ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту Закону України «Про внесення змін до деяких законодавчих актів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури»

1. Обґрунтування необхідності прийняття акта

Проект Закону України «Про внесення змін до деяких законодавчих актів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури» (далі – законопроект) розроблено Адміністрацією Держспецзв'язку спільно зі Службою безпеки України на виконання підпункту «б» підпункту 6 пункту 1 рішення Ради національної безпеки і оборони України від 10 липня 2017 року «Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32», затвердженого Указом Президента України від 30.08.2017 № 254.

Реалізація вищезазначеного рішення РНБО України потребує розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені стосовно державних та інших інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідного розмежування підслідності.

Зважаючи на «гібридну війну» Російської Федерації проти України, значно зросла кількість та потужність кібератак через несанкціоноване втручання в роботу державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури, що несуть загрозу національній безпеці України.

На ефективність протидії вказаним загрозам впливає відсутність кримінально-процесуальних важелів впливу Служби безпеки України на сферу таких злочинів, які наносять значну шкоду державній безпеці України.

Для створення умов безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави необхідним є посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері, забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме

негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Законопроект спрямовано на стримання злочинів у сфері інформатизації та зв'язку, які загрожують національній безпеці нашої країни, завдають реальної шкоди і значних матеріальних збитків, а також сприяють встановленню більш чітких умов діяльності слідчих відповідних органів досудового розслідування.

2. Мета і шляхи її досягнення

Метою законопроекту є розроблення і впровадження правових механізмів кіберзахисту, спрямованих на формування ефективної національної системи кібербезпеки.

3. Правові аспекти

Предмет правового регулювання запропонованого проекту Закону України належить до інформаційно-телекомунікаційної сфери діяльності та сфери національної безпеки і оборони України. У цій сфері правового регулювання діють:

Конституція України;

Кримінальний кодекс України;

Кримінальний процесуальний кодекс України.

4. Фінансово-економічне обґрунтування

Реалізація закону не потребує додаткових матеріальних та інших витрат.

5. Позиція заінтересованих органів

Законопроект погоджено без зауважень: Міністерством економічного розвитку і торгівлі України, Міністерством фінансів України, Міністерством внутрішніх справ України, Службою безпеки України, Державним агентством з питань електронного урядування та із зауваженнями Міністерством юстиції України, які враховано повністю.

Міністерством юстиції України проведено правову експертизу та погоджено без зауважень.

6. Регіональний аспект

Законопроект не стосується питання розвитку адміністративно-територіальних одиниць.

6[1]. Запобігання дискримінації

Положень, які містять ознаки дискримінації, у законопроекті немає.

7. Запобігання корупції

У законопроекті немає правил і процедур, які можуть містити ризики вчинення корупційних правопорушень.

8. Громадське обговорення

Законопроект не потребує проведення консультацій з громадськістю.

8[1]. Розгляд Науковим комітетом Національної ради України з питань розвитку науки і технології.

Законопроект не потребує розгляду Науковим комітетом Національної ради України з питань розвитку науки і технології.

9. Позиція соціальних партнерів

Законопроект не потребує погодження із соціальними партнерами.

10. Оцінка регуляторного впливу

Законопроект не є регуляторним актом.

10[1]. Вплив реалізації акта на ринок праці

Реалізація закону не впливає на ринок праці.

11. Прогноз результатів

Прийняття закону сприятиме захисту державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури від кіберзагроз, кібератак та кіберзлочинів, дозволить запровадити сукупні заходи організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямовані на захист національної системи кібербезпеки.

Голова Державної служби спеціального
зв'язку та захисту інформації України Леонід Євдоченко

26 03 2018 р.