УДК 004.946.5.056

Вікторія Русланівна Балик,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: правові аспекти та механізми забезпечення протидії

Інформаційний злочин – це навмисні дії, спрямовані на руйнування та розкрадання інформації в мережі, інформаційних джерелах, тощо. Згідно Кримінального кодексу України статті 361–363 кіберзлочинами є злочини, що входять до розділу 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [2, с. 170–175]. Злочини, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки мають свої закономірності виникнення матеріальних та ідеальних слідів-відображень, що властиві тому чи іншому способу впливу на комп'ютерну інформацію.

Специфічними для цієї групи злочинів є віртуальні сліди – тобто будь-які зміни стану автоматизованої інформаційної системи, що залишаються на машинних носіях, відображаючи зміни в програмах, базах даних і текстових файлах упродовж часу вчинення злочину, як при безпосередньому так й віддаленому доступі [1, с. 52–53].

Учинення комп'ютерного злочину у більшості випадків має на меті будь-який вплив на машинний носій в ЕОМ – файл і, відповідно, файл даних або прикладного програмованого забезпечення з точки зору криміналістики стає носієм інформаційних слідів, що класифікуються за різними ознаками. До них відносять структурні сліди файлів – зміна тексту, локальні сліди, які з'являються на робочих місцях користувача як результат роботи клієнтської частини операційної системи, мережні сліди, тобі ті, які виникають як результат роботи операційної системи мережі чи прикладного програмного забезпечення мережі та утворюються на вузлах мережі або пристроях та інші.

Нажаль, кіберзлочинність з кожним роком стає все більшою проблемою. За офіційними даними Національної поліції України у 2016 році зафіксовано 3594 кіберзлочинів, а у 2017 їх кількість зросла вдвічі – до

6974. Близько 40% правопорушень з використанням ІТ залишаються не розкритими [3].

Сьогодні всесвітня павутина – це простір для вчинення неправомірних дій організованими злочинними угрупованнями або злочинцями-одинаками. Злочини в мережі відбуваються найрізноманітніші: вимагання з погрозою знищення або блокування баз даних, інформація про теракти, компромат, розкрадання інтелектуальної власності або майна. Комп'ютер все частіше стає знаряддям для вчинення і більш традиційних злочинів. Шахраї в інтернеті можуть використовувати віртуальну мережу для розтрат, розкрадань та привласнення грошових коштів, підробки грошових купюр, документів і кредитних карт, посягання на авторські права і багато чого іншого.

В Україні на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини, пов'язані із злочинами у інформаційних системах, мережах. Станом на 2019 рік до правової основи кібернетичної безпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» інші закони, доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Це пов'язано з тим, що у сучасному світі послуги, виробництво все більше використовує інформаційні технології. Ми залежимо від безперервності та коректності функціонування комп'ютерних систем об'єктів критичної інфраструктури, і атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства.

Для захисту своїх особистих прав, інтересів та даних варто дотримуватися правил безпечного використання мережі Інтернет. Насамперед варто встановити комплексну систему захисту, користуватися ліцензійним програмним забезпеченням, здійснювати покупки в офіційних Інтернет-магазинах, з обережністю ставитись до завантажуваних файлів [4].

Злочинці можуть намагатися отримати доступ до вашої інформації, а саме пароль електронної пошти, банківські реквізити чи номер соціального страхування. Для цього вони можуть установлювати зловмисне програмне забезпечення на ваш комп'ютер, пробувати зламати ваш

обліковий запис або оманливим шляхом змушувати вас надати цю інформацію. Після цього злочинці можуть обкрадати вас, видавати себе за вас або навіть продавати ваші дані на торгах.

З огляду на вищезазначене, можу сказати, що кіберзлочинність набирає обертів у сучасному суспільстві, тому створюються відповідні заходи для захисту інтересів громадян. Кібербезпека – це безпека життя, майна людини, так як ми тісно пов'язані з інформаційними технологіями, які заполонили увесь спектр життя суспільства в цілому. Сьогодні на законодавчому рівні створюються всі можливі заходи щодо врегулювання питання кіберзлочинів.

Список бібліографічних посилань

1. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій : посібник // Б. В. Романюк, М. І. Камлик, В. Д. Гавловський та ін. Київ : Нац. акад. внутр. справ України, 2000. 64 с.
2. Кримінальний кодекс України: зі змінами та доповненнями станом на 25.09.2019 р. : офіц. текст. Київ : Паливода А. В., 2019. 212 с.
3. Уряд погодив проект національної Стратегії забезпечення кібернетичної безпеки // Newsme : сайт. 19.07.2014. URL: http://newsme.com.ua/ua/tech/technologies/2561163/ (дата звернення: 21.10.2019).
4. Як захистити себе в мережі // Українська Наукова Інтернет-Спільнота : сайт. 21.12.2013. URL: https://nauka-online.org/content/yak-zakhystyty-sebe-interneti (дата звернення: 21.10.2019).

Одержано 01.11.2019