Практика Верховного Суду щодо кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Денис С. Р.[1]

Опубліковано	Секція	УДК
10.10.2022	Право	343.2

DOI: http://dx.doi.org/10.5281/zenodo.7214268

Анотація. У статті проведено аналіз і узагальнення практики Верховного Суду щодо кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Досліджено передумови збереження тенденції до зростання числа кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Доведено, що особливостями відповідних діянь є їхня високотехнологічність, латентність та високий рівень суспільної небезпечності. Наголошено, що ці особливості зумовлюють складність виявлення та розслідування відповідних кримінальних правопорушень, притягнення винних осіб до кримінальної відповідальності, а отже – здійснення загальної та спеціальної превенції. На основі аналізу постанов Верховного Суду узагальнено особливості кримінально-правової кваліфікації за статтею (статтями) Розділу XVI Кримінального кодексу України.

Ключові слова: практика Верховного Суду, кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, розповсюдження шкідливих програмних засобів, несанкціонована зміна інформації, несанкціоноване знищення інформації.

[1] Денис С. Р., кандидат юридичних наук, доцент кафедри кримінального права і кримінології, юридичний факультет, Львівський національний університет імені Івана Франка, https://orcid.org/0000-0001-6079-2300

The practice of the Supreme Court regarding criminal offenses in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks

Annotation. The acceleration of technological progress has become one of the leading trends in the development of human civilization in recent decades. The development of information and telecommunication technologies, which contributed to finding new solutions to our time's legal, economic and social problems, became the most dynamic. At the same time, the emergence of new opportunities is usually accompanied by new risks and threats to social relations. The reverse side of the rapid development of information and telecommunication technologies was the emergence of a new type of socially dangerous acts, which in criminal law were combined into a group of criminal offenses in the use of electronic computing machines, systems and computer networks and telecommunication networks. With the increasing development of information and telecommunication technologies, the public danger of crimes that infringe on relevant relationships is growing significantly.

The author conducted an analysis and summarized the practice of the Supreme Court regarding criminal offenses in the use of electronic computing machines (computers), systems and computer networks and telecommunication networks. First, the author investigated the prerequisites for maintaining the tendency to increase the number of criminal offenses in using electronic computing machines (computers), systems, computer networks and telecommunication networks. The specifics of the relevant acts are their high technology, latency and high level of public danger. These features make it challenging to identify and investigate relevant criminal offenses, bring guilty persons to criminal responsibility, and, therefore, implement general and special prevention. Finally, based on the analysis of the decisions of the Supreme Court, the author summarized the features of the criminal-legal qualification according to the article(s) of Chapter XVI of the Criminal Code of Ukraine.

Keywords: the practice of the Supreme Court, criminal offenses in using electronic computing machines (computers), systems and computer networks and telecommunications networks, distribution of malicious software, unauthorized change of information, unauthorized destruction of information.

Вступ

Прискорення технологічного прогресу стало однією з провідних тенденцій розвитку людської цивілізації протягом останніх десятиліть. Найбільш динамічним став розвиток інформаційно-телекомунікаційних технологій, що сприяли віднайденню нових рішень правових, економічних та соціальних проблем сучасності. Разом з тим, поява нових можливостей зазвичай супроводжується новими ризиками та загрозами для суспільних відносин. Зворотнім боком стрімкого розвитку інформаційно-телекомунікаційних технологій стало виникнення нового різновиду суспільно-небезпечних діянь, які у кримінальному праві були об’єднані у групу кримінальних правопорушень у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж і мереж електрозв’язку. По мірі усе більшого розвитку інформаційно-телекомунікаційних технологій, суспільна небезпечність кримінальних правопорушень, які посягають на відповідні відносини, суттєво зростає.

Питання кримінальної відповідальності за вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж і мереж електрозв’язку досліджували Д. С. Азаров, Ю. М. Батурин, М. В. Карчевський, С. А. Кузьмін, Т.М. Луцький, О.Ф. Пасєка, О. Е. Радутний та ін.

