CRIMINAL LAW AND CRIMINOLOGY. CRIMINAL AND PENAL LAW

DOI https://doi.org/10.30525/978-9934-588-92-1-73

НЕКАРАНІ ДІЇ ЗА КІБЕРАТАКИ НА САЙТИ ДЕРЖАВНИХ УСТАНОВ

Бондаренко М. С.
помічник судді
Касаційного кримінального суду у складі Верховного Суду,
здобувач
Державного науково-дослідного інституту
Міністерства внутрішніх справ України
м. Київ, Україна

Кримінальна відповідальність є найсуворішим видом юридичної відповідальності, яка може бути реалізована як наслідок вчинення винуватою особою злочину, що визначається як суспільно небезпечне діяння. Саме підвищений ступінь суспільної небезпечності діяння змушує законодавця до визнання певного діяння кримінально караним, з огляду на заподіяння істотної шкоди охоронюваним кримінальним законом суспільним відносинам або створення загрози заподіяння їм такої шкоди. Визнання вказаних діянь законодавцем злочинними та караними є відображенням об'єктивної необхідності суспільного життя.

Досить влучно з цього ж приводу висловився В. М. Кудрявцев. Так, він зазначав, що у підставі визнання того чи іншого вчинку або групи людських вчинків одиничним злочином, а таким чином й у підставі конструкції норми Особливої частини Кримінального кодексу України (далі – КК України), містяться соціальні властивості цих вчинків. До цих властивостей він відносив: поширеність, повторюваність, типовість та підвищену суспільна небезпечність саме такого комплексу діянь і шкідливих наслідків від них, що й мають відображатись у відповідній нормі кримінального закону [3, с. 218].

Є беззаперечним той факт, що кіберзлочин має відносну поширеність, але не набув масового характеру. Водночас є таким, що суперечить моральним принципам суспільства, оскільки вчинення, зокрема, кібератак на веб-сайти органів державної влади, заподіяння

шкоди або загроза її заподіяння об'єктам критичної інформаційної інфраструктури, не може визнаватися прийнятною нормою поведінки у суспільстві. Отже, підвищений ступінь суспільної небезпечності цих діянь має знайти адекватне відображення у нормах закону України про кримінальну відповідальність, але постає питання чи є караними дії за кібератаки на сайти державних установ?

Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року (далі – Закон) зроблені перші кроки законодавчого врегулювання щодо захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. У цьому ж Законі (п. 8 ч. 1 ст. 1) вперше й надано визначення кіберзлочину (комп'ютерному злочину), як суспільно небезпечного винного 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 [2].

Як передбачено ч. 3 ст. 3 КК України кримінальна протиправність діяння, а також його караність та інші кримінально-правові наслідки визначаються лише положеннями цього Кодексу [1].

Натомість в Особливій частині КК України передбачено лише шість статей, об'єднаних за родовим об'єктом у розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», за якими кримінально-караними є дії, пов'язані із несанкціонованим втручанням в роботу систем/мереж, створення та розповсюдження шкідливого програмного забезпечення, розповсюдження інформації з обмеженим доступом, несанкціоновані дії з інформацією всередині мережі, порушення правил експлуатації систем/мереж та перешкоджання роботі систем/мереж.

При цьому слід відзначити, що чинний закон України про кримінальну відповідальність не послуговується такими термінами як «кіберзлочин», «кібератака», «кібербезпека» та навіть таким розповсюдженим терміном як «комп'ютерний злочин».

А отже можна зауважити, погодившись із думкою О. В. Ободовського, який проаналізувавши праці вчених з соціології кримінального права, дійшов висновку, що певний вид поведінки особи можна назвати злочином лише у разі її передбачення законом про кримінальну відповідальність, тобто після законодавчої оцінки [4, с. 68].

Втім, на підставі згаданого Закону отримали подальшого розвитку й дії суб'єктів національної системи кібербезпеки у межах їх компетенції.

