УДК 343

Поліна Романівна Бортнік,
студентка 4 курсу юридичного факультету
Харківського національного університету імені В. Н. Каразіна

Ігор Сергійович Воєводін,
викладач кафедри міжнародного і європейського права
юридичного факультету Харківського національного
університету імені В. Н. Каразіна

Правова природа та сутність кіберзлочинності

Невідворотність глобалізаційних процесів призвела до появи принципово нового сприятливого середовища для вчинення кіберзлочинів. Даний вид суспільно-небезпечного діяння характеризується креативним підходом, інноваційними методами досягнення злочинної мети та високою латентністю.

Терміни «кіберзлочин» та «комп'ютерний злочин» дуже часто стоять поруч у науковій літературі, проте за своєю суттю не є синонімічними. Зокрема «кіберзлочин» є більш широким, в той час, як середовищем вчинення комп'ютерних злочинів виступає інформаційний простір, мережа Інтернет.

Конвенція Ради Європи «Про кіберзлочинність» не містить легальної дефініції кіберзлочинності [1]. Проте, даний термін визначений в українському законодавстві. У ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність трактується як сукупність кіберзлочинів [2, ст. 1]. У свою чергу, кіберзлочин ототожнюється із комп'ютерним злочином та трактується як 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. Кіберпростором є середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене у результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних ко-

мунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Серед найпоширеніших кіберзлочинів виділяють:

- використання програм, що несуть загрозу;
- DDOS атаки (злочинець надсилає велику кількість запитів, що в результаті виводить з ладу об'єкт функціонування);
- комбінація соціальної інженерії і шкідливого коду (фішинг) – передбачає спонукання жертви до певних дій. Наприклад відвідання сайту, натискання на вміст електронного листа, що в подальшому призводить до зараження системи;
- незаконна діяльність: домагання, поширення незаконного контенту. У цьому випадку зловмисники приховують свої сліди за допомогою анонімних профайлів, зашифрованих повідомлень та інших подібних технологій;
- незаконна діяльність з обчислювальними машинами та фінансовими апаратами [3].

У механізмі детермінації кіберзлочинності можна умовно виділити такі групи чинників: соціальні, політичні, економічні, технологічні, психологічні, а також чинники пов'язані з діяльністю правоохоронних органів та віктимною поведінкою потерпілих.

Небезпека кіберзлочинності полягає ще й у її територіальній розповсюдженості. Даний злочин є транснаціональним, що значно ускладнює розслідування та відстеження місцезнаходження суб'єктів злочину.

Серед основних нормативних джерел, що регулюють вищезазначені правовідносини виділяють:

- Конвенцію Ради Європи про кіберзлочинність від 23.11.2001 р.
- Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р.
- Кримінальний кодекс України від 05.04.2001 р.
- Закон України «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» від 23.03.2000 № 1587-III
- Закон України «Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи» від 21.07.2006 № 23-V.

Аналізуючи сучасний стан справ, можна помітити низький рівень кібербезпеки в Україні. Це пояснюється недостатнім розумінням самої природи та системи інформаційних технологій, що в свою чергу унеможливлює створення каркасу правових норм, які б на належному рівні врегулювали дані правовідносини.

Дотепер у національному і навіть міжнародному законодавстві бракує єдиного підходу до визначення підстав віднесення протиправних діянь до категорії кіберзлочинів. Отже, першим кроком до створення безпечного кіберпростору є гармонізація національного законодавства із міжнародними нормативно-правовими актами. Важливим елементом є міжнародна співпраця та залучення професіоналів у царині ІТ. Також варто зосередитися на належному функціонуванні єдиних баз (реєстрів) кіберзлочинців та веденні статистики.

Список бібліографічних посилань

1. Конвенція про кіберзлочинність : від 23.11.2001 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 30.10.2019).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.10.2019).
3. Киберпреступления: понятие, виды и методы защиты // IT-Skills : сайт. 27.03.2018. URL: https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html (дата звернення: 30.10.2019).

Одержано 01.11.2019