Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 6, Is. 4, pp. 140-145, 2015

DOI: 10.13187/vesp.2015.6.140
www.ejournal21.com

UDC 004.056.53

Actual Problems of Computer Crimes in the Conditions of Perfection of Information and Telecommunication Technologies

[1] Xenia N. Zolotareva
[2] Ekaterina N. Zolotareva

[1] ITMO University, Russian Federation
197101, Saint-Petersburg, Kronverkskiy prospekt, 49
E-mail: ksenya2894@rambler.ru
[2] ITMO University, Russian Federation
197101, Saint-Petersburg, Kronverkskiy prospekt, 49
E-mail: katerina2794@rambler.ru

Abstract

This article discusses the concept of computer crime, set out current problems of computer crimes in the conditions of perfection of information and telecommunication technologies and ways of their solution. There are also described the main types and ways of implementing them. The types of punishment and criminal liability for computer crimes are presented.

Keywords: computer crimes, relevant problems, solutions, criminal responsibility, types of computer crimes.

Введение

Глобальное внедрение современных информационных технологий создает новые возможности для активного и эффективного развития экономики, политики, государства, общества. Но в тоже время, совершенствование технологий приводит к появлению новых источников угроз для пользователей информационных сетей и в первую очередь к увеличению количества компьютерных преступлений.

Часто сотрудники полиции, что выяснено, при проведении опроса следователей и дознавателей, сталкиваются с расследованием таких преступлений, предусмотренных УК РФ, как ст. 159.6 "Мошенничество в сфере компьютерной информации", ст. 273 "Создание, использование и распространение вредоносных компьютерных программ", ст. 272 "Неправомерный доступ к компьютерной информации", ст. 183 "Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну". Все эти преступления является компьютерными – это преступления в сфере высоких технологий, когда компьютеры или компьютерные сети выступают в качестве объекта преступных посягательств, а также средства или способа совершения преступлений.

Обсуждение

Одной из проблем, с которыми в этом случае приходится сталкиваться сотрудникам полиции, это недостаточный объем имеющихся знания для расследования киберпреступлений. Отсутствием достаточной практики и механизмов раскрытия и расследования компьютерных преступлений. То есть недостаточная компетентность лиц, которые занимаются их выявлением и раскрытием [1]. Для решения данной проблемы, как правило, необходимо проведение их дополнительного обучения по расследованию данного вида преступлений, а также организация семинаров, посвященных модификации компьютерных технологий.

Также сказывается несовершенство уголовного и уголовно-процессуального законодательства в этой сфере, Уголовный кодекс РФ не содержит указания, что именно следует понимать под "киберпреступлениями". Это приводит к проблемам квалификации преступлений в сфере информационных технологий и сложности организации и проведения компьютерных экспертиз. При назначении компьютерно-технической экспертизы следователям приходится сталкиваться с загруженностью государственных судебно-экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз. И не всегда у экспертных учреждений есть необходимое оборудование и средства для проведения судебной компьютерно-технической экспертизы, что является еще одной проблемой [2].

В настоящее время существует много видов компьютерных преступлений, каждый из которых характеризуется определенным способом реализации и несет разный ущерб. К ним можно отнести:

- Несанкционированный доступ к информации, хранящейся в компьютере. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных. Несанкционированный доступ может осуществляться и в результате системной поломки [3];
- Ввод в программное обеспечение "логических бомб", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему;
- Разработка и распространение компьютерных вирусов;
- Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям. Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т. п.;
- Подделка компьютерной информации. Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию. К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов и т.п.
- Хищение компьютерной информации. Если "обычные" хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

Помимо данного представления видов компьютерных представлений существуют коды, характеризующие компьютерные преступления [4]. Каждый код имеет идентификатор, начинающийся с буквы **Q**. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

- **QA - Несанкционированный доступ и перехват**
- **QAH** - компьютерный абордаж
- **QAI** - перехват
- **QAT** - кража времени
- **QAZ** - прочие виды несанкционированного доступа и перехвата
- **QD - Изменение компьютерных данных**
- **QUL** - логическая бомба
- **QDT** - троянский конь
- **QDV** - компьютерный вирус
- **QDW** - компьютерный червь
- **QDZ** - прочие виды изменения данных
- **QF - Компьютерное мошенничество**
- **QFC** - мошенничество с банкоматами
- **QFF** - компьютерная подделка
- **QFG** - мошенничество с игровыми автоматами
- **QFM** - манипуляции с программами ввода-вывода
- **QFP** - мошенничества с платежными средствами
- **QFT** - телефонное мошенничество
- **QFZ** - прочие компьютерные мошенничества
- **QR - Незаконное копирование**
- **QRG** - компьютерные игры
- **QRS** - прочее программное обеспечение
- **QRT** - топография полупроводниковых изделий
- **QRZ** - прочее незаконное копирование
- **QS - Компьютерный саботаж**
- **QSH** - с аппаратным обеспечением
- **QSS** - с программным обеспечением
- **QSZ** - прочие виды саботажа
- **QZ - Прочие компьютерные преступления**
- **QZB** - с использованием компьютерных досок объявлений
- **QZE** - хищение информации, составляющей коммерческую тайну
- **QZS** - передача информации конфиденциального характера
- **QZZ** - прочие компьютерные преступления

Итак, существует огромное количество видов киберпреступлений. А сама компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. Согласно экспертным оценкам, она способна нанести ущерб, сопоставимый с объемом хищений произведений искусства во всем мире.

