інформаційних систем;

4) здійснення комплексу організаційно-технічних заходів з фізичного захисту об'єктів, кібербезпеки інформаційно-комунікаційних систем та інформації, що в них обробляється;

5) розроблення, створення (побудову), модернізацію, розвиток, впровадження та супроводження програмного забезпечення інформаційної системи (платформи) для побудови та ведення реєстрів;

б) переміщення протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування резервних копій національних електронних інформаційних ресурсів до закордонних дипломатичних установ України зокрема до їх інформаційних (автоматизованих), інформаційно-комунікаційних систем та/або центрів обробки даних, розташованих в будівлях, спорудах таких закордонних дипломатичних установ України та/або на їх території, в порядку, встановленому Кабінетом Міністрів України.

Суб'єкти, порядок функціонування та порядок надання послуг Національного центру резервування національних електронних інформаційних ресурсів визначаються Кабінетом Міністрів України.

6. У підпункті 9 пункту 1 розділу I законопроекту абзаци четвертий, п'ятий та шостий викласти у такій редакції:

«частину першу викласти у такій редакції:

«1. Завданнями CERT-UA є:

1) здійснення організаційно-технічних заходів із запобігання, виявлення, дослідження та реагування на кіберзагрози, кіберінциденти, кібератаки, а також усунення наслідків їх реалізації;

2) аналіз засобів та способів реалізації кіберзагроз, інцидентів кібербезпеки та кібератак, проведення комп'ютерно-технічних досліджень;

3) інформування про кіберзагрози та відповідні методи кібербезпеки, в тому числі, з використанням офіційних вебресурсів та інших засобів обміну інформацією;

4) взаємодія з органами виконавчої, законодавчої і судової влади, державними органами, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, підприємствами, установами і організаціями незалежно від форми власності, в тому числі, ідентифікованими як об'єкти критичної (інформаційної) інфраструктури з питань запобігання, виявлення та усунення наслідків кіберінцидентів та кібератак;

5) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти та обміну інформацією про кіберзагрози, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

6) організація та проведення навчальних заходів з питань кібербезпеки;

7) взаємодія з іншими командами реагування на кіберінциденти, пов'язані з комп'ютерною безпекою (CSIRT), суб'єктами виконання вимог з кібербезпеки та іншими суб'єктами, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору.»».

7. Законопроектом пропонується внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», зокрема шляхом виключення терміну «кіберзахист» з його тексту.

Враховуючи зазначене, пропонуємо у пунктах 1, 2 та 10 розділу I законопроекту включити норму щодо заміни у текстах Законів України «Про основні засади забезпечення кібербезпеки України», «Про національну безпеку України» та «Про публічні електронні реєстри» слова «кіберзахист» на слово «кібербезпека».

8. У законопроекті використовуються терміни, зокрема «об'єкт критичної інфраструктури», «оператор критичної інфраструктури», «оператор критичної інфраструктури міждержавного значення», «оцінка ризику», «Реєстр операторів критичної інфраструктури», які вживаються у значенні, визначеному у проекті Закону України «Про внесення змін до Закону України «Про критичну інфраструктуру» щодо імплементації положень Директиви (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих об'єктів і скасування Директиви Ради 2008/114/ЄС», реєстр. № 12208 від 14.11.2024.

Однак, наразі відсутній офіційний переклад Директиви (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих об'єктів і скасування Директиви Ради 2008/114/ЄС (далі – Директива), що унеможлиблює коректне використання у законопроекті термінології у сфері стійкості критичної інфраструктури та як наслідок може мати прийняття норм, які не відповідатимуть положенням Директиви.