Відповідно до оперативної інформації, розміщеної на офіційному сайті Державної служби спеціального зв'язку та захисту інформації

України, щодо захисту державних інформаційних ресурсів, у період лише двох останніх місяців, з 12 серпня до 20 жовтня 2020 року, система захищеного доступу державних органів до мережі Інтернет заблокувала біля 1 982 114 різних видів атак. З цієї сукупності атак заблоковано було також 57 DDoS-атак, переважна більшість – на веб-ресурси Офісу Президента України [6].

За даними Служби безпеки України, опублікованими на офіційному сайті, вже за 9 місяців 2020 року нейтралізовано 460 кібератак і кіберінцидентів. За матеріалами кіберпідрозділів СБУ розпочато 408 кримінальних проваджень, з них лише 106 за злочини, передбачені розділом XVI КК України, а саме несанкціоноване втручання у роботу комп'ютерів та автоматизованих мереж (статті 361, 362, 363 КК України). Разом з тим, 42 кримінальні провадження було розпочато за статтями 109, 110 КК України (злочини проти основ національної безпеки України). Зазначено також про засудження 24 осіб у вказаний період [7].

З наведених статистичних даних вбачається проведення надоб'ємної роботи (і не лише вказаними вище суб'єктами національної системи кібербезпеки) у протидії таким суспільно небезпечним діянням як кібератаки. Однак, недосконалість норм кримінального закону призводить до неможливості проведення ефективного розслідування, можливого уникнення кримінальної відповідальності, притягнення до кримінальної відповідальності за іншими статтями Особливої частини КК України, хоча вчинені злочини можуть бути наслідком успішно реалізованої кібератаки тощо.

З найбільш відомих кібератак, вчинених в Україні, можна загадати: кібератаки на енергетичні компанії України в грудні 2015 року (вимкнення близько 30 підстанцій, 230 тисяч мешканців залишились без світла протягом 1-6 годин, загальний недовипуск електричної енергії); 6 грудня 2016 року атака на урядові сайти (Держказнайчейства та інших) та на внутрішні мережі державних органів (призвела до масштабних затримок бюджетних виплат); 18 травня 2017 року сталась перша масова кібератака вірусом XData, а 27 червня 2017 року – друга масштабна атака хробаком-винищувачем NotPetya, яка вразила майже 80% підприємств в Україні, а також перекинулась на підприємства закордоном (тривалий час після цього винні особи викрадали інформацію з підприємств та відкривали доступ іншим до комп'ютерних мереж) та ін. [8].

З огляду на що не варто применшувати ступінь суспільної небезпечності дій, спрямованих на вчинення кібератак, які потребують точного й конкретного відображення у нормі закону України про кримінальну відповідальність.

Насамкінець хотілось би наголосити, що не існує термінологічних непорозумінь з існуючими нормами кримінального закону, але наразі є доцільним розроблення певного законопроекту задля передбачення у КК України статей про кримінальну відповідальність за кіберзлочини. Зокрема й статей за кібератаки на сайти державних установ й об'єктів критичної інформаційної інфраструктури, це фактично буде процесом криміналізацією діянь іншого рівня, на відміну від передбачених чинним кримінальним законом.

Література:

1. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 22.10.2020).

2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 22.10.2020).

3. Основания уголовно-правового запрета: Криминализация и декриминализация/ П. С. Дагель, Г. А. Злобин, С. Г. Келина и др.; под ред. В. Н. Кудрявцева и А. М. Яковлева. Москва: Наука, 1982. 303 с.

4. Ободовський О. В. Триваючі злочини у кримінальному праві України: монографія / О. В. Ободовський. Одеса: Юридична література, 2016. 256 с.

5. Петров С. Г. Міжнародний досвід з протидії протиправним посяганням на державні електронні інформаційні ресурси. URL: http://www.academy.ssu.gov.ua/ua/page/page_1581082113.htm (дата звернення: 22.10.2020).

6. Оперативна інформація Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/filter?tagId=8151 (дата звернення: 22.10.2020).

7. 460 кібератак і 20 хакерських угруповань нейтралізувала СБУ з початку року. URL: https://ssu.gov.ua/novyny/460-kiberatak-i-20-khakerskykh-uhrupovan-neitralizuvala-sbu-z-pochatku-roku (дата звернення: 22.10.2020).

8. Перелік кібератак. URL: https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA (дата звернення: 22.10.2020).