ПРОБЛЕМАТИКА ІНТЕРНЕТ–ШАХРАЙСТВА В УКРАЇНІ ТА СПОСОБИ БОРОТЬБИ З НИМ

Качашвілі К. С.,
магістрантка, кафедра правознавства, ПУЕТ;
науковий керівник – доц. Четвертак Д. Ю.

На сьогодні, шахрайство з використанням комп'ютерних мереж – це одна з найдинамічніших груп суспільно небезпечних посягань. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Актуальність протидії використанню у злочинній діяльності комп'ютерних технологій на цьому етапі розвитку української держави не викликає сумнівів.

Шахрайство з використанням комп'ютерних мереж, незважаючи на еволюційні процеси, залишається злочином проти власності, що вчиняється з використанням обману чи зловживання довірою. Різниця полягає лише в тому, що обман відбувається не під час безпосереднього фізичного вербального чи невербального контакту з жертвою, а дистанційно, тобто з використанням можливостей комп'ютерно-телекомунікаційних пристроїв, систем або мереж [4,с. 159].

Поява в 90-ті роки XX ст. графічного інтерфейсу для роботи з ЕОМ стала каталізатором стрімкого зростання кількості користувачів мережі Інтернет, спричинила виникнення нових проблем: інформація, розміщена на законних підставах у сегменті мережі однієї країни, ставала доступною в будь-якій точці земної кулі, в тому числі в країнах, де її публікація суперечила закону[5].

Останнім часом, рівень кібершахрайства швидко зростає в Україні. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Росією, Бразилією, Китаєм та меншою мірою – Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування [5, с. 133].

Виходячи із суті кібершахрайств, можна визначити наступні загрози суспільству та державі:

– відкритість суспільства та держави. Створена на основі комп'ютерних мереж та інформаційних технологій зручна інфраструктура для міжнародних постачань товарів, надання послуг, переказу коштів між фізичними і юридичними особами, зберігання інформації у мережі Інтернет та під'єднання до неї кожного

комп'ютера, надає одночасно широкі можливості як власне кіберзлочинів за допомогою комп'ютерних технологій;

– висока технологічність. Надзвичайно швидкий розвиток інформаційних технологій та складність цієї сфери поряд з відносно тривалим та бюрократичним підходом до розвитку нормативно-правових баз призводить до значного відставання заходів щодо упередження та боротьби з кібершахрайством;

– складний характер злочину. Інтернет-шахраї використовують комп'ютерні технології, інформаційні мережі з соціально-психологічних міркувань, зокрема дискредитації урядів і держав, розміщення сайтів терористичної спрямованості, псування і руйнування ключових систем, виведення цих систем з робочого стану (що є свого роду доповненням до традиційного виду тероризму);

– анонімність злочину. Шахраїв приваблює відсутність фізичного контакту з жертвою та, безперечно, складність виявлення, фіксування та вилучення криміналістично-значущої інформації у віртуальному просторі;

– транснаціональний та популярний характер шахрайства. Особливістю даного виду злочинності є те, що підготовка та скоєння злочину, за наявності доступу до мережі Інтернет, може здійснюватись практично з будь-якого місця. А враховуючи, що комп'ютерна техніка та Інтернет-послуги стають доступнішими для все ширшого кола осіб, кіберзлочинність стає все більш популярною.

Чинним КК України охоплено лише частину відповідних кримінально караних діянь, для позначення яких, ґрунтуючись на аналізі сутності та ознак посягань, використовують такі термінологічні звороти, як «кіберзлочини», «злочини у сфері ІТ-технологій», «високотехнологічні злочини», «інтернет-злочини», «комп'ютерні злочини», «злочинність у сфері високих технологій», «е-злочини» тощо [1]. Наведені словосполучення у нашій країні сьогодні вживаються лише як дефініції.

Усе зазначене вище свідчить, що розв'язання проблеми потребує вдосконалення нормативно-правових актів, які є підґрунтям єдиної державної політики забезпечення інформаційної безпеки та її реалізації.

