DOI https://doi.org/10.30525/978-9934-26-493-1-50

ADVANCED ACHIEVEMENTS IN THE FIELD OF LEGAL REGULATION OF UNAUTHORIZED INTERFERENCE IN COMPUTER NETWORKS: THE VIEW OF DOMESTIC AND FOREIGN SCIENTISTS

ПЕРЕДОВІ ДОСЯГНЕННЯ У СФЕРІ ПРАВОВОГО РЕГУЛЮВАННЯ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В КОМП'ЮТЕРНІ МЕРЕЖІ: ПОГЛЯД ВІТЧИЗНЯНИХ ТА ЗАРУБІЖНИХ ВЧЕНИХ

Dryzhakova D. Yu.
Postgraduate Student at the Department of Criminal Law Policy and Criminal Law
Taras Shevchenko Kyiv National University
Kyiv, Ukraine

Дрижакова Д. Ю.
аспірантка кафедри кримінально-правової політики та кримінального права
Київський національний університет імені Тараса Шевченка
м. Київ, Україна

З розвитком технологій та все більшою залежністю суспільства від цифрових систем, питання кібербезпеки набуває все більшої актуальності. Несанкціоноване втручання в комп'ютерні мережі стає серйозною загрозою для державної безпеки, економіки та приватного життя громадян. Саме тому правове регулювання цієї сфери постійно розвивається, а вчені з усього світу шукають ефективні рішення для боротьби з кіберзлочинністю.

Проблематиці боротьби з кіберзлочинністю присвячено праці М. О. Будакова, В. М. Бутузова, М. Вертузаєвої, М. М. Галамби, Р. А. Калюжного, В. В. Коваленко, Я. Ю. Кондратьєва, Б. А. Кормича, Ю. М. Максименка, В. В. Маркова, А. І. Марущака, Г. В. Новицького, Ю. М. Онищенка, О. В. Орлова, А. Л. Осипенко, Т. Л. Сироїд, В. С. Сідак, Р. Ю. Сень, І. М. Сопілко та інших. Проте питання особливостей правового регулювання боротьби із кіберзлочинністю у США та шляхів запозичення позитивного досвіду в практику України потребує більш комплексного та деталізованого підходу, що і зумовлює актуальність обраної теми дослідження.

У 2003 році Н.А. Розенфельд здійснила дисертаційне дослідження на тему: «Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». Дисертація присвячена теоретичним та

практичним питанням застосування кримінально-правової норми, що передбачає відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж в Україні. Досліджений юридичний склад злочину, передбаченого ст. 361 КК України, види, співвідношення аналізованих злочинів з іншими злочинами та критерії їх відмежування від суміжних складів злочинів, питання кваліфікації за сукупністю з іншими злочинами, а також нормативно-правові та міжнародно-правові заходи захисту від таких злочинів[1, с. 126–127].

М.В. Карчевським у дисертації «Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)» розкрито кримінально-правовий зміст інформаційних відносин у сфері використання комп'ютерної техніки як родового об'єкта злочинів, передбачених розділом XVI КК України, обґрунтовано пропозицію про доцільність визначення їх загальним терміном «комп'ютерні злочини». На підставі визначення родового об'єкта розкрито зміст безпосереднього об'єкта незаконного втручання як суспільних відносин власності на комп'ютерну інформацію [2, с. 67]. Відповідно по-новому визначено комп'ютерну інформацію як предмет цього злочину і надано пропозиції щодо недоцільності передбачення в диспозиції ст. 361 КК України вказівки на носії інформації як самостійний предмет незаконного втручання. Визнано необґрунтованим передбачення комп'ютерного вірусу в ч. 1 ст. 361 КК України як самостійного предмета злочину. Замість цього запропоновано визначити предметами незаконного втручання програмні та технічні засоби, призначені для незаконного втручання, до яких відносяться комп'ютерні віруси. По-новому визначено знищення та перекручення комп'ютерної інформації як різні форми порушення права власності на комп'ютерну інформацію. Автором вперше у вітчизняній науці здійснено спробу класифікації способів незаконного втручання, що має важливе значення для встановлення об'єктивної сторони та ступеня суспільної небезпечності злочину, що досліджується. Доведено необхідність доповнення ч. 2 ст. 361 КК України кваліфікуючими ознаками, як «вчинення незаконного втручання шляхом несанкціонованого доступу до комп'ютерної інформації» та «вчинення незаконного втручання особою, яка має доступ до роботи на ЕОМ», у системі чи комп'ютерній мережі зважаючи виконувану роботу або посадою, яку займає особа. Обґрунтовано необхідність доповнення ст. 361 КК України частиною 3, яка б передбачала відповідальність за незаконне втручання, що спричинило тяжкі наслідки, та розкрито зміст таких наслідків. Запропоновано нову редакцію ст. 361 КК України «Незаконне

втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» [2, с. 67].

О.Д. Ричкою у дисертації «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» розкрито особливості кримінально-правової кваліфікації у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено засади здійснення кримінально-правової кваліфікації. Окреслено ознаки, притаманні даній категорії злочинної діяльності. Визначено ознаки кібернетичних злочинів. Висвітлено ґенезу та поняття злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Досліджено різновиди як міжнародних, так і національних кібернетичних злочинів. Проведено комплексний аналіз елементів складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено об'єкт і предмет 17 кібернетичних злочинів, здійснено аналіз та розкрито зміст об'єктивної сторони; встановлено суб'єктів та досліджено особливості суб'єктивної сторони злочинів даної категорії. Розглянуто кваліфікуючі ознаки та здійснено їх відмежування від суміжних складів, на підставі чого сформовано нововведення та доповнення до чинного законодавства України з питань здійснення кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [3, с. 78–79].

Законом «щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 р. № 2149-IX, який набрав чинності 3 квітня 2022 р., внесені зміни до КК України.

У статтях 361 і 361-1 КК слова «електронно-обчислювальні машини (комп'ютерів), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку» замінені словами «інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі» – з метою приведення термінології КК у цій частині у відповідність до термінології Закону «Про електронні комунікації» від 16 грудня 2020 р. № 1089-IX й іншого законодавства України у сфері кібербезпеки.

Наслідки у виді «витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації», що були передбачені в ч. 1 ст. 361 КК, з цієї частини виключені і визначені у новій частині 3 ст. 361 КК.

При цьому злочин, передбачений ч. 1 ст. 361 КК, який карався, зокрема, позбавленням волі на строк до трьох років, трансформовано у кримінальний проступок.

Тут має місце помилка законодавця – надмірна криміналізація.

Так, саме по собі несанкціоноване втручання в роботу згаданих систем чи мереж не є кримінальним правопорушенням, оскільки не створює жодних наслідків, які можна було б охопити поняттям істотної шкоди (див. ст. 11 КК).

Наприклад, колега по роботі бажає подивитися новини з використанням ПК іншого працівника, поки свій в ремонті, включає його і робить пошук на сайтах. Це – малозначне діяння.

Статтю 361 КК доповнено новою частиною 5, в якій визначено особливо кваліфікований склад злочину: «Дії, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану».

Водночас ст. 361 КК доповнено новою частиною 6, в якій визначено: «Дії, передбачені частинами 1–4 цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж».

Т*ут також має місце помилка законодавця*: дії, передбачені частиною 5 ст. 361 КК, про яку не згадано у ч. 6 цієї статті, ніби слід визнавати злочином, навіть якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж. Насправді ні, адже згідно зі ст. 62 Конституції України, усі сумніви щодо доведеності вини особи тлумачаться на її користь. Довести ж вину особи у діянні, протиправність якого не визначена відповідно до принципу юридичної визначеності, неможливо [4].

Аналізуючи сучасні вітчизняні реалії, можна відзначити незавершеність даного процесу в Україні та потребу у подальших перетвореннях. За таких умов набуває актуальності вивчення позитивного досвіду США, що є цілком доцільним вектором розвитку досліджуваного інституту.

