

Також набув подальшого розвитку метод оцінки ефективності роботи криптосистем, який за рахунок співвідношення складності атаки на системи в елементарних операціях обчислювальної техніки до ймовірності успішної реалізації атаки дозволяє визначити границі для відносної ефективності системи захисту інформації в АС переробки та управління КВОІ в умовах кібернетичних атак.

Література:

1. Наговицин А.И., Севрюков А.Г. Робототехнические комплексы военного назначения, опыт и перспективы их применения в РВиА СВ // Известия Южного федерального округа, – 2016, – с. 197-210.
2. Сашников Т.К. К вопросу обеспечения информационной безопасности беспилотных авиационных систем с летательными аппаратами малого и лёгкого класса в специализированных АСУ // Журнал Т-Comm - Телекоммуникации и Транспорт, – 2013, №6, – с. 71-72.
3. Харченко В.С. Гарантоспособность и гарантоспособные системы: элементы методологии // Радиоелектронні і комп'ютерні системи, – 2006, №5 (7), – с. 7-19.

Щодо визначення кіберзлочину

Ржеуцька М.О.

курсант 2-го курсу факультету підготовки
фахівців для підрозділів Національної поліції
Донецького юридичного інституту МВС України

Данилевський А.О.

кандидат юридичних наук, доцент
доцент кафедри кримінально-правових дисциплін та судових експертиз
Донецького юридичного інституту МВС України,

Із посиленням інформатизації суспільства, коли комп'ютерні технології заповнили майже всі сфери життєдіяльності суспільства, проблема комп'ютерних злочинів набуває особливої актуальності, адже із розвитком технологій, які несуть за собою позитивні зміни у житті, зручні сервіси, вільний доступ до великої кількості інформації тощо, приходять і негативні явища, такі як кіберзлочини. Останні події, пов'язані із розповсюдженням шкідливих програм «WannaCry» та «Petya» показали, що жодна країна не може вважати себе захищеною від кіберзагроз, для кіберзлочинців немає кордонів, тож протидія злочинності у цій сфері є пріоритетним завданням не тільки нашої держави, а й усієї світової спільноти. З метою об'єднання зусиль держав у цій сфері було прийнято Конвенцію про кіберзлочинність, ратифіковану Україною у 2005 році. Велике значення для ефективної протидії має термінологічна визначеність у сфері протидії зазначеним злочинам, зокрема визначення поняття кіберзлочину.

Проблеми кіберзлочинності розглядали у своїх роботах Д.С. Азаров, Ю.М. Батурин, М.В. Карчевський, А.А. Музика, Н.А. Савінова, Є.Д. Скулиш, М.В. Рудик, К.В. Юртаєва та інші. Проте розвиток суспільних відносин та законодавства у цій сфері обумовлює необхідність подальших досліджень, спрямованих, зокрема, на уточнення поняття кіберзлочину.

Метою цієї роботи є аналіз законодавчого визначення поняття кіберзлочину.

Довгий час поняття кіберзлочину було суто кримінологічним, адже визначення цього терміну у законодавстві не наводилося. Але ситуація змінилась у зв'язку з прийняттям Закону України «Про основні засади кібербезпеки України» від 05.10.2017 № 2163-VIII, у статті 1 якого наводиться наступне визначення: кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Як бачимо, за основу законодавець взяв визначення злочину, передбачене у частині 1 статті 11 КК України, зазначивши специфічні риси такого виду злочину – місце його вчинення (кіберпростір) та/або використання кіберпростору як засобу. Разом з тим порівняння законодавчого визначення кіберзлочину із визначенням злочину настановує на цікаві висновки.

1. На відміну від визначення злочину у частині 1 статті 11 КК України для кіберзлочину не вказана така ознака як вчинення його суб'єктом злочину. Або про таку ознаку просто забули, або законодавець зробив це свідомо, маючи на увазі, що такий злочин може бути вчинений не тільки фізичною осудною особою, яка вчинила злочин у віці, з якого може наставати кримінальна

відповідальність, й іншими суб'єктами, які будуть притягатись до кримінальної відповідальності (юридичні особи або «штучний інтелект»). Але тоді таку законодавчу новелу необхідно узгоджувати із положеннями Загальної частини КК України.