Зміст та особливості кримінальних правопорушень у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж і мереж електрозв’язку потребують ретельного дослідження та аналізу, адже їх вплив виходить

за межі кримінального права і торкається відносин у сфері інтелектуальної власності, безпеки держави і суб'єктів господарювання, економіки, розвитку науки і техніки.

Метою статті є аналіз і узагальнення практики Верховного Суду щодо кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Результати

Кримінальні правопорушення, що посягають на суспільні відносини щодо забезпечення контрольованого використання комп'ютерної інформації та нормальної роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку законодавець виокремив у розділ XVI Кримінального кодексу України [1].

Як зазначали свого часу суддя Верховного Суду України М. І. Гриців та головний консультант управління вивчення та узагальнення судової практики Верховного Суду України В. В. Антощук, завдяки удосконаленню комп'ютерних систем постають нові можливості щодо учинення раніше невідомих правопорушень. В Україні спостерігається стійка тенденція щодо зростання числа кримінальних правопорушень, вчинених у сфері використання комп'ютерів, комп'ютерних мереж та мереж електрозв'язку, щодо яких уживається узагальнена назва «комп'ютерні злочини» [6]. Такі висновки авторами зроблено на основі узагальнення судової практики. Проте поза увагою дослідників залишається інша кримінально-правова тенденція – зростання кількості кримінальних правопорушень у аналізованій сфері не обумовлює паритетного зростання числа кримінальних проваджень та ухвалених вироків.

До основних причин виникнення такої тенденції Т.М. Луцький та О.Ф. Пасєка відносять:

а) недосконаліть законодавства;
б) високий рівень латентності цих кримінальних правопорушень;
в) обмежену ефективність доступних засобів виявлення, розслідування, запобігання;
г) недостатній рівень спеціальних знань у правоохоронців, які забезпечують виявлення і розслідуванням відповідної категорії справ та ін. [5, с. 271].

У силу специфіки аналізованої групи правопорушень можемо висловити припущення щодо того, що об'єднавчим стрижнем методологічного характеру для ефективної кримінально-правової боротьби з ними виступає єдність судової практики. Як наголошує М. О. Деменчук, забезпечення єдності судової практики є тривалим та складним процесом, який в Україні покладено на Верховий суд [7]. Я. О. Берназюк акцентує на тому, що призначення Верховного Суду як найвищої судової установи в Україні – це, у першу чергу, сформувати обґрунтовану правову позицію стосовно способу застосування всіма судами конкретної норми матеріального права або дотримання норми процесуального права і таким чином, спрямувати судову практику в єдине та узгоджене правозастосування (вказати напрямок, у якому слід здійснювати вибір норми права); на прикладі конкретної справи роз`яснити зміст акту законодавства в аспекті його розуміння та реалізації на практиці в інших справах з вказівкою на обставини, які потрібно враховувати при застосуванні тієї чи іншої правової норми, але не нав`язуючи, при цьому, нижчестоящим судам результат вирішення конкретної судової справи [8].

Судова практика є сукупністю правових положень, вироблених судовою владою. У вузькому сенсі це сукупність рішень судів щодо справ певної категорії. Для розуміння змісту правових норм, особливостей їх реалізації, а також виявлення можливих прогалин чи суперечностей, що можуть у них міститись особливо важливим виступає дослідження рішень судів. У світлі наведених вище аргументів, користуючись методом сходження від конкретного до загального ми проаналізуємо низку рішень Верховного

Суду для забезпечення різносторонньої характеристики та узагальнення практики щодо кримінальних правопорушень у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку.

Перш за все розглянемо нюанси доведення вини особи у вчиненні відповідних кримінальних правопорушень на основі аналізу Постанови Верховного Суду (№726/2173/18 від 09 грудня 2020 р.) щодо кримінального провадження по обвинуваченню особи у вчиненні кримінальних правопорушень, передбачених ч. 1 ст. 176, ч. 2 ст. 176, ч. 1 ст. 361, ч. 2 ст. 361 Кримінального кодексу України.

