УДК 343.9
DOI https://doi.org/10.32844/2618-1258.2021.6.2.40

ВОЛКОВ О.О.

СПОСОБИ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ВИКОРИСТАННЯ, РОЗПОВСЮДЖЕННЯ АБО ЗБУТУ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ: ОКРЕМІ АСПЕКТИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ

METHODS OF COMMITTING CRIMINAL OFFENSES IN THE SPHERE OF USE, DISTRIBUTION OR SALE OF HARMFUL SOFTWARE OR TECHNICAL MEANS: CERTAIN ASPECTS OF CRIMINAL CHARACTERISTICS

У статті проаналізовано способи вчинення кримінальних правопорушень усфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. Установлено, що відповідна категорія кримінальних правопорушень є однією з найбільш небезпечних, зокрема й в умовах стрімкого збільшення злочинних посягань, а також системно здійснюваних трансформаційних процесів у правоохоронній системі. Автором було здійснено аналіз окремих аспектів криміналістичної характеристики вчинення кримінальних правопорушень у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів і надано визначення основним дефініціям і поняттям, а зокрема способам учинення відповідного правопорушення в контексті науки криміналістики та шкідливих програмних чи технічних засобів, що й формують (є підставою) специфічності процесу досудового розслідування відповідного правопорушення. Крім цього, досліджено спосіб учинення кримінального правопорушення у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів як основну й характерну для нього рису. Класифікація способів учинення відповідних діянь охоплює основні напрями розповсюдження комп'ютерного вірусу, але не відображає їх механічної специфіки щодо кримінального умислу злочинця. Основним критерієм активного та пасивного ураження як способу вчинення злочину, на наш погляд, виступає кримінально-правова характеристика мети вчинення злочину, яка відображає криміналістичні особливості, такі як у першу чергу слідова картина способів. Способи використання і поширення шкідливих програмних засобів можуть бути класифіковані за різними підставами, які в подальшому будуть мати значення для криміналістичної характеристики. Основна їх класифікація, ґрунтується на поділі всіх способів на дві основні групи: активні і пасивні. Активні способи вчинення злочинів пов'язані з безпосереднім впливом злочинця на засоби комп'ютерної техніки. Тобто злочинець сам здійснює взаємодію з ЕОТ або їх мережею, завантажуючи шкідливий програмний засіб та використовуючи її. Потерпіла сторона або не знає про сам факт впровадження шкідливого програмного засобу, або не усвідомлює її шкідливий характер. До пасивних способів використання та поширення відносяться всі способи дій злочинця, спрямовані на створення умов, при яких користувач (користувачі) ЕОТ або їх мережі, самостійно або опосередковано під виглядом доброякісної програми отримують шкідливі програмні засоби.

Ключові слова: *криміналістика, шкідливі програмні засоби, шкідливі технічні засоби, способи вчинення, кримінальний процес, досудове розслідування.*

The article analyzes the methods of committing criminal offenses in the sphere of use, distribution or sale of malicious software or technical means. It was established that the corresponding category of criminal offenses is one of the most dangerous, in particular, in the conditions of a rapid increase in criminal offenses, as well as systematically

© ВОЛКОВ О.О. – начальник сектору Головного слідчого управління Національної поліції України

implemented transformational processes in the law enforcement system. The author carried out an analysis of certain aspects of the forensic characteristics of the commission of criminal offenses in the sphere of the use, distribution or sale of malicious software or technical means and defined the main definitions and concepts, and in particular the methods of committing the corresponding offense in the context of the science of forensics and malicious software or technical means, as well as form (are the basis of) the specifics of the process of pretrial investigation of the relevant offense. In addition, the method of committing a criminal offense in the field of use, distribution or sale of malicious software or technical means as its main and characteristic feature has been investigated. The classification of the methods of committing the relevant acts covers the main directions of computer virus distribution, but does not reflect their mechanical specificity in relation to the criminal intent of the criminal. In our opinion, the main criterion of active and passive damage as a method of committing a crime is the criminal-legal characteristics of the purpose of committing the crime, which reflects forensic features, such as, first of all, the trace pattern of the methods. Ways of using and spreading malicious software can be classified on various grounds, which will be important for forensic characterization in the future. Their main classification is based on the division of all methods into two main groups: active and passive. Active ways of committing crimes are related to the direct influence of the criminal on computer equipment. That is, the criminal himself interacts with the EOT or their network by downloading and using a malicious software tool. The affected party either does not know about the very fact of introducing a malicious software tool, or is not aware of its malicious nature. Passive methods of use and distribution include all methods of the criminal's actions, aimed at creating conditions in which the user(s) of EOT or their networks, independently or indirectly under the guise of a benign program, receive malicious software.

