О.О. Кирбят`єв
ад'юнкт
(Дніпропетровський державний університет внутрішніх справ)

УДК 343.3

ДІЯННЯ ЯК ОЗНАКА ОБ'ЄКТИВНОЇ СТОРОНИ СКЛАДУ ЗЛОЧИНУ, ПЕРЕДБАЧЕНОГО ст. 361-1 КК УКРАЇНИ

Проаналізовано діяння як ознаку об'єктивної сторони створення, розповсюдження або збуту шкідливих програм чи технічних засобів, а саме: визначено поняття "незаконне створення", "розповсюдження", "збут" шкідливих програмних чи технічних засобів.

Ключові слова: *шкідлива програма, шкідливий технічний засіб, комп'ютерна інформація, розповсюдження, збут.*

Проанализировано деяние как признак объективной стороны создания, распространения или сбыта вредоносных программ или технических средств, а именно: определены понятия "незаконное создание", "распространение", "сбыт" вредоносных программ или технических средств.

Ключевые слова: *вредоносная программа, вредносное техническое средство, компьютерная информация, распространение, сбыт.*

The article is devoted the analysis of act as a sign of objective side of creation, distribution or sale of the harmful programs or hardwares, namely: to the decision of concepts "illegal creation", "distribution", "sale" of the harmful programs or hardwares.

Keywords: *harmful program, harmful hardware, computer information, distribution, sale.*

Постановка проблеми. Створення, розповсюдження або збут шкідливих програм, часто є першою ланкою в ланцюзі скоєння злочинів у сфері комп'ютерної інформації, служить першоосновою для формування цього виду правопорушень, що зачіпають цілий комплекс суспільних відносин, які складаються з приводу використання комп'ютерної інформації, а значить охоплюють велику частину сфер життя сучасного суспільства. Для забезпечення ефективної протидії такому делікту важливо чітко визначити ознаки об'єктивної сторони цього виду злочинів.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. До аналізу ознак об'єктивної сторони створення, розповсюдження або збуту шкідливих програмних чи технічних засобів зверталися такі вітчизняні та зарубіжні науковці як П.Д. Біленчук, В.О. Голубєв, М.В. Карчевський, Ю.І. Ляпунов, В.Ю. Максимов, Д.Г. Малишенко, Т.В. Михайліна, М.М. Менжега, С.В. Полубінська, Н.А. Розенфельд та інші.

Мета статті полягає у характеристиці ознак об'єктивної сторони складу злочину, передбаченого ст. 361-1 КК України «Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку».

Виклад основного матеріалу. З моменту, коли комп'ютерні злочини опинилися у сфері уваги учених-правознавців, проблема визначення об'єктивної сторони комп'ютерних, злочинів вийшла на перший план. Об'єктивній стороні складу злочину завжди притаманна певна сукупність ознак, „але не всі ознаки об'єктивної сторони входять до кожного складу злочину, а тому не всі вони мають значення для кваліфікації" [1]. І.А. Вартилецька серед ознак об'єктивної сторони складу злочину виділяє: обов'язкові для формальних складів (лише суспільно небезпечне діяння); обов'язкові для матеріальних складів (суспільно небезпечне діяння, причинний зв'язок, суспільно небезпечні наслідки) та факультативні (місце, час, обстановка, знаряддя, засоби, спосіб) [2], що, на нашу думку, є повністю обґрунтованим.

Отже центральним елементом об'єктивної сторони будь-якого складу злочину є діяння у формі дії чи бездіяльності. Під суспільно небезпечною дією розуміється активний, вольовий, свідомий акт зовнішньої поведінки суб'єкта, який відображається у вчиненні суспільно небезпечного посягання.

Останнім часом все більше уваги приділяється питанням безпеки комп'ютерної інформації, комп'ютерних систем і мереж передачі даних. Основне питання захисту інформації в комп'ютері лягає на спеціально розроблене програмне забезпечення – так звані антивірусні програми, міжмережеві екрани. Сьогодні існує чимала кількість компаній, що виробляють антивірусні програми захисту (Антивірус Касперського, Drweb, Eset Nod32, Panda Antivirus, Symantec Antivirus, Trend Micro, Bitdefender, Avast, Mcafee). За родом своєї діяльності всі ці компанії безпосередньо пов'язані зі шкідливими програмами, можуть створювати і вносити зміни до існуючих програм. Проте вони мають на меті забезпечення безпеки, хоча, з точки зору Кримінального кодексу, в їх діяльності є формальні ознаки складу злочину, передбаченого ст. 361-1 КК.