Згідно з матеріалами кримінального провадження ОСОБА_1 із ціллю здійснення несанкціонованого розповсюдження (ретрансляції) телевізійних каналів «Футбол 1» і «Футбол 2», що належать ТОВ «Телерадіокомпанія Україна», розуміючи, що його такого роду його дії спричинять витік, а також спотворення процесу обробки інформації і порушення встановленого порядку її маршрутизації та бажаючи цього, вчинив налаштування придбаних ним заздалегідь телевізійних приставок через завантаження на них додатку, що має назву «Lazy IpTv», який дає змогу використовувати вказані телевізійні приставки як IpTv-програвач. Далі з ціллю доведення умислу до кінця ОСОБА_1, у налаштуваннях роботи додатку «Lazy IpTv» установив завантажений ним з ресурсу ІНФОРМАЦІЯ_2 програмний код, що в ньому є рядки, які дають змогу через програмне забезпечення «Lazy IpTv» переглядати і здійснювати трансляцію із використанням вказаних телевізійних приставок програми мовлення телеканалів «Футбол 1» і «Футбол 2». Отже, було здійснено додаткові налаштування, метою яких є організація несанкціонованого перегляду трансляцій зазначених телевізійних каналів.

Далі ОСОБА_1 з ціллю одержання прибутку, здійснив розміщення оголошення на веб-ресурсі «www.olx.ua» щодо продажу і надання послуг із налаштування телевізійних приставок для їх використання у якості IpTv-програвача. Пізніше ОСОБА_1 збув «покупцю» ОСОБА_2 заздалегідь ним налаштовану для несанкціонованого перегляду трансляцій телевізійних каналів медіаприставку «SmartTV Box». На цій підставі ОСОБА_1 обвинувачувався у вчиненні кримінального правопорушення, що передбачене ч. 1 ст. 361 Кримінального кодексу України.

Згодом ОСОБА_1 діючи умисно, повторно, та з ціллю несанкціонованого втручання у роботу мережі електрозв`язку, підключив обрану ОСОБА_3 медіаприставку, що спричинило до витоку інформації, а саме, спотворення процесу обробки інформації, що обробляється у мережі електрозв`язку «Футбол 1» та «Футбол 2» й до порушення встановленого порядку маршрутизації інформації, що виразилось в отриманні інформації особами, які не мають на це відповідних прав. Відтак ОСОБА_1 обвинувачувався у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 361 Кримінального кодексу України, тобто у діянні, передбаченому ч. 1 ст. 361 Кримінального кодексу України, вчиненому повторно.

Твердження прокурора й представника потерпілої особи стосовно необґрунтованості виправдання ОСОБА_1 у вчиненні інкримінованих йому кримінальних правопорушень Верховний Суд відхилив.

Верховний Суд звернув увагу на те, що відповідно до положень ст. 361 Кримінального кодексу України, кримінальна відповідальність встановлюється за несанкціоноване втручання у роботу мереж електрозв`язку, що спричинило до витоку, втрати, підроблення, блокування інформації, спотворення процесу обробки інформації чи до порушення установленого порядку її маршрутизації. Тоді об`єктивна сторона кримінального правопорушення, передбаченого ст. 361 Кримінального кодексу України, охоплює не усі дії, які спричинили витік, втрату, підробку, блокування інформації, спотворення процесу обробки інформації чи до порушення встановленого порядку її маршрутизації. Кримінальна відповідальність за зазначеною статтею настає

тільки в разі, коли такі наслідки мають місце у результаті несанкціонованого втручання в роботу мереж електрозв`язку.

У такому разі несанкціоноване втручання у роботу мереж електрозв`язку є будь-якими діями, вчиненими без наданої власником згоди, унаслідок яких припиняється робота мережі електрозв`язку або ж змінюється режим такої роботи.

Зазначені вище дії ОСОБА_1 були кваліфіковані за ч. ч. 1, 2 ст. 361 Кримінального кодексу України, тобто як несанкціоноване втручання в роботу мереж електрозв`язку, що спричинило витік, а також спотворення процесу обробки інформації і порушення встановленого порядку щодо її маршрутизації.