Key words: *forensics, malicious software, malicious technical means, methods of committing, criminal process, pre-trial investigation.*

Актуальність тематики. Криміналістичний аналіз вчинення злочинів, пов'язаних із шкідливими програмними заходами уявляє собою певну структуру, у якій одне з основних місць належить вивченню способів вчинення досліджуваних злочинів, як одного з найбільш специфічних інструментів злочинної діяльності, оскільки вчинити подібні злочини можуть тільки висококваліфіковані спеціалісти, що і ускладнює механізми розслідування, кваліфікації і профілактики даних злочинних проявів.

За результатами соціологічних досліджень, на кіберзлочинність припадає 23% випадків шахрайства у світі, 17% – в Україні. Дані також свідчать про те, що кіберзлочини стають витонченішими, що ускладнює їхнє виявлення й запобігання. Це може призвести до ще більших збитків і втрат у майбутньому. 36% респондентів в Україні вважають, що кіберзлочинність – це зовнішня загроза, 24% – внутрішня. На думку 34% респондентів, загроза може йти як ззовні, так і зсередини організації. Ці показники трохи відрізняються від результатів Всесвітнього огляду, оскільки в організаціях інших країн відзначають, що ризик такої злочинності переважно йде ззовні (46%) і тільки 13% переконані, що злочин вчиняли співробітники фірм і корпорацій. Основними кібершахраями визнані клієнти й постачальники [1].

Метою статті є аналіз окремих аспектів криміналістичної характеристики вчинення кримінальних правопорушень у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. Така мета, на нашу думку потребує розв'язання таких дослідницьких завдань, як: 1. Надання визначення основним дефініціям і поняттям; 2. Дослідження способу вчинення кримінального правопорушення у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів як основну й характерну для нього рису.

Об'єктом статті виступають суспільні відносини, в сфері досудового розслідування кримінальних правопорушень пов'язаних із використанням, розповсюдженням або збутом шкідливих програмних чи технічних засобів.

Предметом дослідження є способи вчинення кримінальних правопорушень у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів.

Виклад основного матеріалу статті. Правова наука визначає спосіб вчинення злочину як форму прояву суспільно небезпечного діяння тобто прийоми і методи, які використовував

злочинець для вчинення злочину [2, с. 119]. Кримінально-правове визначення поняття способу вчинення злочину, як факультативної ознаки об'єктивної сторони складу злочину дещо відрізняється від свого криміналістичного аналогу. Відповідно до положень криміналістичної науки, способом вчинення злочину прийнято вважати прояв діяльності суб'єкта (не тільки його поведінку, а й закономірне відтворення використання предметів – засобів діяльності), опосередкований об'єктивними умовами, в яких виникла й розвивалася протиправна дія [3].

Як правило, така діяльність стосується підготовки, вчинення і приховування злочинного діяння. Проте не обов'язково, щоб спосіб мав усі названі елементи. Існують злочини, в яких злочинець з низки причин не здійснює ніяких дій з їх приховання або не може їх здійснити (наприклад, через неадекватний психічний стан злочинця і так далі). Але такі факти зустрічаються досить рідко. Здебільшого під час учинення злочинів, що вимагають від злочинця інтелектуального підходу, він намагається приховати злочин шляхом знищення залишених слідів, а крім того, і вживання заходів, щоб таких слідів не залишати, фальсифікації обстановки події або самих слідів та ін. Мета цих дій, з одного боку, перешкодити своєчасному виявленню злочину, з другого – перешкодити встановленню особи злочинця [4, с. 284].

Наслідки вчинення злочину з використанням шкідливих програмних засобів не завжди можуть відображати способи їх вчинення, оскільки інколи про вчинення даного злочину можуть свідчити тільки негативні соціальні зміни. Спосіб вчинення досліджуваного злочину тісно пов'язаний з технологічними особливостями створення, використання, розповсюдження або збуту шкідливих програмних засобів. Слід погодитись із Р.С. Бєлкіним у тому, що «просто описання способу вчинення злочину не досягає мети», необхідно виявити сліди застосування цього способу з тим, щоб за ними розкривати механізм злочину, зуміти виявити докази вчиненого злочину й встановити особу злочинця [5, с. 314].

