Хахановський Валерій Георгійович – кандидат юридичних наук, доцент, професор кафедри інформаційних технологій Національної академії внутрішніх справ

ОСОБЛИВОСТІ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КІБЕРЗЛОЧИНІВ

Висвітлено особливості деяких елементів криміналістичної характеристики кіберзлочинів. Проаналізовано й уточнено певні терміни та поняття у сфері кіберзлочинності.

Ключові слова: кіберзлочинність; криміналістична характерристика кіберзлочинів; хакери; способи вчинення кіберзлочинів.

Освещены особенности некоторых элементов криминалистической характеристики киберпреступлений. Проанализированы и уточнены определенные термины и понятия в сфере киберпреступности.

Ключевые слова: киберпреступность; криминалистическая характеристика киберпреступлений; хакеры; способы совершения киберпреступлений.

The peculiarities of some elements of criminalistic characteristics of cybercrime are illustrated. Certain terms and concepts of cybercrime are analyzed and clarified.

Keywords: cybercrime; criminalistic characteristics of cybercrimes; hackers; methods of feasance of cybercrimes.

Проблема комп’ютерної злочинності набуває дедалі більшої актуальності як у всьому світі, так і в нашій державі. Дослідженню питань протидії цьому виду злочинів присвятили свої роботи закордонні та вітчизняні науковці, зокрема: Ю. М. Батурин, В. М. Бутузов, В. Б. Вєхов, В. Д. Гавловський, В. О. Голубєв, М. В. Гуцалюк, Р. А. Калюжний, М. В. Карчевський, В. Є. Козлов, Е. В. Рижков, Б. В. Романюк, І. Р. Шинкаренко, В. П. Шеломенцев, Н. Г. Шурухнов та ін. [1–7].

Метою цієї статті є вивчення певних елементів криміналістичної характеристики кіберзлочинів, які в роботах зазначених авторів розглянуто лише фрагментарно.

Найважливішим елементом криміналістичної характеристики злочину є спосіб його вчинення, який складається з комплексу специфічних дій правопорушника з підготовки, вчинення злочину та його маскування. Ці дії являють собою певну систему, вони у зовнішній обстановці утворюють відповідні відображення, які в інформаційному плані є своєрідною моделлю злочину.

Стосовно кіберзлочинів найбільший інтерес становлять сліди, що вказують на те, як злочинець потрапив і зник з місця події, подолав перешкоди, використав своє службове становище, виконав поставлену злочинну мету, які знання та навички використав, чи спробував приховати сліди своїх дій. Важливі також сліди, що свідчать про характер зв’язку злочинця з предметом злочинного посягання тощо.

Спосіб учинення злочину в низці складів є необхідним елементом об’єктивної сторони злочину та входить до його кримінально-правової характеристики, а іноді служить навіть кваліфікуючою обставиною. Однак у кримінально-правовій характеристиці спосіб учинення злочину подано у загальному вигляді, для неї байдужі конкретні способи проникнення, засоби, що використовують при цьому, джерела їх отримання і т. д. Якщо ж ці обставини суттєві, застосовують криміналістичну характеристику способу вчинення злочину.

Елементи криміналістичної характеристики злочинів достатньо вивчені та описані, зокрема Є. І. Зуєвим [8, с. 120]. Однак кіберзлочини відрізняються від відомих криміналістичній науці злочинних посягань певною специфікою.

Так, Н. Г. Шурухнов поділяє способи неправомірного доступу до комп’ютерної інформації на такі три групи:

способи безпосереднього доступу;

способи віддаленого доступу;

комплексні способи [9, с. 103–110].

До першої групи належать способи, які в літературі іноді називають “за дурнем” (коли для проникнення у заборонену зону правопорушник, тримаючи в руках предмети – елементи маскування, разом з якоюсь особою

проникає до приміщення) та "прибирання сміття" (використання відходів інформаційного процесу – фізичних чи електронних, що залишені користувачем після роботи з комп'ютером)
[10, с. 28].

До другої групи способів належать:

підключення до телекомунікаційного обладнання, комп'ютерної системи чи мережі;

проникнення в комп'ютерні мережі шляхом автоматичного перебирання абонентських номерів із подальшим з'єднанням з тим або іншим комп'ютером;

проникнення у комп'ютерну систему з використанням чужих паролів ("непоспішний вибір");

безпосереднє та електромагнітне перехоплення інформації. Останній спосіб ґрунтується на тому, що робота електронних пристроїв (дисплеї, принтери) супроводжується побічними електромагнітними випромінюваннями (так, сигнали з електронно-променевої трубки дисплея можна приймати, записувати й аналізувати на відстані понад 1000 м).

Третю групу утворюють такі способи:

уведення в комп'ютерну програму команд, що дають змогу здійснювати незаплановані функції ("троянський кінь");

модифікація комп'ютерної програми ("містифікація");

доступ до баз даних і файлів шляхом знаходження слабких місць у системах захисту ("маскарад");

використання помилок і недоліків у комп'ютерній програмі
[10, с. 30–32].

Осіб, які вчиняють комп'ютерні злочини (кіберзлочини), у криміналістичній літературі поділяють на декілька категорій. Так, М. С. Полєвой та В. В. Крилов виокремлюють такі типи:

порушники правил користування ЕОМ (несанкціоноване використання комп'ютерів, поширення вірусів і т. п.);

"білокомірцеві" злочинці;

"комп'ютерні шпигуни" – підготовлені професіонали, метою яких є отримання важливих стратегічних даних про супротивника в економічній, політичній, технічній та інших сферах;

"хакери" ("одержимі програмісти") – технічно підготовлені особи, які, вчиняючи злочини, часто не переслідують при цьому прямих матеріальних вигод (для них має значення самоствердження, помста за образу, бажання пожартувати тощо) [11, с. 234, 239].