Результаты

Безусловно, специфика совершения компьютерных преступлений связана с фактическим отсутствием межгосударственных границ. Но в УК РФ должен быть предусматривать наказания за киберпреступления.

Так, как интернет в настоящее время проникает во все сферы жизнедеятельности общества, то ответственность за правонарушение должна быть предусмотрена в каждой из этих сфер, т.е. конституционная, уголовная, административная, дисциплинарная и гражданско-правовая, а в некоторых случаях и материальная. Но выделяют три основных вида наказаний или ответственности:

– Уголовной;

– Административной;

– гражданской.

Наиболее распространенной по юридической нагрузке является уголовная ответственность.

УК. Глава 28 «Преступления в сфере компьютерной информации» содержит три статьи [5]:

1. «Неправо-мерный доступ к компьютерной информации» (ст. 272):

«1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет» [6].

2. «Создание, использование и распространение вредоносных компьютерных программ» (ст. 273):

«1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет».

3. «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (ст. 274):

«1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок до четырех лет».

Сейчас привлечение киберпреступников к ответственности является сложным процессом, но мировая статистика борьбы с киберпреступностью заметно улучшается [7].

Заключение

Таким образом, можно сказать, что проблемы в данной области обусловлены отчасти отсутствием системных обобщений материалов следственной и судебной практики, нехваткой методических рекомендаций по организации расследования данного вида преступлений, небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов, а также недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях. Для решения данных проблем уже существует решение: необходимо повысить уровень мониторинга данного вида преступлений; разработать программы повышения квалификации сотрудников полиции по расследованию данной категории дел; повысить технические возможности экспертов, специализирующихся в области исследования компьютерных технологий; увеличить объем научно-методической литературы, посвященной прикладным аспектам расследования

компьютерных преступлений и кроме того в высших учебных заведениях появилось специальное направление – 10.03.01 «Информационная безопасность».

Иными словами, для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания. Соответственно, возникает необходимость выработки единого понятия киберпространства с точки зрения криминалистики.

Примечание:

1. Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. 272 с.

2. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология интернет-пространства – 2011. [Электронный ресурс]. URL: http://cyberleninka.ru/article/n/kiberprestu

pnost-kak-novaya-kriminalnaya-ugroza (Дата обращения: 10.11.2015)

3. Патлах В.В. Классификация компьютерных преступлений. // «Энциклопедия технологий и методик». 2010. [Электронный ресурс]. URL: http://patlah.ru/biznes/biz-01/int-profi/int-profi-18.htm (Дата обращения: 05.11.2015)

4. Батурин Ю.М., Жодзинский А.М. Компьютерная преступность и компьютерная безопасность. М.: Юрид. лит., 1991.

5. Корнева Л.А. Уголовная ответственность за нарушение имущественных авторских и смежных прав в интернете // Российский следователь. 2008. №6.

6. Уголовный кодекс Российской Федерации. Глава 28. Преступления в сфере компьютерной информации. 13.06.1996 N 63-ФЗ (ред. от 29.06.2015) // Собрание законодательства РФ. 1996.

7. Бондарь В.В. Киберпреступность – современное состояние и пути борьбы. // Юридические записки. №2. 2013. [Электронный ресурс]. URL: http://cyberleninka.ru/ article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby

References:

1. Yuri Baturin Problems of computer law. M .: jurid. Lighted., 1991. 272 s.

2. V.A. Nomokonov, T.L. Tropin. Cyber crime as a new criminal threat // Criminology Internet space - 2011 [electronic resource]. URL: http://cyberleninka.ru/article/n/kiberprestu

pnost-kak-novaya-kriminalnaya-ugroza (Date of treatment: 10/11/2015)

3. V.V. Patlakh. Classification of computer crimes. // "Encyclopedia of technologies and techniques" - 2010 [electronic resource]. URL: http://patlah.ru/biznes/biz-01/int-profi/int-profi-18.htm (Date of treatment: 05/11/2015)

4. The Y.M. Baturin, Zhodzinsky A.M. Computer crime and computer security. M .: jurid. lit., 1991.

5. L.A. Kornev. Criminal liability for infringement of proprietary copyright and related rights on the Internet. // Russian investigators. 2008. №6.

6. The Criminal Code of the Russian Federation. Chapter 28. Crimes in the sphere of computer information. 13.06.1996 N 63-FZ (ed. by 06.29.2015) // Meeting of the legislation of the Russian Federation. 1996.

7. V.V. Cooper. Cybercrime - the current state and ways of fighting. // Legal notes №2 – 2013. [Electronic resource]. URL: http://cyberleninka.ru/article/n/kiberprestupnost-sovremennoe-sostoyanie-i-puti-borby

УДК 004.056.53

Актуальные проблемы компьютерных преступлений в условиях совершенствования информационно-телекоммуникационных технологий

[1] Ксения Николаевна Золотарева
[2] Екатерина Николаевна Золотарева

[1] Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
E-mail: ksenya2894@rambler.ru
[2] Университет ИТМО, Российская Федерация
197101, Санкт-Петербург, Кронверский проспект, 49
E-mail: katerina2794@rambler.ru

Аннотация. В данной статье рассматривается понятие компьютерных преступлений, изложены актуальные проблемы компьютерных преступлений в условиях совершенствования информационно-телекоммуникационных технологий и предложены пути их решения. Также описаны основные виды и способы реализации их. Рассмотрены виды наказаний и уголовной ответственности за компьютерные преступления.

Ключевые слова: компьютерные преступления, актуальные проблемы, решения, уголовная ответственность, виды компьютерных преступлений.