Мороз М.
студентка юридичного факультету
Західноукраїнського національного університету.
Науковий керівник: доктор юридичних наук, доцент,
професор кафедри теорії права та конституціоналізму
Західноукраїнського національного університету
Колесніков А. П.

КІБЕРЗЛОЧИННІСТЬ : АКТУАЛЬНА СВІТОВА ПРАКТИКА

У наш час почалась дуже стрімка і швидка цифровізація суспільства, яка охопила всі сфери життя - від державних сервісів до приватного спілкування, та нажаль вона спричинила не тільки позитивні але і протиправних діяння у кіберпросторі. Як доречно зазначають аналітики, у статях які я знайшла на просторах інтернету, сучасний світ не уявляє себе без технологій, що й обумовило появу такого явища, як кіберзлочинність [1]. В умовах війни ці загрози набувають особливого значення, адже кібератаки стають елементом гібридної агресії, не раз росія застосовувала фейкові статті, які поширювали між українцями напругу, зневіру. Однак аналіз судової практики показує, що переважна більшість українців також вчиняють кібератаки злочини які стосуються їхніх корисливих посягань, та дій щодо інших громадян [2]. Вміння правильно кваліфікувати такі діяння, збирати електронні докази та застосовувати релевантні правові позиції є нагальною потребою для юриста, що й робить обрану мною тему надзвичайно актуальною.

Метою моєї роботи є комплексний аналіз актуальної судової практики у сфері кіберзлочинності. Я ставлю перед собою завдання не лише узагальнити найтиповіші склади кіберзлочинів за Кримінальним кодексом України, а й порівняти національні підходи до правосуддя з практикою Європейського Союзу та США, визначивши ключові тенденції розвитку цього інституту.

При написанні роботи я детально опрацювала аналітичні публікації, знайшла навіть статті, з сайту ligazakon з яким нещодавно я сама працювала, також з сайту Верховного суду, і звичайних статей на тему моїх тез, а ще матеріали судової практики, це все дозволило мені виокремити три взаємопов’язані блоки проблематики.

По-перше, це найпоширеніші склади кіберзлочинів в Україні та особливості їх судового розгляду. Вивчення Єдиного державного реєстру судових рішень засвідчує, що домінуючим правопорушенням є несанкціоноване втручання в роботу комп’ютерів, систем і мереж (це ст. 361 КК України). Цікаво, що способи такого втручання постійно змінюються. Скажімо, Заводський районний суд м. Дніпродзержинська у січні 2022 року засудив особу, яка за допомогою програми для підбору паролів зламала поштову скриньку потерпілого, - зловмисника звільнили від покарання з іспитовим строком на 1 рік [1]. Ще більш нестандартний

приклад - вирок Шевченківського райсуду м. Києва від 12.10.2021, де було засуджено пособника: він за винагороду підключався до Wi-Fi мережі приватної компанії та надавав віддалений доступ невстановленим особам, які через корпоративну пошту листувалися від імені фірми [1]. Не менш поширеними є злочини, пов'язані зі створенням шкідливого програмного забезпечення (ст. 361-1 КК). Показовою тут є справа, розглянута Уманським міськрайонним судом 14.01.2022 року: студента 4 курсу ІТ-спеціальності оштрафували на 34 000 грн за створення і збут програми, яка приховано збирала логіни, паролі та навіть дані криптовалютних гаманців. Окремо варто згадати порушення авторських прав (ст. 176 КК), де суди демонструють, що навіть звичне для багатьох користувачів «встановлення піратського софту» може мати наслідком кримінальну відповідальність, як у випадку з використанням «кряку» для ArchiCAD [1]. Це свідчить, що судова практика поступово долає стереотип про «безкарність» подібних діянь. Всі ці справи я знайшла у статті від «Ліги Закон Бізнес»

Не можна оминути увагою й кібершахрайство (ст. 190 КК), яке часто поєднується з легалізацією доходів. Як зазначають фахівці, з розвитком інтернет-банкінгу зловмисники вигадують дедалі витонченіші схеми: від фішингу до перевипуску SIM-карт. Приміром, Знам'янський міськрайонний суд Кіровоградської області 18.05.2021 засудив шахрая до 6 років позбавлення волі з конфіскацією за те, що він під виглядом допомоги хворій дитині вивідав особисті дані, перевипустив сім-карту потерпілої та вивів гроші з її рахунку. Також аналітики наголошують на важливості ст. 362 КК (незаконні дії з інформацією з обмеженим доступом), яка застосовується до «інсайдерів» - службових осіб, що мають легальний доступ до систем. Яскравим прикладом є вирок Приморського районного суду м. Одеси від 08.10.2021, яким держреєстратора покарали за безпідставне внесення зміндо реєстру прав на нерухомість, що фактично є сучасним рейдерством [1]. Це доводить, що кіберзлочини скоюються не лише хакерами-одинаками, а й особами, які зловживають своїми службовими повноваженнями. По-друге, я звернулася до проблематики електронних доказів. Як наголошувала суддя Верховного Суду Наталія Марчук, електронні докази відіграють ключову роль, однак потребують специфічного підходу до фіксації та оцінки. ВС сформував принципову позицію у справі № 554/5090/16-к (постанова ОП ККС від 29.03.2021), згідно з якою допустимість електронного документа не можна заперечувати лише через його електронну форму, а усі ідентичні за змістом файли мають вважатися оригіналами [2]. Це означає, що скріншоти, відеозаписи з камер спостереження, дані месенджерів при правильному оформленні визнаються повноцінними доказами. Водночас, як показує практика, сторона захисту чи обвинувачення часто стикається з проблемою ідентифікації файлів; для цього можуть залучатися спеціалісти, які обчислюють хеш-суми або проводять експертизу [2, 4]. Від якості такої

фіксації безпосередньо залежить перспектива справи в суді.

По-третє, я порівняла міжнародний досвід, що дає змогу побачити загальносвітові тренди. Спираючись на дослідження адвоката Юрія

Жовтана, я виокремила три моделі правосуддя [3]. Україна сьогодні діє в умовах кібервійни, тому наші суди демонструють «воєнно-правовий» підхід. Найрезонансніший приклад - справа №760/8515/23, де у вересні 2024 року двох експсівробітників СБУ заочно засуджено до 15 років позбавлення волі за державну зраду та кібератаки на систему «АСКОД», яку використовують сотні державних установ [3]. Це означає, що кібератаки в контексті збройної агресії прирівнюються до шпигунства. Натомість ЄС зосереджується на правозахисному аспекті. У справі Vastaamo (Фінляндія) хакера, який викрав медичні дані 33 000 пацієнтів і шантажував їх, у квітні 2024 року засудили до 6 років 3 місяців ув'язнення, причому суд визнав сам страх потерпілих перед можливим зливом даних нематеріальною шкодою, що підлягає компенсації [3]. Своєю чергою, США реалізують глобальнопревентивну модель, домагаючись екстрадиції хакерів з усього світу. До приклад, у справі ShinyHunters француза Себастьяна Раулта у січні 2024 року засудили до 3 років ув'язнення та зобов'язали виплатити понад 5 млн доларів реституції за злам 60 компаній [3]. Таким чином, незалежно від юрисдикції, світ рухається до невідворотності покарання за кіберзлочини. Ія вважаю що це дуже добре, тому що чим швидше фахівці вивчать всі аспекти боротьби з такими злочинами, звичайним людям стане краще жити, адже коли злочинці будуть чути про міру покарання і те як легко їх буде вичислити, страх бути знайденим переконає їх не вчиняти протиправні дії. Підсумовуючи викладене, можу констатувати, що судова практика у сфері кіберзлочинності розвивається надзвичайно динамічно. По-перше, національні суди поступово відходять від надмірної ліберальності, застосовуючи реальні терміни ув'язнення за найтяжчі кібератаки, особливо в контексті збройної агресії. По-друге, ключовим елементом доказування стають електронні докази, і завдання юриста - забезпечити їх бездоганну фіксацію відповідно до стандартів, вироблених Верховним Судом, ну і також щоб ці докази не були фальсифіковані. По-третє, враховуючи транснаціональний характер таких злочинів, вивчення досвіду ЄС та США є критично важливим. На мою думку, на часі подальша імплементація в українське законодавство міжнародних стандартів, зокрема Другого протоколу до Будапештської конвенції, що дозволить ефективніше співпрацювати у сфері збору доказів. Чим краще вони будуть розвиватися в цій сфері тим легше юристам буде виконувати свою роботу, адже з кожним роком випадків точно побільшає, людство розвивається щодня, що несе за собою не тільки плюси, але нажаль і безліч мінусів неналежного використання їхніх можливостей.

Література:

1. Кіберзлочинність: актуальна судова практика. ЛІГА:ЗАКОН. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualnasudovapraktika
2. Кіберзлочинність та електронні докази: суддя ВС розповіла про оцінку електронних доказів у кримінальному провадженні. Верховний Суд. URL: https://supreme.court.gov.ua/supreme/prescentr/news/1594957/
3. Жовтан Ю. Показові судові справи у сфері кіберзлочинів: практика України, ЄС та США. URL: https://protocol.ua/amp/ua/pokazovi_sudovi_spravi_u_sferi_kiberzlochiniv_praktika_ukraini_es_ta_ssha/
4. Кримінальна відповідальність за кіберзлочини в Україні. Дипломат. URL: https://diplomat.net.ua/blog/kryminalna-vidpovidalnist-za-kiberzlochyny-vukrayini/
5. Колесніков А. П., Зяйлик М. Ф. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. *Актуальні проблеми правознавства*. 2017. №1. С. 26-29.