Сполучені Штати Америки, як держава, що зазнає значного негативного впливу від кіберзлочинців, та є однією із перших в історії, що зайнялась розробкою відповідних нормативно-правових актів є надзвичайно цікавою та вагомою для дослідження.

Серед норм Національної стратегії внутрішньої безпеки США, прийнятої в 2015 році, особливий інтерес представляє розділ «Кіберзахист», в якому наголошується на необхідності захисту від

кібератак у кіберпросторі. США, проголошуючи себе батьківщиною Інтернету, взяли на себе відповідальність перед усім мережевим світом за забезпечення безпеки в кіберпросторі. Окрім того, цією державою проголошено курс на посилення законодавчої бази та підвищення стандартів захисту прав та інтересів громадян [5, с. 12].

Найбільшу кількість нормативно-правових актів США у досліджуваній сфері прийнято щодо емісії цінних паперів, охорони інтелектуальної власності, захисту від несанкціонованого доступу до інформації, авторського права тощо [6, с. 25].

У 2001 році США було прийнято Закон «Про об'єднання та зміцнення США», згідно з нормами якого будь-яка дія, яка спричиняє порушення в роботі чи призводить до незаконного проникнення в комп'ютер, класифікується як тероризм. В свою чергу, провайдер зобов'язаний надати всю відому йому інформацію про користувача на першу вимогу Федерального бюро розслідувань [7]. Таким чином, на сьогодні вектор правового регулювання боротьби із кіберзлочинністю в США пов'язується із протидією кібертероризму як найнебезпечнішому прояву кіберзлочинності.

Деструктивна діяльність в кіберпросторі США карається значно жорсткіше, ніж у Європі. Так, у США визначено кримінальну відповідальність за неналежне зберігання та обробку персональної інформації чи її знищення у відмінному від встановленого законом способу. Для порівняння, у країнах ЄС кримінальні справи можуть порушуватися лише у випадку завдання шкоди державній безпеці та основним правам громадян [8, с. 126]. Це свідчить про те, що соціальним аспектом правового регулювання боротьби із кіберзлочинністю в США не знехтувано, оскільки величезне значення все ще має не лише захист державних інтересів, а й кожного окремого громадянина.

Правове регулювання несанкціонованого втручання в комп'ютерні мережі є динамічним процесом, який вимагає постійного оновлення. Вітчизняні та зарубіжні вчені роблять значний внесок у розвиток цієї галузі, пропонуючи нові підходи та рішення. Однак, для ефективної боротьби з кіберзлочинністю необхідна комплексна робота, яка включає в себе як законодавчі зміни, так і розвиток технологій та міжнародне співробітництво.

Література:

1. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. : дис. ... канд. юрид. наук. Київ. 222 с.

2. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : дис. ... канд. юрид. наук. Луганськ, 2002. 175 с.

3. Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. ... канд. юрид. наук. Ірпінь, 2019. 212 с.

4. Микола Хавронюк. Втручання в роботу інформаційно-комунікаційних систем: кримінальна відповідальність. Аналіз Закону «щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» із серії науково-практичних коментарів Миколи Хавронюка про зміни до Кримінального кодексу, прийняті під час воєнного стану. https://pravo.org.ua/blogs/vtruchannya-v-robotu-informatsijno-komunikatsijnyh-system-kryminalna-vidpovidalnist/

5. National Security Strategy. The White House, February 2015. Washington D. C., 2015. 29 p. URL: http://nssarchive.us/wp-content/uploads/2015/02/ 2015.pdf

6. Савчук Н. В. Світовий досвід державного регулювання ринку інтернет-по- слуг. *Формування ринкових відносин в Україні*. 2012. No 4. С. 24–28.

7. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism: USA PATRIOT ACT (Act of 2001). Public Law 107-56-OCT. 26, 2001. URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

8. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України.* 2013. No 3. С. 123–126.