Таким чином, створення спеціальних програм, що мають у тому числі і шкідливі властивості (в їх кримінально-правовому розумінні), може бути одним із засобів захисту інформації, засобом контролю ефективності захисту інформації, а також одним із способів проведення спеціальних заходів при здійсненні контртерористичної операції.

Перекручення, доповнення, видалення, дублювання частини програмного коду й інші модифікації – неповний перелік змін, які можуть бути внесені до існуючої програми, у тому числі додавання їй шкідливих властивостей, яких раніше не було. Виникає ще одне питання: при видаленні зі шкідливої програми її шкідливих властивостей програма перестає бути шкідливою, а значить і особа, що внесла до неї подібні зміни, не підлягає кримінальній відповідальності? У той же час при внесенні змін до існуючої шкідливої програми вона може втратити не всі свої шкідливі властивості. І тоді це діяння не можна назвати злочинним, оскільки жодні шкідливі властивості до існуючої програми не вносилися, хоча, з іншого боку, така зміна може бути зроблена в цілях поліпшення алгоритму функціонування програми, додавання їй властивостей, що перешкоджають швидкому виявленню.

Процес програмування, тобто створення програми, процес творчий, що здійснюється шляхом внесення змін у існуючі програми. Створення програми шляхом внесення змін до існуючої програми характеризується збереженням хоч би частини її первинних функцій або її зовнішнього вигляду.

Не повинно бути і заборони на будь-яке створення шкідливої програми, оскільки, наприклад, це може призвести до закриття й припинення наукових та дослідницьких розробок. Аналогічної позиції дотримується і В. Ю. Максимов: «Не можна забороняти будь-яке створення комп'ютерних вірусів, що мають шкідливі властивості, оскільки це може відбуватися і в суспільно корисних цілях» [3]. У зв'язку з цим ми вважаємо своєчасними, виправданими як диспозицію статті, так і її назву почати словом «Незаконне», доповнивши відповідні нормативні документи випадками законного поводження з програмами, що мають властивість шкідливості.

Об'єктивна сторона, що полягає у використанні і розповсюдженні шкідливих програм, представляється нам найбільш небезпечною дією, у тому числі і з точки зору настання наслідків. Якщо при створенні шкідливої програми існує імовірність неспричинення шкоди комп'ютерній інформації, то явне використання і розповсюдження такої програми обов'язково призведе до негативних наслідків, завдавши значної шкоди. Створення шкідливих технічних засобів полягає у виготовленні будь-яким способом відповідного пристрою (обладнання). Причому, зважаючи на специфічність такого устаткування, виготовлення може полягати не лише у його фізичному збиранні, а й, наприклад, у налагодженні устаткування відповідним чином або його перепрограмуванні, після чого пристрій набуватиме шкідливих ознак.

З приводу використання шкідливих програм у кримінально-правовій літературі існує декілька не завжди співпадаючих точок зору. Так, на думку А.Н. Попова, «Використання – випуск у світ, відтворення, розповсюдження і інші дії з введення у господарський обіг». А.В. Пушкін розуміє під використанням «введення (установку) в пам'ять комп'ютера» [4]. Б.В. Коробєйників вважає, що використання – це «вживання розроблених винною або іншою особою шкідливих програм при експлуатації ЕОМ та обробці інформації». На думку Ю.Л. Красикова, використання – «обіг, вживання їх за призначенням, приведення в дію, коли вони починають проявляти свої шкідливі якості» [5].

Перше наведене нами формулювання розуміння «використання» нічим не відрізняється від розповсюдження шкідливих програм, яке криміналізується в даній статті окремо, друге ж має на увазі, що введення шкідливої програми в чужий комп'ютер є тотожним його розповсюдженню, а якщо у свій, то – створенню. Ми вважаємо, що дія з використання шкідливої програми – це поводження зі свідомо готовими предметами, тому це ніскільки не змінює їх якостей і функцій, а, навпаки, проявляє і підсилює їх. Таким чином, на нашу думку, має місце витягання вигоди з речі, набуття вдоволення від володіння нею, хоча мова і йде про шкоду.

Використання шкідливої програми – це її використання за призначен-

ням, приведення в дію, при якій вона проявляє свої шкідливі якості. Момент здійснення подібної дії може настати виключно унаслідок властивостей і функцій, закладених у шкідливу програму. Якщо вона розрахована на негайне виконання своїх шкідливих дій, то використання настає з моменту її проникнення в комп'ютер або у пристрій, який використовує обчислювальні компоненти. Якщо ж ми маємо справу з «логічною бомбою» або «закладкою» – з моменту прояву шкідливих властивостей.