ОСОБА_1 встановив на телевізійні приставки застосунок «Lazy IpTv», що дають змогу переглядати трансляції програми мовлення телеканалів «Футбол 1» і «Футбол 2», що надавало можливість здійснювати несанкціонований перегляд трансляцій телевізійних каналів. На думку сторони обвинувачення саме такі дії спричинили до витоку інформації, а саме, до спотворення процесу обробки інформації, що обробляється у мережі електрозв`язку «Футбол 1» та «Футбол 2», а також і до порушення порядку маршрутизації інформації. Зазначені ознаки кримінального правопорушення знайшли своє вираження у отриманні інформації особами, які не мають на це відповідних прав.

Верховний Суд зазначає, що такі формулювання обвинувачення не містять жодних даних про настання зазначених наслідків у результаті учиненого ОСОБА_1 несанкціонованого втручання в роботу мереж електрозв`язку, тобто у роботу комплексу технічних засобів телекомунікацій, завданням яких є маршрутизація, комутація, передавання та/або приймання знаків, сигналів, письмового тексту, зображень і звуків між кінцевим обладнанням. За таких обставин ОСОБА_1 обвинувачується у тому, що ним продано телевізійні приставки із відповідним налаштуваннями на перегляд трансляцій телеканалів «Футбол 1» та «Футбол 2», що перебувають хоча і у нелегальному, проте вільному доступі у мережі Інтернет. Водночас відомості стосовно того, хто організував цю нелегальну ретрансляцію програми мовлення зазначених телеканалів у мережі Інтернет обвинувальний акт не надає.

Зважаючи на викладене, висновки щодо недоведеності у діянні ОСОБА_1 складу кримінального правопорушення, передбаченого ч. ч. 1, 2 ст. 361 Кримінального кодексу України, Верховний Суд вважає законними та обґрунтованими [3].

Таким чином, слід розрізняти несанкціоноване втручання у роботу електронних комунікаційних мереж та застосування особами, не причетними до такого втручання, технічних засобів і обладнання, що дають змогу, не створюючи цього втручання, використати його зі своєю метою. Використання телевізійних приставок для перегляду нелегальної трансляції ефіру телеканалів не є такою нелегальною трансляцією.

Далі проаналізуємо Постанову Верховного Суду від 27 вересня 2021 року №570/2835/16-к, що наочно демонструє важливість техніко-технологічних компетенцій як сторони обвинувачення, так і захисту у рамках судового розгляду справ, пов’язаних з вчиненням кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

З матеріалів Постанови випливає, що вироком суду ОСОБА_1 було засуджено до покарання за частиною 1 статті 361 КК України. ОСОБА_1 вчинив незаконне відтворення на жорсткий диск комп`ютера, що належить ОСОБА_2, програмного забезпечення, що майнові авторські права на нього належать ДП «Єврософтпром», завдавши такими діями правовласнику шкоди. Згодом він вчинив такі дії повторно. Також, маючи дистрибутив програмного продукту «1С:Предприятие», застосовуючи спеціальні знання, завдяки шкідливим програмам утрутився у роботу автоматизованої

системи «1С:Предприятие» і нейтралізував її засіб інтелектуального захисту, що спричинило незаконне копіювання комп`ютерної інформації, незаконний запуск та використання програмного продукту, отримання несанкціонованого доступу до інформації із можливістю для її модифікації, спотворення або знищення. Також після проведених зазначеною особою дій шкідливі програми почали автоматично відтворюватися у автоматизованій системі «1С:Предприятие».

З точки зору засудженого, суди неправильно визначили поняття «автоматизована система». Окреме програмне забезпечення, що ним він справді скористався без надання відповідного дозволу правовласника не можна вважати автоматизованою системою. Натомість нею є кілька (система) комп'ютерів, що є об’єднані поміж собою в спільну автоматизовану мережу, по якій і здійснюється маршрутизація інформації (трафік). Матеріали справи не містять доказів, що підтверджують втручання ним у будь-яку систему, що її ознаки відповідали би вимогам закону, а також і докази стосовно розповсюдження ним шкідливих програм.

