



ВЕРХОВНА РАДА УКРАЇНИ

Комітет з питань правоохоронної діяльності

01008, м.Київ-8, вул. М. Грушевського, 5, тел.: 255-35-06

ВЕРХОВНА РАДА УКРАЇНИ

Комітет з питань правоохоронної діяльності на виконання доручення Голови Верховної Ради України Д. Разумкова та відповідно до статті 16 Закону України «Про комітети Верховної Ради України» розглянув на своєму засіданні 23 грудня 2020 року (протокол № 54) проект Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання інформаційно-телекомунікаційних (автоматизованих) систем, телекомунікаційних мереж та об'єктів критичної інформаційної інфраструктури» (**реєстр. № 3897 від 17.07.2020р.**), поданий народним депутатом України Федієнком О.П. та іншими народними депутатами України.

Метою законопроекту, як зазначено в пояснювальній записці до нього, є розроблення і впровадження правових механізмів кіберзахисту, спрямованих на формування ефективної національної системи кібербезпеки, вдосконалення норм чинного законодавства у частині запровадження посиленої кримінальної відповідальності за злочини, вчинені щодо об'єктів критичної інформаційної інфраструктури, державних інформаційних ресурсів, а також закріплення підслідності зазначених кримінальних правопорушень за слідчими органів безпеки України.

Законопроект передбачає низку змін до розділу XVI Особливої частини Кримінального кодексу України (далі – КК України), які, загалом, полягають у наступному:

1) термінологічні зміни в назві вищезазначеного розділу, а також у статтях 361, 361¹, 361², 362, 363, 363¹ КК України з метою приведення їх положень у відповідність до сучасних термінів, що застосовуються у законодавстві про телекомунікації та кібербезпеку;

2) запровадження нових кваліфікованих видів таких злочинів, як:

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в інформаційно-телекомунікаційних (автоматизованих) системах або на носіях такої інформації (стаття 361² КК України);

- несанкціоновані дії з інформацією, яка оброблюється в інформаційно-телекомунікаційних (автоматизованих) системах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 КК України);

3) посилення караності кримінальних правопорушень, передбачених статтями 361, 361¹, 361², 362, 363, 363¹ КК України у частині мінімальних та максимальних меж покарання у вигляді штрафу;

4) доповнення статей 361² та 362 КК України новими частинами, які посилюють відповідальність у випадку вчинення відповідних діянь щодо об'єктів критичної інформаційної інфраструктури;

5) поширення сфери дії статті 363 КК України на випадки порушення вимог до кіберзахисту;

6) доповнення кримінального закону новою статтею 363², що встановлює караність посягання на державний інформаційний ресурс або іншу інформацію, вимога щодо захисту якої встановлена законом, комунікаційну чи технологічну систему об'єкту критичної інфраструктури.

Крім того, змінами до Кримінального процесуального кодексу України (далі – КПК України) розслідування злочинів, вчинених щодо об'єктів критичної інформаційної інфраструктури, віднесено до підслідності Служби безпеки України.

В ході обговорення законопроекту народні депутати України – члени Комітету дійшли думки, що законодавча ініціатива, що спрямована на термінологічне осучаснення законодавчих положень у частині нормативної регламентації кримінальної відповідальності за злочини, вчинені у сфері використання інформаційно-телекомунікаційних (автоматизованих) систем, телекомунікаційних мереж, заслуговує на підтримку.

Водночас, не зважаючи на те, що посилення рівня захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів від кіберзагроз та кібератак продовжує залишатися актуальним, більшість положень законопроекту потребують суттєвого доопрацювання з огляду на наступне.

Назва законопроекту не повною мірою відповідає його змісту. Так, у назві законопроекту йдеться виключно про «розмежування підслідності злочинів, вчинених у сфері використання інформаційно-телекомунікаційних (автоматизованих) систем, телекомунікаційних мереж та об'єктів критичної інформаційної інфраструктури».

Тобто, фактично йдеться про відповідні зміни до статті 216 КПК України. У той же час більшість положень законопроекту стосується саме внесення змін до розділу XVI Особливої частини КК України, у якому передбачені кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Законопроектом пропонується доповнити КК України новою статтею 363², в якій встановити відповідальність за посягання на державний інформаційний ресурс або іншу інформаційну, комунікаційну чи технологічну систему об'єкта критичної інфраструктури шляхом застосування засобів електронних комунікацій.

Положення запропонованої редакції цієї статті структурно занадто ускладнені. Зокрема, ця стаття містить п'ять частин. Разом з тим частини перша і третя передбачають відповідальність за одні й ті ж дії за певних кваліфікуючих ознак.

Крім того, у частинах другій та четвертій вказано однакові кваліфікуючі ознаки. Прикладом зайвого ускладнення цієї норми є викладення однакових кваліфікуючих ознак «повторність вчинення, попередня змова, заподіяння значної шкоди» при вчиненні аналогічних складів злочинів.

Відповідно до диспозиції частини третьої та четвертої статті 361² КК України (у редакції проекту) предметом даного складу злочину є «інформація з обмеженим доступом, яка обробляється на об'єктах критичної інформаційної інфраструктури».

Використане поняття «інформація з обмеженим доступом» у контексті частини третьої та четвертої статті 361² КК України потребує конкретизації, оскільки, її використання призведе до неоднозначного тлумачення поняття даного виду інформації та до конкуренції з іншими складами кримінальних або ж адміністративних правопорушень (зокрема, зі статтями 111 (Державна зрада), 114 (Шпигунство), 328 (Розголошення державної таємниці), 330 (Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни) КК України та статтями 212² (Порушення законодавства про державну таємницю), частини третьої статті 186³ (Порушення порядку подання або використання даних державних статистичних спостережень) Кодексу України про адміністративні правопорушення).

Виділення в якості кваліфікуючої ознаки об'єктів критичної інформаційної інфраструктури у контексті статей 361² та 362 КК України (у редакції проекту) позбавлене сенсу, адже внаслідок наявності наслідку у вигляді «заподіяння значної шкоди» у диспозиції чинної статті 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється) КК України, а також того, що порушення експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, стосується будь-яких об'єктів інформаційної інфраструктури.

Тобто, склад злочину, передбачений чинною статтею 363 КК України, фактично охоплює такі ж самі дії, вчинені стосовно об'єктів критичної інформаційної інфраструктури.

Законопроектом встановлено, що об'єктом кримінальних правопорушень, передбачених запропонованими статтями 361² та 362 КК України є інформація, що обробляється або зберігається на об'єктах критичної інформаційної інфраструктури.

Відповідно до частини третьої статті 4 (Об'єкти кібербезпеки та кіберзахисту) Закону України «Про основні засади забезпечення кібербезпеки України» порядок формування переліку об'єктів критичної інформаційної інфраструктури, перелік таких об'єктів та порядок їх внесення до державного реєстру об'єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об'єктів

критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.

Однак, на цей час перелік об'єктів критичної інформаційної інфраструктури не визначено, а постановою Кабінету Міністрів України від 19.06.2019 № 518 затверджено лише загальні вимоги до кіберзахисту об'єктів критичної інфраструктури.

Згідно з кримінальною доктриною норми кримінального права не можуть передувати нормам матеріального права, а відповідно передбачати в кримінальному законодавстві норми, що криміналізують, для прикладу несанкціонований збут або розповсюдження створеної та захищеної відповідно до чинного законодавства інформації з обмеженим доступом, яка обробляється на об'єктах критичної інформаційної інфраструктури, потрібно після затвердження переліку таких об'єктів.

Дискусійною є пропозиція законопроекту щодо розмежування підслідності злочинів, передбачених різними частинами однієї статті КК України, за різними органами досудового розслідування. На практиці це неминуче призведе до процесуальної невизначеності та плутанини. При цьому, слід ураховувати, що у структурі Національної поліції України діє Департамент кіберполіції, до основних завдань якого належить саме розкриття та розслідування злочинів у вказаній сфері.

