УДК 343.98:340.6
ББК 67.52+67.711-91
П 78

Печатается по решению
редакционно-издательского совета
НИУ «БелГУ»

П 78 **Проблемы законодательного регулирования Интернет-ресурсов и правового разрешения конфликтов с участием субъектов Интернет-сообщества :** материалы междунар. науч.-практ. конф. в рамках проекта «Российско-украинские криминалистические чтения на Слобожанщине», г. Белгород, 19 апр. 2013 г.: / отв. ред. И.М. Комаров. – Белгород : ИД «Белгород» НИУ «БелГУ», 2013. – 276 с.

ISBN 978-5-9571-0683-8

В сборнике представлены материалы конференции «Проблемы законодательного регулирования Интернет-ресурсов и правового разрешения конфликтов с участием субъектов Интернет-сообщества», посвященной 20-летию Юридического института НИУ «БелГУ», которая состоялась 19 апреля 2013 года в Белгородском государственном национальном исследовательском университете.

Для студентов, аспирантов, преподавателей вузов, научных работников и практикующих юристов, а также читателей, проявляющих интерес к криминалистике и судебной экспертизе.

УДК 343.98:340.6
ББК 67.52+67.711-91

ISBN 978-5-9571-0683-8

СОДЕРЖАНИЕ

Авдеева Г.К.

ИННОВАЦИОННЫЕ ПРИЕМЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Проанализированы следы преступлений в сфере использования информационных технологий, а также инновационные средства и методы борьбы с ними.

Ключевые слова: инновационный прием, информационная технология, компьютерная преступность.

Abstract. Analyzed traces of crimes in the sphere of information technologies, as well as innovative means and methods of struggle with them.

Key Words: innovative technique, information technology, computer crime.

Развитие современных информационных технологий[1] и телекоммуникационных систем, компьютеризация общества в целом приводят к появлению новых средств и методов преступной деятельности. Это, в свою очередь, требует использования инновационных приемов для своевременного выявления, квалифицированного расследования и профилактики преступлений в сфере использования информационных технологий.

Инновационными являются не любые нововведения, а лишь такие средства и методы, которые существенно повышают эффективность определенной деятельности.

Преступления в сфере использования электронно-вычислительных машин, систем и компьютерных сетей (раздел 16 – ст. ст. 361-363 УК Украины) подразделяются на такие виды:

– несанкционированный доступ в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей;

– создание с целью использования, распространения или сбыта вредоносных программных продуктов или технических средств, а также их распространение или сбыт;

– несанкционированные сбыт или распространение информации с ограниченным доступом, которая хранится в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации;

– преступления, совершенные путем использования компьютерной системы, как средства достижения преступной цели и другие.

1 В Законе Украины «О Национальной программе информатизации» указано, что «информационной технологией (IT) является целенаправленная организованная совокупность информационных процессов с использованием средств вычислительной техники, обеспечивающих высокую скорость обработки данных, быстрый поиск информации, доступ к информации независимо от места ее расположения». – См.: Про Національну програму інформатизації. Закон України // ВВР, 1998, N 27-28, ст.181 с изменениями, внесенными в соответствии с Законом N 2684-III от 13.09.2001, ВВР, 2002, N 1, ст.3.

Одним из средств совершения преступления в сфере использования компьютерных технологий являются вредоносные программные продукты.

Сегодня в сети Интернет размещены предложения хакеров по осуществлению DDoS-атак[1] за деньги. 12 января 2013 в Киеве задержан хакер, который совершал такие атаки на сайты украинских и зарубежных коммерческих структур по заказу конкурентов. В целях конспирации хакер общался с заказчиками через анонимные интернет-пейджеры, а средства получал с помощью виртуальных платежных систем, зарегистрированных на подставных лиц.

Термин «преступления, совершаемые с использованием компьютерных технологий» охватывают все действия, предполагающие использование достижений этих технологий и те, которые посягают на компьютерную информацию.

В криминалистическом аспекте такое определение позволило разработать инновационные типовые приемы, средства и методы обнаружения, фиксации и исследования компьютерной информации.

Одним из важнейших определяющих факторов в борьбе с данными преступлениями является область их совершения – киберпространство. Киберпространством называют сферу существования компьютерной информации, которая образована совокупностью средств компьютерной техники[2].

Компьютерная информация[3] в зависимости от характера преступных деяний выступает как предмет посягательства и как область возможного сохранения следов преступной деятельности.