Загалом погоджуючись із такою класифікацією, вважаємо, що зазначені автори не повною мірою характеризують "хакерів". Адже це не просто "одержимі програмісти", а ще й "комп'ютерні хулігани".

Крім того, переважна більшість опитаних (слухачів-офіцерів, курсантів і студентів) на початку розмови про комп'ютерні злочини згадують, передусім, саме хакерів, що насправді не цілком відповідає дійсності. Так, унаслідок вивчення кримінальних справ в Україні науковці виявили, що лише у 10 % кримінальних справ, класифікованих як кіберзлочини, особу злочинця можна назвати фахівцем високого рівня – хакером. А у 90 % справ – це звичайний комп'ютерний користувач, який володіє специфічною інформацією у зв'язку з обійманням певної посади. Водночас у США в 80-х роках минулого століття з кожної тисячі комп'ютерних злочинів лише сім вчиняли хакери, проте нині, за даними Національного центру кримінальної інформації США, хакери вчиняють уже близько 20 % таких правопорушень. Тобто в Україні невдовзі можна також очікувати підвищення рівня кіберзлочинів, учинених підготовленими фахівцями – хакерами [12, с. 54–55].

В. Б. Вєхов виділяє такі три групи комп'ютерних злочинців:

особи, особливістю яких є стійке сполучення професіоналізму у сфері комп'ютерної техніки та програмування з елементами своєрідного фанатизму та винахідливості;

особи, які страждають на новий вид психічних захворювань – інформаційні хвороби (комп'ютерні фобії);

професійні комп'ютерні злочинці з яскраво вираженою корисливою метою [13, с. 38–39].

Ми цілком підтримуємо позицію В. Є. Козлова, який у цій класифікації уточнює назву другої групи правопорушників, пропонуючи іменувати їх особами, які страждають на новий різновид психічної неповноцінності – інформаційні хвороби чи комп'ютерні фобії [14, с. 162].

За наявності подібних фактів у процесі розслідування призначають судово-психіатричну експертизу на предмет установлення осудності злочинця на час учинення ним злочинних дій.

Потерпілими від кіберзлочинів найчастіше є юридичні особи. Це зумовлено тим, що процес комп'ютеризації широко охоплює, насамперед, юридичних осіб (організації, установи), а значно меншою мірою – фізичних осіб.

Виокремлюють три головні групи потерпілих від таких злочинів: власники комп'ютерної системи; клієнти, які користуються їх послугами; інші особи. Слід відзначити, що потерпіла сторона першої групи, як правило, неохоче звертається (якщо робить це взагалі) до правоохоронних органів за фактом учинення злочину, що, зокрема, є одним з головних факторів, який спричиняє високий рівень латентності такого виду злочинів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие : монографія / [И. Р. Шинкаренко и др.]. – Донецк : РВВ ЛДУВС, 2007. – 267 с.

2. Компьютерная преступность и кибертерроризм : сб. науч. ст. / под ред. В. А. Голубева, Э. В. Рыжкова. – Запорожье : Центр исслед. компьютерной преступности, 2005. – Вып. 3. – 448 с.

3. Вехов В. Б. Расследование компьютерных преступлений в странах СНГ : [монография] / В. Б. Вехов, В. А. Голубев ; под ред. Б. П. Смагоринского. – Волгоград : ВА МВД России, 2004. – 304 с.

4. Голубев В. А. Проблемы борьбы с преступлениями в сфере использования компьютерных технологий : [учеб. пособие] / Голубев В. А., Гавловский В. Д. , Цимбалюк В. С. ; под общ. ред. Р. А. Калюжного. – Запорожье : ЗИГМУ, 2002. – 292 с.

5. Крылов В. В. Информационные компьютерные преступления : [учеб. и практ. пособие] / Крылов В. В. – М. : ИНФРА-М, 1997. – 276 с.

6. Романюк Б. В. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологий : [наук.-практ. посіб.] / Б. В. Романюк, В. Д. Гавловський, М. В. Гуцалюк, В. М. Бутузов ; за заг. ред. Я. Ю. Кондратьєва. – К. : Вид. ПАЛИВОДА А. В., 2004. – 144 с.

7. Бутузов В. М. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : [наук.-практ. посіб.] / В. М. Бутузов, В. Д. Гавловський, К. В. Тітунина, В. П. Шеломенцев ; за ред. І. В. Бондаренка. – К. : Вид. дім "Аванпост-Прим", 2009. – 182 с.

8. Криминалистика : актуальные проблемы / под ред. Е. И. Зуева. – М., 1988.

9. Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. – М. : Щит-М, 1999. – 254 с.

10. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юрид. лит., 1991. – 160 с.

11. Полевой Н. С. Компьютерные технологии в юридической деятельности / Н. С. Полевой, В. В. Крылов. – М. : БЕК, 1994.

12. Бутузов В. М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук. практ. посіб. / [В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін.]. – К. : Вид. дім "Аванпост-Прим", 2010. – 245 с.

13. Вехов В. Б. Компьютерные преступления. Способы совершения, методики раследования / Вехов В. Б. – М. : Право и закон, 1996. – 182 с.

14. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью / Козлов В. Е. – М. : Горячая линия–Телеком, 2002. – 336 с.