Також, законопроект потребує доопрацювання в частині визначення термінології, використаної у статті 363² КК України, згідно якої злочином є «умисні дії в кіберпросторі та/або з його використанням, які здійснюються шляхом застосування засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) для впливу на державний електронний інформаційний ресурс, інформацію, вимога щодо захисту якої встановлена законом, з метою порушення конфіденційності, цілісності, доступності державного електронного інформаційного ресурсу, інформації, вимога щодо захисту якої встановлена законом, отримання несанкціонованого доступу до таких ресурсів (інформації), що призвело до витоку, втрати, підробки, блокування ресурсу (інформації), спотворення процесу обробки ресурсу (інформації) або до порушення встановленого порядку їх маршрутизації».

Застосоване у назві та диспозиції статті 363² КК України поняття «державний електронний інформаційний ресурс» не відповідає положенням чинного законодавства України, оскільки на сьогодні функціонує Національний реєстр електронних інформаційних ресурсів, це державний репозитарій, який створено для обліку всіх електронних інформаційних ресурсів держави: електронних реєстрів, кадастрів, класифікаторів, а також - інформаційних систем, які забезпечують їх функціонування та використовують інформацію з них.

Тому, застосування понять, що не відповідають положенням діючих нормативних актів, неминуче призведе до довільного їх тлумачення стороною

захисту в судовому провадженні та висунення тверджень щодо зміни кваліфікації за статтею 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України, визнання зібраних доказів недопустимими, у зв'язку з порушенням правил підслідності, визначеними статтею 216 КПК України .

У частині п'ятій статті 363² КК України пропонується за вчинення вказаних дій, якщо вони спричинили тяжкі наслідки, встановити відповідальність у виді позбавлення волі на строк від 10 до 15 років з конфіскацією майна. Натомість, проект не містить визначення, що слід розуміти під «тяжкими наслідками» при вчиненні цього злочину.

Загалом, не можна погодитися із пропозицією авторів законопроекту щодо встановлення за вчинення вказаних дій покарання у виді конфіскації майна.

Так, відповідно до вимог статті 59 КК України конфіскація майна як вид покарання встановлюється за тяжкі та особливо тяжкі корисливі злочини, а також за злочини проти основ національної безпеки України та громадської безпеки незалежно від ступеня їх тяжкості і може бути призначена лише у випадках, спеціально передбачених в Особливій частині КК України.

Проте запропонований склад не містить обов'язкового корисливого мотиву та розміщуватиметься у розділі XVI КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Отже, застосування конфіскації майна за вчинення цих дій не кореспондується з положеннями Загальної частини КК України.

На думку Комітету, не обґрунтованим є суттєве підвищення розмірів покарання у виді штрафу за вчинення кримінальних правопорушень, передбачених частинами першими статтями 361, 361¹, 361², 362, 363, 363¹ КК України.

До того ж окремі санкції положень розділу XVI Особливої частини КК України, які пропонуються посилити в законопроекті, були нещодавно підвищені Законом України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень» № 2617-УІІ від 22.11.2018 року. Тобто, не зрозумілою є необхідність посилювати їх ще раз (причому не кардинально), якщо від 1 липня 2020 року минуло лише декілька місяців.

Також, додаткового обґрунтування потребує пропозиція авторів законопроекту щодо встановлення однакового розміру покарання у виді штрафу для кримінальних правопорушень, передбачених частинами першими статей 361, 361¹, 361², 362, 363¹ КК України (від трьох тисяч до п'яти тисяч неоподатковуваних мінімумів доходів громадян). Адже, у разі прийняття цієї пропозиції суд (суддя) за вчинення різних за ступенем та характером суспільної небезпеки кримінальних правопорушень буде змушений призначати покарання у виді штрафу більш-менш однакового розміру, що є неприйнятним.

Про необхідність ґрунтовного доопрацювання законопроекту зазначають правоохоронні органи, експерти міністерств і відомств, а також науковці.

Зокрема, Міністерство внутрішніх справ України та Національна поліція України висловили низку критичних зауважень до законопроекту та вважають, що законопроект потребує суттєвого доопрацювання.