Як слушно наголошує Д.В. Пашнєв, у криміналістиці такі злочини варто називати «злочинами, скоєними з використанням комп'ютерних технологій». Такий термін буде вказувати на саму технологію здійснення злочинів, що визначає способи їх скоєння. Крім того, комп'ютерні технології розроблені для обробки інформації в цифровому виді, яка і є, зрештою, предметом злочинного посягання даних злочинів. Таким чином, термін «злочини, скоєні з використанням комп'ютерних технологій» дозволить охопити всі діяння, вчинені з використанням досягнень цих технологій і такі, що посягають на оброблювану комп'ютерну інформацію [6, с. 109].

У криміналістичному аспекті таке об'єднання важливе з тієї точки зору, що дозволить виробити і застосовувати на практиці універсальні прийоми, способи, засоби і методи виявлення, фіксації і дослідження комп'ютерної інформації, що є криміналістично значущою при розслідуванні злочинів, елементом об'єктивної сторони яких є засіб комп'ютерної техніки, незалежно від кримінально-правової кваліфікації такого діяння. Одним з найважливіших визначальних факторів у боротьбі з даними злочинами є сфера їх вчинення, точніше середовище. Вони відбуваються в кіберпросторі – області находження комп'ютерної інформації, утвореній сукупністю засобів комп'ютерної техніки [7, с. 41]. Отже, спосіб вчинення досліджуваного злочину безпосередньо виражений у формі створення, використання, розповсюдження або збуту шкідливих програмних засобів.

У той же час не можна не звернути уваги на те, що наведене в законі визначення є некоректним з точки зору сутності поняття «розповсюдження комп'ютерного вірусу». За особливостями розповсюдження комп'ютерні віруси поділяються на файлові, бутові (завантажувальні) та мережні. До файлових вірусів відносяться такі, що розповсюджуються шляхом упровадження в командні, виконавчі файли або файли драйверів, які завантажуються, тобто програм, до яких звертається і з якими працює користувач. Бутові віруси, або віруси, що завантажуються, розповсюджуються шляхом «зараження» завантажувального сектора гнучкого або жорсткого носія. Мережні віруси використовують для свого розмноження можливості спеціального програмного забезпечення, яке організовує функціонування комп'ютерної мережі. Наслідки використання таких вірусів, як правило, полягають у переповненні пам'яті комп'ютера, підключеного до мережі, копіями вірусу, що призводить до неможливості роботи з інформацією, яка міститься в цій ЕОМ [8, с. 87–88].

Отже, як наголошує М.М. Коваленко, розповсюдження комп'ютерного вірусу можна здійснити трьома способами: упровадженням вірусу в програми; «зараженням» завантажувального сектора носія; розповсюдженням вірусу з використанням мережного програмного забезпечення [9, с. 140].

Проте, на наш погляд дана класифікація охоплює основні напрями розповсюдження комп'ютерного вірусу, але не відображає їх механічної специфіки щодо кримінального умислу злочинця.

Основним критерієм активного та пасивного ураження як способу вчинення злочину, на наш погляд, виступає кримінально-правова характеристика мети вчинення злочину, яка відображає криміналістичні особливості, такі як у першу чергу слідова картина способів.

Способи використання і поширення шкідливих програмних засобів можуть бути класифіковані за різними підставами, які в подальшому будуть мати значення для криміналістичної характеристики. Основна їх класифікація, ґрунтується на поділі всіх способів на дві основні групи: активні і пасивні.

Активні способи вчинення злочинів пов'язані з безпосереднім впливом злочинця на засоби комп'ютерної техніки. Тобто злочинець сам здійснює взаємодію з ЕОТ або їх мережею, завантажуючи шкідливий програмний засіб та використовуючи її. Потерпіла сторона або не знає про сам факт впровадження шкідливого програмного засобу, або не усвідомлює її шкідливий характер.

До пасивних способів використання та поширення відносяться всі способи дій злочинця, спрямовані на створення умов, при яких користувач (користувачі) ЕОТ або їх мережі, самостійно або опосередковано під виглядом доброякісної програми отримують шкідливі програмні засоби.