Верховний Суд не погодився з відсутністю в діянні засудженого складу кримінального правопорушення, передбаченого частиною 1 статті 361^1 КК, а саме розповсюдження шкідливих програм. Таке рішення Суд мотивував наступним чином. Відповідно до показів представника ДП «Єврософтпром» усі програмні продукти компанії є захищеними і комплектуються ключами програмно-апаратного захисту, ціллю яких є перешкоджання несанкціонованому доступу до даних. У разі незаконного втручання у захищену ключем програму відбувається блокування доступу до ряду функцій програми, що спричиняє порушення працездатності автоматизованої системи. Інший свідок не заперечив, що шляхом свідомого обходу електронного захисту програмного забезпечення 1С та запуску програми без застосування апаратного ключа доступу відбувається збій в функціонуванні програми, що і є втручанням до автоматизованої системи «1С:Предприятие» із використанням шкідливих програм. Наведені стороною захисту доводи не спростовують достовірності і достатності доказів, а є лише їх переоцінкою.

Стосовно засудження за частиною 1 статті 361 Кримінального кодексу України Верховний Суд звертає увагу на те, що диспозиція статті 361 КК в частині, що застосовується до цієї справи, передбачає несанкціоноване втручання у роботу автоматизованих систем, що призвело до порушення встановленого порядку маршрутизації інформації.

Законом України «Про захист інформації в інформаційно-комунікаційних системах» встановлено, що інформаційна (чи автоматизована) система є «організаційно-технічною системою, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів». Порушенням цілісності інформації у системі є несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст. Об`єктами захисту в системі виступає інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації. Відтак, Верховний Суд дійшов висновку про те, що законодавець розрізняє поняття інформаційної (автоматизованої) системи та програмного забезпечення, що є елементом такої системи.

Далі, Суд наголошує на тому, що втручання у автоматизовану систему вимагає щоби певна автоматизована система була вже створена й функціонувала, тобто виконувала певні запрограмовані операції із наявною у ній інформацією, та в результаті такого втручання порушується порядок виконання операцій, зокрема, якщо мова йде про порядок маршрутизації інформації, інформація за наслідком втручання передається не на ті адреси або не тим шляхом, які задані програмою [4].

Тобто Верховний Суд звертає увагу на те, що програмне забезпечення є елементом інформаційної (автоматизованої) системи. Втручання до автоматизованої

системи вимагає щоби така система була створена та функціонувала, а наслідком такого втручання виступає порушення порядку виконання операцій, а якщо це стосується порядку маршрутизації інформації то інформація тоді передається не на ті адреси або не тим шляхом, які задані програмою.

Заслуговує на увагу і Постанова Верховного Суду від 16 квітня 2019 року № 727/3242/17 щодо справи за обвинуваченням ОСОБА_1, у вчиненні злочину, передбаченого частиною 1 статті 362 Кримінального кодексу України. ОСОБА_1 знаходячись на власному робочому місці, користуючись робочим персональним комп'ютером, умисно, а також протиправно учинила несанкціоновані щодо зміни інформації, що зберігалася на носії інформації – сервері, через підключення за протоколом до віддаленого робочого столу сервера, а саме, умисно, протиправно, без відома та надання дозволу працівників товариства, здійснила зміну файлу програмного забезпечення «1С Бухгалтерія», що у ньому містилась база даних із інформацією стосовно фінансовою діяльності закладів харчування, які належать товариству. Продовжучи діяльність протиправного характеру, спрямовану на умисне змінення та знищення інформації відповідного ТОВ, ОСОБА_1 умисно, протиправно, та без відома і отримання належного дозволу від посадових осіб ТОВ, здійснила видалення файлів програмного забезпечення «1С Бухгалтерія», що містили бази даних із фінансовою інформацією роботи закладів харчування.