2. Відповідно до наведеного визначення кіберзлочину, відповідальність за його вчинення передбачена законом України про кримінальну відповідальність. Словосполучення «закон України про кримінальну відповідальність» використовує зокрема КПК України (стаття 3) для позначення законодавчих актів, які встановлюють кримінальну відповідальність (КК України та закону України про кримінальні проступки). Такий підхід враховує останні тенденції розвитку законодавства у сфері кримінальної юстиції. Проте на відміну від КПК, який оперує поняттям «кримінальне правопорушення», законодавець назвав відповідне діяння саме злочином. Чи свідчить це про те, що серед кримінальних проступків, які повинні бути запроваджені у кримінальне законодавство найближчим часом не буде посягань у кіберпросторі та/або з його використанням? На нашу думку, ні, адже у чинній редакції Розділу XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» достатньо злочинів невеликої тяжкості, які є першими претендентами на переведення у категорію кримінального проступку. Тому більш доцільно було використовувати термінологічний зворот на кшталт «кримінальне кіберправопорушення».

3. З аналізу визначення кіберзлочину можна зробити висновок, що ним може визнаватись діяння, відповідальність за яке не передбачена законом України про кримінальну відповідальність, але яке визнається злочином міжнародними договорами України. Таке положення прямо суперечить положенням частини 3 статті 3 КК України, де зазначається, що злочинність діяння, а також його караність та інші кримінально-правові наслідки визначаються тільки КК України.

4. Початок визначення свідчить про те, що законодавець визнає синонімічними словосполучення «кіберзлочин» та «комп'ютерний злочин». Така позиція підтримується деякими дослідниками [2, с. 222]. Проте більшість дослідників із цим не погоджується і розуміє поняття кіберзлочину значно ширше. Як правило, дослідники, посилаючись на X Конгрес ООН з попередження злочинності і поведження із правопорушниками, пов'язаними з комп'ютерами та комп'ютерними мережами, кіберзлочин розуміють у двох значеннях: 1) у вузькому сенсі (комп'ютерний злочин) – будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є безпека комп'ютерних систем і оброблюваних ними даних; 2) у широкому розумінні (як злочин, пов'язаний з комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж [3, с. 49; 4; 5, с. 146]. Як бачимо, у Законі України «Про основні засади кібербезпеки України» законодавець вклав у це поняття найбільш вузьке розуміння, що навряд чи відповідає усталеному розумінню таких злочинів і положенням міжнародних нормативно-правових актів, зокрема, згадана Конвенція про кіберзлочинність вкладає у це поняття значно ширший зміст, адже передбачає відповідальність за діяння, що вчиняються не тільки у кіберпросторі або з його використанням [6]. Під таке визначення підпадає навіть далеко не кожне злочинне діяння, відповідальність за яке передбачено у Розділі XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Враховуючи викладене можна зробити наступні висновки. Визначення кіберзлочину у законодавстві України є важливим кроком, який спрямований на усунення розбіжностей щодо уявлення про таке явище та ефективну протидію йому, проте таке визначення суперечить окремим положенням кримінального законодавства, положенням міжнародних нормативно-правових актів а також тенденціям розвитку законодавства у сфері кримінальної юстиції. Це свідчить про необхідність подальших досліджень у цій сфері та вдосконалення законодавства.

Література:

1. Про основні засади кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII [Електронний ресурс] // Сайт «Законодавство України». – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/2163-19>.
2. Правдюк С.А. Комп'ютерні правопорушення та інформаційні правопорушення: аспекти співвідношення / С.А. Правдюк // Науковий вісник Національного університету біоресурсів і природокористування України. – 2013. – Вип. 182. – Ч. 3. – с. 216-223.
3. Скулиш Є.Д. Теоретико-методологічні засади визначення об'єкта та предмета кіберзлочинів / Є.Д. Скулиш // Правова інформатика. – 2014. – № 2. – с. 47-53.