Основна відмінність пасивних способів від активних полягає в тому, що між самим злочинцем і засобами комп'ютерної техніки, на яких буде використовуватися шкідливий програмний засіб, є проміжна ланка (або ланки), користувач, який і здійснює безпосередню взаємодію із засобами комп'ютерної техніки. Чи є такий користувач законним чи незаконним не має принципового значення для описуваних способів використання та поширення.

Потерпілий в даному випадку може знати про встановлення шкідливого програмного засобу, але не знає про наявність в ній шкідливих функцій. Активні способи використання і поширення шкідливих програмних засобів містять у собі багатоступеневу структуру. Всього в діях злочинця можна виділити три основні етапи:

1. Доступ до конкретної ЕОТ або їх мережі.

2. Доступ до програмного забезпечення, що забезпечує роботу з файлами даних або безпосередньо до файлів даних.

3. Завантаження шкідливого програмного засобу в ЕОТ або в їх мережу.

Використання і поширення шкідливих програмних засобів може здійснюватися як в разі правомірного, так і неправомірного доступу до засобів ЕОТ.

У разі правомірного доступу значно полегшується підготовка проникнення до конкретної ЕОТ або їх мережі та до комп'ютерної інформації, однак зазначені перші два етапи присутні все одно, в той час як третій етап – завантаження шкідливого програмного засобу в ЕОТ, залишається незмінним за своїм змістом.

Виходячи з цього, всі способи вчинення таких злочинів на погляд Н.Г. Шурухнова можна поділити використовуючи класифікацію способів здійснення несанкціонованого доступу до комп'ютерної інформації. До таких груп способів вчинення відносять:

– способи безпосереднього доступу до комп'ютерної інформації та подальша установка (інсталяція) шкідливого програмного засобу на ЕОТ або в їх мережу;

– способи опосередкованого (віддаленого) доступу до комп'ютерної інформації та подальша установка шкідливого програмного забезпечення на ЕОТ або їх мережу;

– змішані способи доступу, які можуть здійснюватися як шляхом безпосереднього, так і опосередкованого (віддаленого) доступу з подальшою установкою шкідливого програмного засобу на ЕОТ або в їх мережу. [10, с. 103–110].

Висновки. Таким чином у змісті статті автором було здійснено аналіз окремих аспектів криміналістичної характеристики вчинення кримінальних правопорушень у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів і надано визначення основним дефініціям і поняттям, а зокрема способам учинення відповідного правопорушення в контексті науки криміналістики та шкідливих програмних чи технічних засобів, що й формують (є підставою) специфічності процесу досудового розслідування відповідного правопорушення. Крім цього, досліджено спосіб учинення кримінального правопорушення у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів як основну й характерну для нього рису.

Список використаних джерел:

1. Кіберзлочинність в Україні зростає : дані звіту PricewaterhouseCoopers. URL: http://ladynews.com.ua/newsline/kiberprestupnost-v-ukraine-nabiraet-oboroty-96603.html.

2. Кримінальне право України. Загальна частина : підручник. К. : «Правові джерела». 2002. С. 425.

3. Криміналістика (криміналістична техніка) : курс лекцій / П. Д. Біленчук, А. П. Гель, М. В. Салтевський, Г. С. Семаков. К. : МАУП, 2001. 216 с.

4. Школьний Б.В. Питання загальної теорії слідоутворення у контексті боротьби з кіберзлочинністю. *Юридична психологія та педагогіка.* 2011. № 1(9). С. 284–287.

5. Белкин, Р. С. Курс криминалистики : в 3-х т. ; т. 3: Криминалистические средства, приёмы и рекомендации. М. : Юристъ, 1997. 480 с.

6. Пашнєв Д.В. Особливості виявлення і фіксації криміналістично значимої комп'ютерної інформації при розслідуванні злочинів. *Право і безпека.* 2003. № 1. С. 108–111.

7. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. 2002.

8. Карчевський М.В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : дис. ... канд. юрид. наук: 12.00.08 / Нац. юрид. акад. України ім. Я. Мудрого. Х., 2003. 175 с.

9. Коваленко М.М. Комп'ютерні віруси і захист інформації. К. : Наукова думка, 1999. С. 138–143.

10. Расследование неправомерного доступа к компьютерной информации / Под ред. Н.Г. Шурухнова. М.: Издательство «Щит-М», 1999. С. 103–110.