

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРЗЛОЧИНИ, ВЧИНЕНІ В УМОВАХ ВОЄННОГО СТАНУ

Ковальова Аліна Ігорівна

курсант 3 курсу Навчально-наукового інституту права та підготовки
фахівців для підрозділів Національної поліції
Дніпропетровський державний університет внутрішніх справ, Україна

Яковлева Анна Андріївна

курсант 3 курсу Навчально-наукового інституту права та підготовки
фахівців для підрозділів Національної поліції
Дніпропетровський державний університет внутрішніх справ, Україна

Науковий керівник: Чорна Аліна Геннадіївна

старший викладач кафедри
кримінального права та кримінології
Дніпропетровський державний університет внутрішніх справ, Україна

На сьогоднішній день у сучасному світі спостерігається явище активної інформатизації суспільства. З одного боку така тенденція має значну кількість переваг. Використання можливостей інформаційних технологій в усіх сферах суспільного життя значно заощаджує час, надає можливість швидкого доступу до інформації, тощо. Водночас, поряд із цим активно розвивається і кіберзлочинність.

Таким чином у 2005 році Верховною Радою України було ратифіковано Конвенцію про кіберзлочинність, у зв'язку з чим був прийнятий відповідний закон. Це стало початком взяття стратегії на нормативно-правове врегулювання кримінальних правопорушень, вчинених із використанням інформаційних технологій, а також, відповідно, протидії цьому.

Відповідно до п. 8 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібернетичний злочин, тобто кіберзлочин (комп'ютерний злочин), визначається 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 [1].

Правове регулювання суспільних відносин, що виникають у сфері використання електронних обчислювальних машин, систем та комп'ютерних мереж, а також мереж електров'язку, здійснюється розділом XVI Кримінального кодексу України.

Проте наразі законодавче регулювання цієї сфери не встигає за стрімким розвитком інформаційних технологій і появою нових способів вчинення кіберзлочинів. Окрім цього, виникає ряд проблем, пов'язаних із кваліфікацією та розслідуванням таких суспільно небезпечних діянь. Це пов'язано, по-перше, з тим, що такі кримінальні правопорушення вчиняються на значній відстані, а дуже часто взагалі за межами України. По-друге, виникають труднощі при документуванні та збиранні доказів у таких справах. Тому варто звернути увагу на вдосконалення нормативно-правових актів, що пов'язані із кіберзлочинністю.

Також ведення на території України воєнного стану значною мірою сприяє вчиненню кіберзлочинів. Насамперед це збільшення кількості випадків інтернет-

шахрайства, зокрема пов'язаного з вимаганням коштів з використанням маніпуляцій щодо, наприклад, допомоги військовополоненим або пораненим, збори коштів на потреби армії, тощо. За повідомленням служби Держспецзв'язу за 2023 рік на українські портали було здійснено 2543 кібератаки [2]. У зв'язку із цим до відповідного розділу Кримінального кодексу України було внесено певні зміни, зокрема посилення кримінальної відповідальності за вчинення кримінального правопорушення. Наприклад була дещо посилена альтернативна санкція ч. 1 ст. 361-1 ККУ шляхом збільшення максимального строку позбавлення волі з двох до трьох років [3].

Такі заходи можуть слугувати фактором стримування правопорушників від вчинення кримінально-протиправних діянь. Проте вжитих заходів недостатньо для ефективної протидії кіберзлочинності. Варто погодитися із Чорною А.Г., що принципами запобігання кримінальним правопорушенням виступають фундаментальні та засадничі ідеї, загальні та основоположні нормативно визначені (та втілені в законодавстві) засади діяльності Національної поліції України, її уповноважених осіб та структурних підрозділів у такій сфері превентивної діяльності, як запобігання кримінальним правопорушенням [4, с. 43-47].

Виходячи з вищенаведеного можна зробити висновок, що необхідно звернути увагу не лише на боротьбу з наслідками, а й здійснювати превентивні заходи, зокрема серед населення. Насамперед проводити профілактичні бесіди з громадянами, інформування та попередження в засобах масової інформації стосовно дотримання правил особистої безпеки в Інтернеті.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року URL:<https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення 09.02.2024)
2. Названа кількість кібератак в Україні за минулий рік URL: <https://www.slovoidilo.ua/2024/01/31/novyna/suspilstvo/nazvana-kilkist-kiberatak-ukrayini-mynulyj-rik> (дата звернення 09.02.2024)
3. Кримінальний Кодекс України URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення 09.02.2024)
4. Чорна А. Принципи запобігання поліцією кримінальних правопорушень на деокупованих територіях. Науковий вісник Дніпропетровського державного університету внутрішніх справ. № 2. 2023. С. 43-47. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/08/2/NV_2-2023-43-47.pdf.