Першим кроком до здійснення цієї мети є визначення кібернетичної безпеки як самостійної сфери національної безпеки. Це дасть змогу формувати засади державної політики у сфері забезпечення кібернетичної безпеки України шляхом визначення основних реальних загроз національній безпеці, основних напрямів державної політики та основних функцій суб'єктів щодо забезпечення національної безпеки в цій сфері.

Надзвичайно швидкий розвиток інформаційних та комп'ютерних технологій останнім часом призводить до стрімкого розвитку кіберзлочинності, тому особливої актуальності сьогодні набувають питання попередження та протидії злочинам у кіберпросторі.

Попередження кіберзлочинності базується на заходах спрямованих на зниження ризику здійснення таких злочинів та нейтралізацію шкідливих наслідків для суспільства.

Однією з причин високої латентності подібних злочинів є відсутність державних кордонів, якщо злочин учиняється за допомогою Інтернету, недосконаліть законодавства і, відповідно, неможливість співпрацювати з іншими країнами під час розслідування цих злочинів у зв'язку зі значними відмінностями в законодавстві різних країн щодо такого злочину.

Все ж таки, для боротьби із загрозою інтернет-шахрайства, необхідна постійна міжнародна співпраця. Контролювати кібершахрайство і боротися з ним на рівні окремої держави практично неможливо. Прийняття міжнародних норм і стандартів повинне супроводжуватись внесенням змін до національного законодавства держав.

Головне ж завдання полягає в тому, щоб на міжнародному рівні, наприклад, в рамках ООН, розробити комплексну програму, що включатиме в себе всі можливі форми та методи боротьби з інтернет-шахрайством. Ці дії матимуть успіх лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу інтернет-простору на міжнародному та національному рівнях.

Відповідно, правоохоронні органи всіх держав повинні паралельно здійснювати заходи по припиненню і попередженню таких злочинів. Якщо стираються рамки місця вчинення таких злочинів – повинні стиратися рамки місця проведення розслідування. Провадження повинно відбуватися в рамках спільного розслідування таких злочинів правоохоронними органами держав.

Відповідно, для комплексної протидії інтернет-шахрайства необхідні:

– Гармонізація кримінального законодавства про інтернет-шахрайства на міжнародному рівні;

– Розробка на міжнародному рівні та реалізація в національне законодавство стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази.

– Налагоджене співробітництво правоохоронних органів при розслідуванні інтернет-шахрайств на оперативному рівні.

Таким чином, міжнародне співробітництво є ключовим моментом у ліквідації правової прірви, існуючої між розвитком інформаційних

технологій та реагуванням на них законодавства. Це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати інтернет-шахрайства.

Проблемою в Україні також є недостатня кількість державних експертів в області комп'ютерно-технічної експертизи. Тому на нашу думку, необхідно в системі вищої юридичної освіти включити в курси кримінального права, та інформатики такі теми, які присвячені характеристиці неправомірного доступу до комп'ютерної інформації, особливостям його розслідування, тощо. А, можливо, і формування такого інституту як «Кіберправо».

Підсумовуючи вище сказане, проблема профілактики кібершахрайства в Україні – це комплексна проблема. Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль з міжнародними правоохоронними органами та спецслужбами.

Список використаних джерел:

1. Кримінальний кодекс України // Відомості Верховної Ради України: кодекс від 05.04.2001, редакція від 19.05.2019 [Електронний ресурс] – режим доступу: http://zakon3.rada.gov.ua/laws/show/2341-14
2. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5
3. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ / В. Прохоренко // Економічна правда. – 26 лют. 2013 р.
4. Шапочка С. В. Класифікація шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства) / С. В. Шапочка // Наука і правоохорона. – 2015. – № 1. – С. 159-165. – Режим доступу: http://nbuv.gov.ua/UJRN/Nip_2015_1_26.
5. International Telecommunication Union of the United Nations : Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector [Електронний ресурс].– Режим доступу : https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf