УДК 343.3/.7
DOI https://doi.org/10.24144/2788-6018.2024.06.124

СТВОРЕННЯ З МЕТОЮ ПРОТИПРАВНОГО ВИКОРИСТАННЯ, РОЗПОВСЮДЖЕННЯ АБО ЗБУТУ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ, А ТАКОЖ ЇХ РОЗПОВСЮДЖЕННЯ АБО ЗБУТ (СТАТТЯ 361[1] КК УКРАЇНИ): ОКРЕМІ АСПЕКТИ ТА ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОЇ КВАЛІФІКАЦІЇ

Леськів С.Р.,
кандидат юридичних наук,
доцент кафедри кримінального права і кримінології
юридичного факультету
ЛНУ ім. Івана Франка
ORCID: 0000-0001-6079-2300

Леськів С.Р. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361[1] КК України): окремі аспекти та проблеми кримінально-правової кваліфікації.

Стаття присвячена аналізу окремих аспектів та проблем кримінально-правової кваліфікації правопорушень, передбачених статтею 361[1] Кримінального кодексу України, що передбачає кримінальну відповідальність за створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут. Автором проведено аналіз наявної судової практики та окреслено статистику на основі 166 вироків суду згідно з даними Єдиного державного реєстру судових рішень. За результатами такого дослідження було виявлено, що зі усього масиву вироків лише 4,22% є виправдувальними, водночас обвинувальні – 95,78% (з яких у 96,2% випадках особа визнала свою вину; 3,8% – особа, заперечила свою вину). Це наводить на сумніви відносно якості та повноти розгляду подібної категорії справ у суді. У роботі досліджується конструкція об'єктивної сторони складу кримінального правопорушення та пропонується власне бачення щодо визначення окремих форм діяння, а саме: чи можна вважати передачею розміщення у відкритому або обмеженому доступі шкідливого програмного забезпечення; чи можна вважати розповсюдженням шкідливого програмного забезпечення, якщо доступ до нього здійснюється користувачем через введення IP адреси. Також акцентується увага на необхідності визначення єдиної методології ідентифікації шкідливого програмного забезпечення та формалізації окремих понять. Відсутність єдиного підходу до визначення термінів, таких як «шкідливе програмне забезпечення» та «автоматизована система», ускладнює правозастосування і викликає неоднорідність судової практики. Особлива увага приділяється проблемі кваліфікації через інструменти ідентифікації шкідливого програмного забезпечення, зокрема з використанням ресурсу «VirusTotal», що може призводити до хибних висновків. Автором наголошується на необхідності формування єдиного та сталого підходу правозастосування судами. Також автором було акцентовано увагу на конкретних заходах, вжиття яких матиме наслідком покращення якості правозастосування норми, що міститься у статті 361[1] КК України та сприятиме формуванню єдиного підходу у судах до кваліфікації та притягнення до кримінальної відповідальності осіб, які вчинили діяння, передбачене вищезазначеною статтею.

Ключові слова: кримінальне правопорушення, електронно-обчислювальні машини (комп'ютери), кримінальна відповідальність, інформаційна (автоматизована) система, шкідливі програмні засоби.

Leskiv S.R. Creation for the purpose of illegal use, distribution or sale of harmful software or technical means, as well as their distribution or sale (Article 361[1] of the Criminal Code of Ukraine): certain aspects and problems of criminal-legal qualifications.

This article analyzes certain aspects and problems of the criminal legal qualification of offences under Article 361[1] of the Criminal Code of Ukraine, which provides for criminal liability for the creation with the purpose of unlawful use, distribution or sale of malicious software or hardware, as well as their distribution or sale. The author analyzes the existing case law and provides statistics based on 166 court verdicts according to the Unified State Register of Court Decisions. The results of this study revealed that only 4.22% of the total number of verdicts were acquittals, while

95.78% were guilty verdicts (of which 96.2% were plea bargains and 3.8% were denials). This raises doubts as to the quality and completeness of the consideration of this category of cases in court. The article examines the construction of the objective aspect of the criminal offence and offers the author's own vision of the definition of certain forms of action, namely: whether the placement of malicious software in open or restricted access can be considered as transfer; whether it can be considered as distribution of malicious software if access to it is provided by the user through entering an IP address. Attention is also drawn to the need to define a unified methodology for identifying malware and formalize certain concepts. The absence of a unified approach to the definition of terms such as "malware" and "automated system" complicates law enforcement and causes heterogeneity in judicial practice. Particular attention is paid to the problem of qualification through malware identification tools, in particular, using the VirusTotal resource, which may lead to erroneous conclusions. The author emphasizes the need for a unified and sustainable approach to law enforcement by the courts. The author also focuses on specific measures which will improve the quality of law enforcement of the provision contained in Article 361[1] of the Criminal Code of Ukraine and will contribute to the formation of a unified approach in the courts to the qualification and prosecution of persons who have committed an act under the above article.

Key words: criminal offense, electronic computing machines (computers), criminal liability, information (automated) system, malicious software.

Постановка проблеми. Стрімке впровадження ІТ-технологій у переважну більшість сфер суспільних відносин зумовило зростання кількості кримінальних правопорушень, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів) (далі – ЕОМ). Опираючись на аналіз даних Єдиного державного реєстру судових рішень (далі – ЄДРСР) слід відмітити, що у більшості випадків суд приходить до висновку про доцільність ухвалення саме обвинувального вироку, а питома вага таких вироків базується на угоді з прокурором, при цьому, підходи до розуміння окремих понять є неоднозначними, що зумовлює інтерес до дослідження питання кваліфікації кримінально-протиправних діянь у сфері використання ЕОМ.

Мета дослідження. Метою цієї наукової статті є дослідження проблематики окремих аспектів кримінально-правової кваліфікації кримінального правопорушення, передбаченого ст. 361[1] Кримінального кодексу України (далі – КК України) [1] через призму судової практики.

Стан опрацювання проблематики. Питання проблематики кримінальної відповідальності за правопорушення у сфері використання ЕОМ, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку досліджувалося Д.С. Азаровим, Т.М. Луцьким, О.Ф. Пасєкою та ін. Науковці відзначають високу латентність таких кримінальних правопорушень та недосконаліть їх розслідування зі сторони правоохоронних органів [2, с. 14; 3, с. 121]. Слід також зазначити, що у вітчизняній правовій науці досі існують прогалини в дослідженні саме проблем кримінально-правової кваліфікації кримінальних правопорушень, передбачених ст. 361[1] КК України, оскільки, здебільшого, українські науковці у своїх дослідження зосереджують свою увагу на системному аналізі розділу XVI Особливої частини Кримінального кодексу України без урахування наявної судової практики та проблем, що виникають внаслідок правозастосування норм, що містяться у вищезгаданому розділі.

Попри наявність глибинних напрацювань щодо кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України, станом на сьогодні доцільно дослідити наявну судову практику з метою з'ясування окремих проблем кримінально-правової кваліфікації саме кримінальних правопорушень, передбачених ст. 361[1] КК України.

Виклад основного матеріалу. Шляхом прийняття Закону України (далі – ЗУ) «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23 грудня 2004 року [4] Кримінальний кодекс України було доповнено статтею 361[1] «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут». Питання кримінально-правової кваліфікації кримінального правопорушення, передбаченого ст. 361[1] КК України становить значний не лише науковий, а й практичний інтерес. Аналіз релевантної судової практики свідчить про наявність неоднорідного тлумачення вказаної норми.

У процесі дослідження було проаналізовано судову практику на основі відкритих даних з Єдиного державного реєстру судових рішень, з огляду на яку виокремлено таку тенденцію, за весь період існування вказаної статті судом ухвалено 166 вироків, серед яких:

Виправдувальні вироки. Всього згідно з даними реєстру налічується 7 виправдувальних вироків суду (6 – набрало законної сили, 1 – по справі № 591/4800/17 відповідно до постанови колегії суддів Третьої судової палати Верховного Суду Касаційного кримінального суду від 15 травня 2024 року скасовано ухвалу Сумського

апеляційного суду від 19 жовтня 2023 року та призначено на новий розгляд у суді апеляційної інстанції. Станом на жовтень 2024 року справа досі розглядається в апеляційній інстанції). Аналізуючи виправдувальний вирок Галицького районного суду міста Львова по справі № 461/3281/21, останній дійшов до висновку про відсутність складу інкримінованого кримінального правопорушення з огляду на відсутність умислу на створення шкідливого програмного забезпечення з огляду на той факт, що обвинуваченим у рамках вказаного кримінального провадження був працівник НУ «Львівська політехніка», який згідно з матеріалами, розробив і використав у навчальних цілях. На думку суду, шкода інформаційним відносинам завдана не була. Зазначив, що для унеможливлення списування, програма під час роботи блокує доступ студентів до сторонніх програм та доступ до мережі Інтернет. Суд зазначає, саме ця властивість програми містить ознаки шкідливості програмного забезпечення, однак шкідливою, не зважаючи на це, не є. Відсутність розповсюдження аргументувалося метою використання виключно для перевірки знань студентів, вважаємо такий висновок сумнівним, з огляду на той факт, що розповсюдження суд ідентифікує як оплатну чи безоплатну передачу у будь-який спосіб зазначених засобів відносно широкому і невизначеному колу осіб (фізичних чи юридичних), навіть через систему Інтернет. Хоча далі, в тексті рішення є суперечність, в мотивувальній частині вироку, коли суд вказує на відсутність умислу щодо створення і розповсюдження, а вкінці спростовує взагалі факт розповсюдження, жодним належним та допустимим доказом не підтверджено ні наявність умислу у обвинуваченого на вчинення протиправного діяння, а саме, що обвинувачений чітко усвідомлював, що створювані та розповсюджувані засоби спеціально призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп`ютерів), автоматизованих систем та комп`ютерних мереж, ні шкідливість програмного забезпечення, ні сам факт розповсюдження». Виправданню у зв'язку з відсутністю суб'єктивної сторони підлягала також особа у справі № 591/4800/17. З огляду на те, що програмне забезпечення було завантажене з мережі Інтернет, судом було встановлено відсутність такої ознаки складу як вина, одночасно наявність прямого умислу не була підтверджена іншими належними та допустимими доказами.

Обвинувальні вироки суду. Всього проаналізовано 158 обвинувальних вироків суду, з числа яких: 79 обвинувальних вироків суду, за матеріалами кримінального провадження яких обвинувачений визнав свою вину; 6 обвинувальних вироків суду, за матеріалами кримінального провадження яких обвинувачений заперечив свою вину; 73 обвинувальних вироки (з затвердженням угоди обвинуваченого з прокурором).

Таким чином, якщо брати до уваги відсоткове співвідношення, то виправдувальні вироки становлять лише 4,22% зі всієї кількості ухвалених вироків (при розрахунку бралося до уваги 7 виправдувальних вироків, один з яких станом на момент публікації не набрав законної сили), одночасно ж обвинувальні – 95,78% (з яких у 96,2% випадках особа визнала свою вину; 3,8% – особа, заперечила свою вину). Така тенденція є доволі контраверсійною та викликає значний інтерес для подальшого наукового дослідження, оскільки остання може свідчити або ж про високий рівень підготовки органами досудового розслідування матеріалів до суду, що містять докази на підтвердження усіх елементів складу відповідного кримінального правопорушення, або ж про те, що суди надають поверхневу оцінку з огляду на недостатність спеціальних знань, що породжує «обвинувальний ухил» при розгляді відповідної категорії справ.