4. Тропина Т.Л. Киберпреступность : понятие, состояние, уголовно-правовые меры борьбы [Електронний ресурс] / Т. Л. Тропинина // Сайт Владивостокського центру дослідження організованої злочинності. – Режим доступу : <http://www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb=1&pb=1>.
5. Грицун О.О. Кримінальний аспект міжнародної інформаційної безпеки / О. О. Грицун // Право і суспільство. – 2015. – № 6. – Ч. 2. – с. 142-147.
6. Конвенція про кіберзлочинність // Офіційний вісник України. – 2007. – № 65. – Ст. 2535.

Питання термінології у визначенні системи злочинів в сфері ІТ (досвід інших держав)

Дмитрук М.М.

кандидат юридичних наук, доцент
доцент кафедри кримінального права

Національного університету «Одеська юридична академія»

5 жовтня 2017 р. Президентом України підписано Закон України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [1]. Прийняття вказаного закону покращує правове регулювання протидії кіберзлочинності, визначає окремі поняття, які мають безпосереднє відношення і до законодавства про кримінальну відповідальність, проте взаємозв'язок та взаємовплив вказаного акту із КК України залишився достатньо примарним.

У п. 8, ст. 1 вказаного законодавчого акту надано визначення «кіберзлочину» (комп'ютерного злочину), яким визначається, суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. Поряд із цим, сам КК України не містить згадки про поняття кіберзлочину або комп'ютерного злочину, а сама система злочинів у Розділі XVI О. ч. КК України іменується як «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Питання термінології злочинів, які посягають на суспільні відносини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку досліджувалось вченими неоднократно, проте узагальнена позиція з цього питання не сформована.

Так, М.В. Карчевський зазначає: «Поняття «комп'ютерний злочин» та «кіберзлочин», в загальновизнаному розумінні можуть бути ефективно використані при проведенні кримінологічних, кримінально-процесуальних, криміналістичних досліджень. Що ж стосується національного кримінально-правового дискурсу, то тут застосування цього поняття слід обмежити, і використовувати запропоноване поняття «злочини в сфері використання інформаційних технологій» [2, с. 14]. При цьому вчений у якості доводів аналізує поняття «злочини у сфері ІТ», «інформаційна безпека» та приходить до висноку: «Таким чином, злочини в сфері використання інформаційних технологій, є одним з видів злочинів в сфері інформаційної безпеки, є передбачені КК України, суспільно небезпечні, винні, вчинені суб'єктом злочину діяння, які заподіюють шкоду, забезпеченим засобами обчислювальної техніки, відносинам у сфері реалізації інформаційної потреби. Аналіз чинного КК дозволяє прийти до висновку, що до таких злочинів слід відносити посягання, передбачені ст. ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 КК [2, с. 11]. Вказане твердження М.В. Карчевського щодо віднесення до «злочинів в сфері використання ІТ» належать виключно вказані діяння залишається необґрунтованим. Якщо погодитись із вказаним вченим, то виходить, що порушення авторських та суміжних прав, яке здійснюється шляхом втручання в роботу ЕОМ не заподіює шкоду «відносинам у сфері реалізації інформаційної потреби» і не вчиняється за допомогою саме «засобів обчислювальної техніки». Проте ситуація є зовсім протилежною. Інші доводи із боку вказаного вченого наведено на користь позначення злочинів передбачених у Розділі XVI О. ч. КК України як «злочинів в сфері використання ІТ» не наведено.

Для етимологічного розуміння, що таке «інформаційна технологія» і чи можна систему злочинів передбачених в Розділі XVI О. ч. КК України визначити як «злочини в сфері інформаційних технологій» розглянемо що таке «інформаційні технології».

«Інформаційна технологія», згідно ст. 1 ЗУ «Про Національну програму інформатизації», – це цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування