Tribune. 2022. Vol. 12. Num. 2. P. 227–245. DOI: 10.24818/TBJ/2022/12/2.05.

8. Cherniei, V., Cherniavskyi, S., Babanina, V., Tykhonova O., & Hudkova, H. (2023). Características de la responsabilidad por revelación del secreto bancario en Europa y Estados Unidos. *Jurídicas CUC*, 19 (1), P. 311–338. https://doi.org/10.17981/juridcuc.19.1.2023.11. URL: https://revistascientificas.cuc.edu.co/juridicascuc/article/view/4598.

Демедюк Марина,
студент Національної академії
внутрішніх справ
Науковий керівник:
Кришевич Ольга Володимирівна,
професор кафедри кримінального права
Національної академії внутрішніх справ,
доктор юридичних наук, професор

КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ КІБЕРЗЛОЧИННОСТІ

Сучасний розвиток цифрових технологій і глобальних інформаційних мереж значно посилює актуальність проблеми кіберзлочинності. Кіберзлочинність являє собою суспільно небезпечну протиправну діяльність, спрямовану на незаконне заволодіння, знищення чи модифікацію інформації, що зберігається в електронних базах даних, а також на несанкціоноване втручання у роботу комп'ютерних систем шляхом використання вірусних програм, фішингових технологій або злому мережевих ресурсів. Такі дії можуть здійснюватися з корисливих, політичних або особистих мотивів, що зумовлює багатогранність і складність цього явища. Крім того, зачіпає не лише окремих громадян і підприємства, а й об'єкти критичної інфраструктури та державні установи, створюючи загрозу інформаційній безпеці на національному рівні. Окрім, безпосередньої матеріальної шкоди, кіберзлочинність підриває довіру до цифрового середовища, що перешкоджає ефективному розвитку електронного урядування та цифрової економіки.

Серед основних проблем кримінального законодавства України у сфері боротьби з кіберзлочинністю виокремлюють: – неповноту нормативного регулювання – відсутність чітких норм, що охоплюють усі види кіберзлочинів, зокрема шахрайство у мережі; – складність кваліфікації – труднощі у відмежуванні кіберзлочинів від суміжних правопорушень; – ускладнене доведення вини, адже злочинці часто діють анонімно, використовуючи захищені канали зв'язку та VPN-технології.

Але понятійним аспектом інформаційного кримінального правопорушення розуміють навмисні дії, спрямовані на знищення, викрадення або незаконне використання інформації, яка зберігається чи передається через інформаційні системи. Відповідно до статей 361–363 Кримінального кодексу України, до кіберзлочинів належать

правопорушення, пов'язані з неправомірним доступом до електронно-обчислювальних машин (комп'ютерів), систем і мереж електрозв'язку [1].

Особливістю цієї категорії злочинів є наявність віртуальних слідів – змін у стані комп'ютерної системи, які фіксуються у програмах, базах даних або текстових файлах під час вчинення злочину. Такі кримінальні правопорушення мають специфічні матеріальні та ідеальні сліди, які утворюються залежно від способу впливу на інформаційні ресурси. Ці сліди можуть залишатися як при безпосередньому доступі, так і при віддаленому втручанні у систему [4].

На думку А. В. Савченка, до категорії кіберзлочинів варто відносити не лише діяння, прямо передбачені розділом XVI КК України, а й інші кримінальні правопорушення, якщо вони здійснюються за допомогою інформаційних мережевих технологій або їх наслідки проявляються у кіберпросторі [5, с. 154]. До таких злочинів учений відносить державну зраду, шпигунство, диверсію, порушення таємниці голосування, незаконне розголошення лікарської, шахрайство, комерційної чи банківської таємниці, сутенерство та інші. Фактично, у кожному розділі Особливої частини КК України можна виокремити діяння, що можуть бути вчинені із використанням комп'ютерних технологій.

В. Б. Дзюндзюк пропонує власну класифікацію кіберзлочинів, виокремлюючи такі їх групи [3]: – злочини проти конституційних прав і свобод людини (порушення недоторканності житла, таємниці листування, авторських прав тощо); – злочини проти життя та здоров'я особи, зокрема розповсюдження рецептів виготовлення наркотичних речовин; – злочини проти честі та гідності, пов'язані з поширенням наклепницької або компрометуючої інформації; – злочини проти власності, особливо у сфері платіжних і банківських систем; – злочини у сфері комп'ютерної інформації – несанкціонований доступ, створення або розповсюдження шкідливих програм; – злочини проти суспільної моральності; –злочини проти державної безпеки, зокрема незаконне отримання чи розголошення державної таємниці.

Враховуючи різні наукові точки зору, можна виділити групи кіберзлочини: – злочини, що посягають на інформаційні комп'ютерні відносини; – злочини у комп'ютерному інформаційному просторі, які стосуються прав на інформаційні ресурси; – інші злочини, для яких використання комп'ютерних технологій є складовою частиною їх вчинення.

Що стосується складу кіберзлочину, то включає такі елементи: об'єкт – інформаційні відносини, безпека комп'ютерних систем, власність тощо; об'єктивна сторона – незаконний доступ, модифікація або знищення даних, поширення вірусів, крадіжка чи шахрайство криптовалюти; суб'єкт – будь-яка осудна особа від 16 років або спеціальний суб'єкт (наприклад, системний адміністратор); суб'єктивна сторона – прямий умисел, часто з корисливими мотивами.

Покарання за кіберзлочини коливається від штрафів та обмеження волі до позбавлення волі строком до 12 років, особливо за масові кібератаки на стратегічні об'єкти. Додатково можуть застосовуватися санкції у вигляді конфіскації техніки чи заборони обіймати певні посади. Зокрема, несанкціоноване втручання в роботу комп'ютерних систем карається до шести років позбавлення волі, а створення або розповсюдження шкідливих програм – до п'яти років [2].

Отже, перспективи вдосконалення кримінально-правового регулювання у сфері кіберзлочинності в Україні пов'язані з модернізацією правової бази, підвищенням цифрової компетентності правоохоронців, інтеграцією міжнародного досвіду та створенням гнучкої системи реагування на нові форми кіберзагроз. Комплексна реалізація цих напрямів дозволить зміцнити правові гарантії кібербезпеки та забезпечити ефективний захист прав громадян у цифровому середовищі. Також, у перспективі доцільним є створення єдиного державного центру моніторингу кіберзлочинів, який би координував діяльність правоохоронних органів, Служби безпеки України, Держспецзв'язку та інших суб'єктів кібербезпеки і така централізація сприятиме оперативному реагуванню на загрози і дозволить ефективно виявляти міждержавні злочинні мережі. Розвиток кримінально-правових засобів протидії кіберзлочинності має відбуватися у тісному взаємозв'язку з адміністративно-правовими, інформаційними та технічними заходами. Законодавець повинен забезпечити баланс між свободою інформаційного простору та його безпекою, не допускаючи надмірного обмеження прав громадян у мережі.

Список використаних джерел

1. Кримінальний кодекс України : документ 2341-III; редакція від 01.02.2025. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

2. Васильковский І. І. Поняття, класифікація та характеристика окремих видів кіберзлочинів. Прикарпатський юридичний вісник. 2017. № 1. ULR: http://www.pjv.nuoua.od.ua/v1-2_2017/44.pdf

3. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3

4. «Кіберзлочинність : виклики часу» URL: https://law.chnu.edu.ua/kiberzlochynnist-vyklyky-chasu/.

5. Савченко А. В. Кваліфікація кіберзлочинів. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. Київ : Видавничий дім «Скіф», 2012. С. 140–210.

6. Шемчук В.В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. Вчені записки ТНУ імені В.І. Вернадського. 2018. Том 29 (68), No 6. – С. 119–124