Касаційне оскарження ОСОБА_1 обґрунтовує тим, що висунуте обвинувачення не є належним чином обґрунтоване і не містить достатніх доказів, які б у єдності могли підтвердити вчинення інкримінованого злочину. Також, на думку засудженої особи, суди не здійснили встановлення мотиву і мети злочину, а також форми її вини, а відтак прийняли помилкове рішення. Із такими міркуваннями засудженої особи, що викладені у касаційній скарзі, колегія суддів Верховного Суду не погодилася, а скаргу не задовольнила із наступних підстав.

Виходячи із матеріалів кримінального провадження, ОСОБА_1 визнано винною, а її дії було кваліфіковано за ч. 1 ст. 362 Кримінального кодексу України, а саме як вчинення несанкціонованої зміни та знищення інформації, що обчислюється у електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах чи зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Пред'явлене органом досудового розслідування обвинувачення було визнано доведеним з огляду на покази самої засудженої, а також покази потерпілого ОСОБА_4, свідків ОСОБА_5 й ОСОБА_6, експерта ОСОБА_7 і з урахуванням письмових доказів стосовно діяльності товариства, призначення ОСОБА_1 на роботу, даних стосовно її особи, потрібних для здійснення працевлаштування, висновку експерта, протоколу обшуку, протоколу огляду речей та ін.

Також суд звертає увагу на те, що ОСОБА_1 надала підтвердження того, що працювала на посаді бухгалтера на відповідному ТОВ у формі сумісництва і мала ключ доступу до програми «1С Бухгалтерія». Водночас власну вину у вчиненні кримінального правопорушення засуджена заперечувала.

Проте, у противагу невизнання засудженою особою власної винуватості, потерпілий ОСОБА_4, а також свідки ОСОБА_5 та ОСОБА_6, серед іншого, зазначили, що засуджена вимагала здійснити розрахунок із нею за надані додаткові послуги, а після того як засуджена звільнилася, база підприємства «1С Бухгалтерія» зникла. Так само експерт ОСОБА_7 підтвердив висновки експертизи.

Верховний Суд звертає увагу на те, що зазначені докази були додатково перевірені так само і під час апеляційного розгляду. Тоді апеляційним судом правильно встановлено і зазначено, що файли було видалено із персонального комп'ютера засудженої, у період часу, до якого відноситься інкриміноване ОСОБА_1 кримінальне

правопорушення, з використанням логіну, а також паролю для доступу до серверу товариства, що були відомими тільки їй. У процесі здійснення експертного дослідження виявлено історію підключень із віддаленого персонального комп'ютера із встановленою IP-адресою та із застосуванням логіну і пароля, що належать засудженій.

Також у апеляційному суді експерт ОСОБА_7 надав додаткове підтвердження висновків експертного дослідження, щодо того, що ОСОБА_1 здійснила вхід за протоколом віддаленого доступу до робочого столу із свого комп'ютера на комп'ютер відповідного ТОВ, опісля чого були змінені й знищені файли.

Отже, судам надано достатньо доказів для здійснення правильної кваліфікації дій засудженої за частиною 1 статті 362 Кримінального кодексу України. Водночас доводи засудженої викладені у касаційній скарзі у формі загальних формулювань. Зважаючи на викладене, колегія суддів Верховного Суду дійшла висновку, що судові рішення стосовно засудженої ОСОБА_1 є законними та обґрунтованими, а тому її касаційна скарга не підлягає задоволенню [2].

Із наведеної постанови Верховного Суду можна зробити декілька висновків. Так, правильна кваліфікація дій за відповідною статтею чи статтями Розділу XVI Кримінального кодексу України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» потребує залучення осіб, які мають необхідні знання для надання висновку з досліджуваних питань. Складність технологічних процесів та пристроїв, що у них здійснюється втручання або які застосовуються під час вчинення даної категорії кримінальних правопорушень найчастіше потребуватиме залучення експерта і до розгляду справи у апеляційному суді. Також принциповим питанням для правильної кваліфікації за ст. 362 КК України є належність персонального комп’ютера, за допомогою якого були вчинені протиправні дії певній особі, а також коло осіб, яким були відомі особисті логін та пароль підозрюваного для доступу до системи.

