Пропозиції
Адміністрації Державної служби спеціального зв'язку та захисту інформації України

до проєкту Закону України
"Про внесення змін до Закону України "Про Службу безпеки України" щодо удосконалення організаційно-правових засад діяльності Служби безпеки України"
(назва законопроєкту)

Зеленський Володимир Олександрович Президент України
(ініціатор(и) законопроєкту)

реєстр.номер 3196 від "10" березня 2020 року

Законопроєкт готується для включення до першого читання
(зазначити, до якого читання надаються пропозиції)

1. Потребує доопрацювання. Надано зауваження та пропозиції.
(чітка позиція Адміністрації Держспецзв'язку до законопроєкту)

2. Обгрунтування позиції Адміністрації Держспецзв'язку.

2.1. Відповідно до пункту 14 частини першої ст. 12 проєкту Закону пропонується розширити повноваження СБУ, а саме в частині здійснення координації нею діяльності зі створення, застосування та розвитку загальнодержавної системи виявлення кібератак, протидії акціям кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури.

В свою чергу, саме поняття «загальнодержавна система виявлення кібератак, протидії акціям кібертероризму і кібершпигупства щодо об'єктів критичної інформаційної інфраструктури» проєктом Закону та іншими законодавчими актами не визначено.

Крім того, визначення СБУ органом, відповідальним за забезпечення координації діяльності із створення, застосування та розвитку такої системи буде суперечити чинному законодавству та фактично призведе до набуття СБУ невластивих для неї повноважень, оскільки відповідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» пункту 1 частини другої ст. 14 Закону України «Про основні засади забезпечення кібербезпеки України» саме Держспецзв'язку здійснює формування та реалізацію державної політики у сфері кіберзахисту, забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі

державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;

Такий підхід щодо побудов подібних систем суперечить міжнародному досвіду. Приклад провідних країн світу підтверджує, що правоохоронним органам важко досягти атмосфери довіри у приватного сектору і громадянського суспільства через наявність у таких органів інструментів для вчинення тиску та притягнення до відповідальності.

Також слід зазначити, що обладнання, яке має використовуватись у цій системі, фактично буде дублювати сенсори, що встановлюються в рамках функціонування підсистеми збору телеметрії інформаційно-телекомунікаційних систем системи кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, що в свою чергу спричинить дублювання функцій суб'єктів забезпечення кібербезпеки (СБУ та Держспецзв'язку) та призведе до збільшення видатків з державного бюджету України (замість оптимізації обсягів фінансування заходів у сфері кібербезпеки та кіберзахисту).

У зв'язку з цим, з метою уникнення дублювань функцій державних органів у сфері кіберзахисту пропонуємо останнє повноваження СБУ, зазначене у пункті 14 частини першої ст. 12 проєкту Закону, викласти в такій редакції:

«14…..; бере участь у діяльності зі створення, застосування та розвитку загальнодержавної системи виявлення кібератак, протидії акціям кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури».

2.2. Абзацами першим та третім частини третьої ст. 13 проєкту Закону визначено, що СБУ має право отримувати у встановленому порядку інформацію від правоохоронних та інших державних органів, військових формувань, органів місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності та фізичних осіб.

Суб'єкти, яким адресовано зазначений запит, зобов'язані невідкладно, але не більше ніж протягом трьох робочих днів надати СБУ запитувану інформацію