Щодо моменту закінчення кримінального правопорушення. За конструкцією об'єктивної сторони кримінальне правопорушення, передбачене ст. 361^1 КК України має формальний склад, тобто останнє вважається закінченим з моменту вчинення діяння. Такий висновок можна зробити, виходячи з буквального тлумачення диспозиції кримінально-правової норми, передбаченої ст. 361^1 КК України. У такому ж ключі висловився ККС ВС у постанові від 15.05.2024 у справі № 591/4800/17 [5], де зазначено, що настання суспільно-небезпечних наслідків у вигляді порушення нормальної роботи комп'ютера чи комп'ютерної мережі, а також знищення, пошкодження чи зміни комп'ютерної інформації, яка зберігається на комп'ютері, тощо, є закінченим з моменту передачі іншій особі хоча б однієї такої програми чи технічного пристрою. Втім, окремої уваги заслуговує уваги питання тлумачення поняття «передача», адже специфікою «комп'ютерних кримінальних правопорушень» є те, що така передача може відбуватися не традиційно шляхом надсилання чи вручення диску, флеш-накопичувача певній особі, а, наприклад, розміщення шкідливого програмного забезпечення на певний інтернет-ресурсах. Відтак, постають логічні питання:

Чи можна вважати передачею розміщення у відкритому або обмеженому доступі шкідливого програмного забезпечення? Вважаємо, що розповсюдження в контексті розміщення шкідливого програмного забезпечення в мережі Інтернет має місце за умови: а) розміщення у відкритому доступі, при якому будь-який користувач має

змогу знайти і завантажити відповідне програмне забезпечення без утруднення пошуку останнього; б) розміщення з обмеженим доступом (у випадку, якщо особа передає паролю (ключ) доступу хоча б одній третій особі).

Як трактувати розміщення програмного забезпечення без пароля, за тієї умови, що знайти відповідне забезпечення зможе лише користувач, який має повний текст IP адреси? IP адреса складається з двох елементів, номера мережі та номера вузла, кількість символів та традиційно складається з чотирьох наборів цифр, однак їх кількість може варіюватися з огляду на тип такої адреси. Вважаємо, що у таких випадках факт розповсюдження матиме місце лише у випадку, якщо власник чи володілець такого програмного забезпечення надасть третій особі конкретну IP адресу для переходу, а за відсутності передачі такої адреси – останню можна позиціонувати як таку, що є з обмеженим доступом.

Щодо розповсюдження та збуту. Особливістю диспозиції кримінально-правової норми, що передбачена ч. 1 ст. 361[1] КК України, є те, що розповсюдження та збут у випадку створення шкідливих програмних чи технічних засобів виступає як мета, а також як самостійні форми діяння. Таким чином, вчинення збуту чи розповсюдження є закінченими з моменту передачі хоча б одній особі шкідливого програмного забезпечення чи технічного пристрою, а в контексті створення доказуванню підлягає наявність мети подальшого збуту чи розповсюдження, за відсутності мети особа не підлягає кримінальній відповідальності за створення шкідливого програмного чи технічного засобу. Такої ж позиції притримується ККС ВС у вищезгаданій постанові від 15 травня 2024 року у справі № 591/4800/17. Втім, не можемо погодитися з формулюванням висновку суду щодо такого «виправдання судом обвинуваченого у зв'язку з відсутністю в його діянні окремих елементів складу кримінального правопорушення, передбаченого ст. 361[1] КК України, є неправильним застосуванням закону України про кримінальну відповідальність». Указані висновки можуть неоднозначно тлумачитися, адже як відомо, відсутність хоча б одного з елементів складу кримінального правопорушення зумовлює відсутність підстав для притягнення до кримінальної відповідальності. У постанові ВС колегії суддів Першої судової палати Касаційного кримінального суду від 27 вересня 2021 року у справі № 570/2835/16-к [6] прийшов до висновку про наявність в діях особи складу кримінального правопорушення, передбаченого ст. 361[1] КК України та констатував факт наявності втручання в роботу автоматизованої системи та нейтралізації її засобу інтелектуального захисту, в результаті чого було порушено порядок маршрутизації інформації в ній. Також, вказав, що будь-яке використання чи розповсюдження програмного забезпечення без дозволу правовласника на безкоштовне його використання є незаконним.

Відсутність єдиного підходу до тлумачення термінології. На сьогодні відсутнє формалізоване визначення понять «шкідливе програмне забезпечення» «автоматизована система», що зумовлює неоднорідність та поверхневість тлумачення вказаних понять. Цей факт є серйозною проблемою, адже прямо впливає на можливість притягнення до кримінальної відповідальності особи. На неправильності тлумачення поняття «автоматизована система» вказував ВС у своїй постанові, зазначивши, що автоматизованою системою є кілька (система) комп'ютерів, об'єднаних між собою у спільну автоматизовану систему. Натомість судами першої і апеляційної інстанції вказане поняття трактувалося, як окреме програмне забезпечення, яким особа скористалася без відповідного дозволу.

Шкідливість як ознака програмного чи технічного засобу. Досліджуючи питання ідентифікації шкідливого програмного забезпечення в контексті кримінально-правової кваліфікації з'ясовано, що з практики, програмне забезпечення в переважній кількості випадків ідентифікується як шкідливе за допомогою інтернет-ресурсу *«Virus Total» (https:www.virustotal.com).* Вважаємо такий механізм ідентифікації недосконалим та таким, що безпосередньо може вплинути на права та законні інтереси громадян. На сайті вказаного інтернет-ресурсу зазначено, що ця програма працює на основі 70 антивірусів-сканерів та служб-блокування доменів. Адміністратором вебсайту розміщена інформація щодо обмеження відповідальності (з указаною інформацією більш детально можна ознайомитися при переході на веб-сайт за адресою: https://docs.virustotal.com/docs/contributors) за помилкові спрацьовування, створені будь-якими ресурсами, які він використовує. Проблеми з хибними спрацьовуваннями слід вирішувати безпосередньо з компанією чи особою, яка стоїть за продуктом, який розглядається. Отже, за змістом вказаний інтернет-ресурс працює на основі антивірусів та фактично відображає звіт за результатами спрацювання антивірусів. Тому, вважаємо, що віднесення конкретного програмного забезпечення до категорії шкідливих повинне встановлюватися на основі усталеної методики та з огляду на обставини конкретного кримінального провадження.

У проєкті КК України (в редакції від 01.09.2024) автори формалізують поняття інформаційна система, несанкціоноване діяння щодо інформаційної системи, шкідливий програмний засіб, шкідливий технічний засіб, шкідливі дані (дані доступу) [7].

Висновки. Відтак, підсумовуючи вищевикладене, вважаємо, що: по-перше, станом на сьогодні наявна проблема у кваліфікації кримінального правопорушення, передбаченого ст. 361^1 КК України через відсутність єдиного підходу до розуміння понять, які вживаються у диспозиції вищезазначеної норми: «шкідливе програмне забезпечення», «автоматизована система», «розповсюдження»; по-друге, доцільно уніфікувати методологію визначення програмного забезпечення як шкідливого; по-третє, Верховному Суду слід зосередитися на формуванні єдиного та сталого підходу до правозастосування норм, передбачених ст. 361^1 КК України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний кодекс України від 5 квітня 2001 року. *Відомості Верховної Ради України*. 2001. № 25-26. URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення 14.10.2024).
2. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінальноправове дослідження): [монографія]. К.: Атіка, 2007. 304 с.
3. 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.* 2022. № 1. С.270-275. URL: http://nbuv.gov.ua/jpdf/FP_index.htm_2016_1_7.pdf (дата звернення: 14.10.2024).
4. Про внесення змін до Кримінального та Кримінально-процесуального кодексів України. *Відомості Верховної Ради України*. 2005. № 6. URL: https://zakon.rada.gov.ua/laws/show/2289-15#Text (дата звернення 14.10.2024).
5. Постанова колегії суддів Третьої судової палати Касаційного кримінального суду Верховного Суду від 15.05.2024. URL: https://reyestr.court.gov.ua/Review/119168551 (дата звернення 14.10.2024).
6. Постанова колегії суддів Першої судової палати Касаційного кримінального суду Верховного Суду від 27.09.2021. URL: https://reyestr.court.gov.ua/Review/100109379 (дата звернення 14.10.2024).
7. Контрольний текст проєкту Кримінального кодексу України станом на 01.08.2024. URL: https://newcriminalcode.org.ua/upload/media/2024/08/02/kontrolnyj-tekst-proyektu-kk-stanom-na-01-08-2024.pdf (дата звернення 14.10.2024).