Верховний Суд у своєму висновку зазначив, що редакції кримінально-правових норм нових статей 363³ та 363² КК України викликають зауваження, ускладнюють однозначне розуміння та правозастосування. Також, потребує свого доопрацювання і запропонована термінологія розділу XVI Особливої частини КК України.

Офіс Генерального прокурора, Національне антикорупційне бюро України, Державне бюро розслідувань, Уповноважений Верховної Ради України з прав людини висловили низку критичних та доречних зауважень до законопроекту та вважають, що він потребує доопрацювання.

Міністерство юстиції України, Національний інститут стратегічних досліджень, Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів повідомили про відсутність зауважень та пропозицій до законопроекту.

Служба безпеки України повідомила про відсутність заперечень щодо запровадження кримінальної відповідальності за вчинення передбачених законопроектом діянь та віднесення нових кримінальних правопорушень до підслідності слідчих органів безпеки України.

Водночас, СБУ пропонує впровадити кримінальну відповідальність окремими статтями Особливої частини КК України, а не окремими частинами статей (нові частини 3 і 4 статті 361², частини 4 і 5 статті 362), як, наразі, пропонується законопроектом.

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації зазначає про підтримку законопроекту та доцільність його прийняття.

Інститут законодавства Верховної Ради України, Національний юридичний університет імені Ярослава Мудрого, Київський національний університет імені Тараса Шевченка, Національна академія внутрішніх справ, визнаючи необхідність удосконалення правових підстав відповідальності за посягання на об'єкти критичної інфраструктури та державних інформаційних ресурсів, вважають, що дана законодавча пропозиція потребує доопрацювання. Крім того, вказується на необхідність ґрунтового техніко-юридичного доопрацювання законопроекту, корегування відповідних термінів тощо.

Науково-дослідний інститут вивчення проблем злочинності імені академіка В. В. Сташиса підтримує запровадження спеціальної кримінальної відповідальності за суспільно небезпечні посягання на інформаційно-телекомунікаційні системи суспільного та державного значення, а також запровадження кваліфікації нових видів злочинів; віднесення розслідування даних злочинів до підслідності Служби безпеки України.

Головне науково-експертне управління Апарату Верховної Ради України у своєму висновку висловило низку критичних зауважень щодо змісту законопроекту та окремих його статей.

Комітет Верховної Ради України з питань цифрової трансформації надав свій висновок до законопроекту та рекомендує Верховній Раді України прийняти за основу законопроект реєстр. № 3897 з урахування зауважень висловлених до нього.

Комітет Верховної Ради України з питань бюджету зазначив, що законопроект за реєстр. № 3897 має опосередкований вплив на показники бюджету (може призвести до збільшення доходів та видатків державного бюджету залежно від санкцій за вчинені правопорушення) та, у разі, прийняття відповідного закону він може набирати чинності згідно із законодавством.

Враховуючи вищезазначене та результати обговорення законопроекту Комітет, керуючись положеннями пункту 3 частини першої статті 114 Регламенту Верховної Ради України, рекомендує Верховній Раді України проект Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання інформаційно-телекомунікаційних (автоматизованих) систем, телекомунікаційних мереж та об'єктів критичної інформаційної інфраструктури» (реєстр. № 3897) за наслідками розгляду в першому читанні **повернути суб'єктам законодавчої ініціативи на доопрацювання.**

Доповідачем від Комітету на пленарному засіданні Верховної Ради України визначено народного депутата України – заступника голови Комітету з питань правоохоронної діяльності Михайлюк Галину Олегівну.

Проект постанови Верховної Ради України та необхідні матеріали додаються.
Просимо розглянути.

Голова Комітету

Д. Монастирський



СЕДО ВЕРХОВНОЇ РАДИ УКРАЇНИ

Підписувач: Монастирський Денис Анатолійович
Сертифікат: 58E2D9E7F900307B04000000ACDE2E00E7788200
Дійсний до: 16.03.2022 0:00:00

Апарат Верховної Ради України
№ 04-27/3-2020/1261 від 04.01.2021



305768