Фахівці-правознавці трактують розповсюдження шкідливих програм так. Ю.А. Красиков вважає, що «розповсюдження шкідливих програм або машинних носіїв з такими програмами полягає в будь-якому випуску в обіг (шляхом продажу, обміну, прокату і т. ін.), у наданні доступу до програми, відтвореної в будь-якій матеріальній формі. Як вважає С.В. Полубінська, «розповсюдження програми передбачає надання доступу до неї, якщо програма відтворена в будь-якій матеріальній формі, у тому числі мережевими й іншими способами, а також шляхом продажу, прокату, найму, надання у позику» [6]. Під розповсюдженням шкідливих програмних засобів певні науковці розуміють злочинні дії, за допомогою яких скопійовані шкідливі програми безпосередньо чи опосередковано пропонуються, доводяться або передаються будь-кому як в платний, так і в безоплатний спосіб [7]. Ю.І. Ляпунов вказував, що «розповсюдження шкідливих програм або машинних носіїв з такими програмами полягає в наданні доступу до відтвореної в будь-якій матеріальній формі програми для ЕОМ або бази даних, у тому числі мережевим і іншим способами, а також шляхом продажу, прокату, найми, надання у позику, включаючи імпорт для будь-якої з цих цілей»[8].

Розповсюдження передбачає збільшення дії предмета за межі його створення, існування – розширення «ареалу проживання», сфери застосування. Таким чином, на нашу думку, для шкідливої програми розповсюдженням вважатиметься як будь-який випуск в обіг, будь-яка форма реалізації, надання доступу будь-яким способом з перерахованих для придбання, так і умисна розсилка за адресами електронної пошти. Комп'ютерний вірус, як різновид шкідливих програм, є програмою, що самостійно розповсюджується, проте, процес самостійного переміщення від одного «зараженого» комп'ютера до іншого, від одного файлу до іншого, не виключає тих випадків, коли власник (або автор) такої програми своїми діями допомагає її розповсюдженню, продаючи, даруючи, обмінюючи таку програму, переписуючи, розсилаючи вірус інформаційно-комунікаційними мережами і т. ін.

Більшість з наведених визначень розповсюдження стосуються формулювання диспозиції відповідної норми КК України до внесення в неї змін у 2004 році. Під час внесення змін у диспозиції даної норми було використано два поняття: „розповсюдження” та „збут” шкідливих програмних чи технічних засобів, які потребують відмежування одне від одного.

Кожна шкідлива програма, будучи різновидом комп'ютерної інформації, розуміється в КК як інформація на машинному носієві, в ЕОМ, системі, мережі. Виходячи з технічних особливостей фіксації будь-якої

комп'ютерної інформації, розповсюджуватися шкідлива програма може лише в декількох фізичних формах:

- разом з машинним носієм (наприклад, передача дискети, компакт-диска, флеш-диска та ін.);
- разом з комп'ютером (наприклад, переміщення ноутбука власником з одного місця в інше);
- усередині локальної мережі або в глобальній мережі Інтернет по лініях зв'язку (наприклад, перенесення вірусу з жорсткого диска сервера на локальні комп'ютери або перенесення «зараженого» листа електронною поштою).

Доречно згадати думку Д.Г. Малишенка, який вважає, що «важко розглядати комп'ютерну інформацію поза її матеріальним носієм» [9].

З метою чіткого розмежування зазначених вище понять, розповсюдженням шкідливих програмних засобів пропонуємо вважати передачу фізичного носія зі шкідливими програмними засобами виключно в безоплатний спосіб або передачу шкідливих програм через автоматизовані системи чи комп’ютерні мережі в оплатний чи безоплатний спосіб.

Збутом шкідливих програмних чи технічних засобів деякі науковці вважають платне чи безоплатне відчуження зазначених засобів іншій особі [10]. Причому деякі з них вказують на те, що таке відчуження може здійснюватись у будь-який спосіб, причому завжди конкретно визначеній особі, а не групі (колу) осіб [11]. Але дані твердження унеможливлюють проведення розмежування термінів „розповсюдження” та „збут”.