Наприкінці даного дослідження звернемо увагу на наступну кримінологічну особливість комп’ютерної злочинності. Як слушно зауважують М.І. Гриців та В.В. Антощук, відповідним кримінальним правопорушенням притаманною є латентність, причиною якої є відсутність бажання користувачів мережі повідомляти про такі злочини у зв’язку із недовірою до дієвості правоохоронних органів, а також небажанням визнати публічно слабкі місця у власних системах безпеки [6]. Можемо додати до переліку причин і низьку обізнаність у суспільстві щодо реальної загрози комп’ютерних злочинів, а також того, що часто вони супроводжують більш тяжкі злочини, як-от шантаж, шпигунство, тероризм та ін.

Висновки

За результатами дослідження судової практики у справах про кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку ми дійшли наступних висновків.

Доведено, що особливостями відповідних діянь є їхня високотехнологічність, латентність та високий рівень суспільної небезпечності. Ці особливості зумовлюють складність виявлення та розслідування відповідних злочинів, притягнення винних осіб до відповідальності, а отже – здійснення загальної та спеціальної превенції.

Встановлено, що правильна кваліфікація діяння за статтею (статтями) Розділу XVI КК України зазвичай потребує залучення експертів, які володіють достатніми знаннями для надання висновку з досліджуваних питань, зокрема і у апеляційному суді.

Наголошено, що діяння не може бути кваліфіковане як втручання у роботу електронних комунікаційних мереж у випадку використання особами технічних чи

програмних засобів, вільно (хоча нелегально) доступних у мережі інтернет для доступу до ретрансльованої інформації.

Додатково встановлено, що програмне забезпечення є елементом інформаційної (автоматизованої) системи, умовою втручання до якої є факт її створення та функціонування, а наслідком такого втручання є порушення порядку виконання операцій, а у випадку порядку маршрутизації інформації – зміна адреси або шляху передачі інформації на відмінні ніж ті, що задані програмою.

Доведено, що умовою правильної кримінально-правової кваліфікації діяння за ст. 362 КК України є з'ясування належності підозрюваному (обвинуваченому) персонального комп'ютера і відомостей для доступу до системи.

Проблемою, на якій акцентують увагу як судді, так і науковці, є високий рівень латентності кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Зазначене питання є *перспективним для подальших наукових досліджень.*

Список використаних джерел

1. Кримінальний кодекс України: Закон України № 2341-III від 05.04.2001 (у редакції від 19.08.2022). *Законодавство України.* URL: https://zakon.rada.gov.ua/laws/show/2341-14/conv#n2491 (дата звернення: 03.10.2022).
2. Постанова Верховного Суду від 16.04.2019 р. у справі №727/3242/17. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/81329306 (дата звернення: 03.10.2022).
3. Постанова Верховного Суду від 09.12.2020 р. у справі №726/2173/18. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/93595905 (дата звернення: 03.10.2022).
4. Постанова Верховного Суду від 27.09.2021 р. у справі №570/2835/16-к. *Єдиний державний реєстр судових рішень.* URL: https://reyestr.court.gov.ua/Review/100109379 (дата звернення: 03.10.2022).
5. Луцький Т.М., Пасєка О.Ф. Окремі проблемні аспекти кримінальної відповідальності та покарання за правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. *Аналітично-порівняльне правознавство. Кримінальне право та кримінологія; кримінально-виконавче право*. 2022. №1. С. 270-275. URL: http://journal-app.uzhnu.edu.ua/article/view/260148 (дата звернення: 03.10.2022).
6. Гриців М.І., Антощук В.В. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. *Верховний Суд України: офіційний веб-сайт.* URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02 (дата звернення: 03.10.2022).
7. Деменчук М. Механізми забезпечення єдності судової практики Верховним Судом: аналіз і шляхи вдосконалення. *Юридичний вісник.* 2019. №1. С.66-70. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/530 (дата звернення: 03.10.2022).
8. Берназюк Я. О. Конституційно-правовий статус Верховного суду як суду права. *Експерт*. 2020. № 6 (12). URL: https://maup.com.ua/assets/files/expert/12/8.pdf