Що ж стосується шкідливих програмних засобів (які за своєю природою є машинною інформацією, тобто не мають матеріальної форми), то їх збутом пропонується вважати форму передачі або реалізації, внаслідок якої вони передаються у володіння, користування або розпорядження інших осіб виключно на платній основі. Також, на відміну від розповсюдження, під час збуту відбувається відчуження програмних засобів виключно на фізичному носії. Тому не можна вважати збутом платну передачу шкідливих програм в електронному вигляді в мережі Інтернет або локальних мережах, тому що така передача вважатиметься розповсюдженням. Збут шкідливих технічних засобів слід розуміти як передачу або реалізацію відповідного шкідливого пристрою, внаслідок якої він передається у володіння, користування або розпорядження інших осіб виключно на платній основі.

Висновки. На підставі твердження про неможливість заборони створення комп'ютерних вірусів, що мають шкідливі властивості, яке може відбуватися в суспільно корисних цілях, вважаємо виправданим та пропонуємо диспозицію статті 361-1 КК України та її назву почати словом «Незаконне», доповнивши відповідні нормативні документи випадками законного поводження з програмами, що мають властивість шкідливості.

Використання шкідливої програми – це введення її в електронну пам’ять ЕОМ з наступною реалізацією алгоритму, який закладений у неї. Якщо не йдеться про реалізацію алгоритму шкідливої програми, а тільки про її введення в електронну пам'ять ЕОМ, то таку дію пропонується вважати розповсюдженням.

Для чіткого розмежування понять „розповсюдження” та „збут” шкідливих програмних чи технічних засобів, під розповсюдженням шкідливих програмних засобів пропонується вважати передачу фізичного носія зі шкідливими програмними засобами виключно в безоплатний спосіб або передачу шкідливих програм через автоматизовані системи чи комп’ютерні мережі в будь-який спосіб. У свою чергу, під збутом треба розуміти передачу шкідливих програмних засобів виключно на фізичному носії у платний спосіб.

Бібліографічні посилання

1. Матишевський П.С. Кримінальне право України. Загальна частина : підручник / П.С. Матишевський. – К., 2001.

2. Вартилецька І.А. Кримінальне право України. Альбом схем : навч. посіб. / І.А. Вартилецька, В.С. Плугатир; за ред. В.Я.Горбачевського. – К., 2003.

3. Максимов В.Ю. Компьютерные преступления (вирусный аспект) : монография / В.Ю.Максимов. – Ставрополь, 1999.

4. Комментарий к Уголовному Кодексу Российской Федерации (постатейный) / под общ. ред. Н.Г. Кадникова. – М., 2004.

5. Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. В.М.Лебедева.- 2-е изд., перераб. и доп. – М., 2004.

6. Учебный комментарий к Уголовному кодексу Российской Федерации/ отв. ред. А.Э. Жалинский. – М., 2005.

7. Актуальні проблеми кримінального права : навч. посіб. / В.М. Попович, П.А. Трачук, А.В. Андрушко, С.В. Логін. – К., 2009.

8. Уголовное право : учебник. / под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М., 2005.

9. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации : автореф. дис. канд. юрид. наук. – М., 2002.

10. Уголовный кодекс Украины : научно-практ. коммент. / под ред. Е.Л. Стрельцова. – Х., 2007.

11. Кримінальний кодекс України : науково-практ. коментар / Ю.В. Баулін, В.І. Борисов, С.Б. Гавриш та ін.; за ред. В.В. Сташиса, В.Я. Тація]. – Вид. 4-те, доп. – Х., 2008.

Надійшла до редакції 26.10.2012

Р.М. Кубрак
здобувач
(Дніпропетровський державний університет внутрішніх справ)

УДК 343.8

ОКРЕМІ АСПЕКТИ ВИКОНАННЯ ПОКАРАННЯ У ВИДІ ПОЗБАВЛЕННЯ ВОЛІ НА ПЕВНИЙ СТРОК СТОСОВНО ЗАСУДЖЕНИХ З ПСИХІЧНИМИ ВІДХИЛЕННЯМИ

Розглянуто окремі аспекти виконання у виправних колоніях кримінального покарання у виді позбавлення волі на певний строк стосовно засуджених чоловіків та жінок з психічними відхиленнями.

Ключові слова: *психічні відхилення, установи виконання покарань, злочин, кримінальне покарання, суспільно корисні зв'язки, засуджені.*

Рассмотрены отдельные аспекты исполнения в исправительных колониях уголовного наказания в виде лишения свободы на определенный срок в отношении осужденных мужчин и женщин с психическими отклонениями.