Компьютерная информация имеет ряд специфических свойств:

– отсутствие неразрывной связи с материальным носителем;

– динамичность, возможность мгновенного переноса в пространстве (в том числе из одной части земного шара в другую);

– возможность изменения и уничтожения информации любого объема за короткие промежутки времени (в т.ч. – при помощи удаленного доступа)[4].

Кроме того, все копии компьютерной информации (не зависимо от вида носителя) идентичны оригиналу.

Компьютерная информация является новым объектом криминалистического исследования, а компьютерная техника – как технико-

[1] DoS-атака (атака типа «отказ в обслуживании», от англ. Denial of Service) – атака при помощи вредоносного программного обеспечения на компьютерную систему с целью ее блокировки, создание таких условий, при которых легальные (правомерные) пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам). Атаку, осуществляемую одновременно с большого числа компьютеров, называют DDoS-атакой. – См.: Дремлюга Р.И. Интернет-преступность: моногр. / Р.И. Дремлюга. – Владивосток: Изд-во Дальневост. ун-та, 2008. – С. 23.

[2] См: Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В.А. Мещеряков. – Воронеж: Издательство Воронежского государственного университета, 2002. – С. 41.

[3] Компьютерной информацией является информация в электронном (цифровом) виде, которая может быть зафиксирована на определенном носителе, в электронно-вычислительной машине (ЭВМ), в телекоммуникационной системе или сети ЭВМ.

[4] Криминалистика: Учебник / Под ред. Т.А. Седовой, А.А. Эксархопуло. – СПб.: Издательство «Лань», 2001. – С. 370.

криминалистический средство для работы с компьютерной информацией, придает этой информации значение источника доказательства.

В частности, сегодня разработано и используется значительное количество эффективных средств восстановления уничтоженной электронной информации.

В зависимости от ситуации и решаемых задач к осмотру средств компьютерной техники и поиску необходимой цифровой информации привлекают специалиста в области компьютерной техники, программных продуктов, телекоммуникационных сетей и средств.

При осмотре и исследовании операционной системы компьютера можно получить данные об информации, хранящейся в памяти компьютера. Например, можно установить последовательность действий, выполнявшихся ранее пользователем, а также информацию о преступнике и его определенной деятельности.

Следы совершения преступления в сфере компьютерной информации редко остаются в виде изменений внешней среды. Они носят информационный характер, т.е. представляют собой внесение изменений в компьютерную информацию.

Информационные следы образуются в результате воздействия на компьютерную информацию путем доступа к ней и представляют собой любые изменения компьютерной информации, связанные с событием преступления. Такими изменениями могут быть следы уничтожения, модификации, копирования, блокирования информационной системы. Следы изменений остаются на машинных носителях информации и отражают изменения в информации, которая в них хранится, (по сравнению с исходным состоянием). Часто преступниками осуществляются модификации баз данных, программ, текстовых файлов, находящихся на жестких дисках ЭВМ, дискетах, магнитных мини-дисках, флешкартах, оптических дисках, предназначенных для многократной перезаписи информации.

Кроме того, электронная информация может нести следы ее частичного уничтожения или модификации (удаление из каталогов имен файлов, удаления или добавления отдельных записей, физического разрушения или размагничивания носителей). Информационными следами являются также результаты работы антивирусных и тестовых программ. Данные следы могут быть обнаружены при экспертном исследовании компьютерного оборудования, рабочих записей программистов, протоколов работы антивирусных программ, программного обеспечения.

Наиболее часто встречаются такие информационные следы в сети Интернет, позволяющие установить лицо, совершившее неправомерный доступ к компьютерной информации:

Данные о фирме-провайдере, при помощи которого пользователь подключен к сети Интернет. В сети Интернет существует специальная служба Whois, предназначенная для установления наименования и адреса провайдера, через которого произошел неправомерный доступ. В общедоступном сервисе по адресу www.ripe.net необходимо указать электронный адрес (IP) атакующего

компьютера. Время работы абонента в сети можно установить у провайдера по специальному лог-файлу (журналу).

Протокол выхода в Интернет с определенного компьютера автоматически ведется на каждом компьютере, с которого возможен выход во всемирную сеть. Совпадение данных этого протокола с лог-файлом провайдера может служить неоспоримым доказательством несанкционированного доступа в определенную компьютерную систему.

Данные о пользователе электронной почты (фамилия, имя, отчество, дата и место рождения, место жительства, работы и проч.).

Данные о пользователе социальных сетей (фотоснимки, родственники, друзья, интересы, контакты и др.), устанавливаемые посредством поиска по электронному адресу, фамилии и др.

Большую информационную ценность имеют смс-сообщения, которые автоматически фиксируются и накапливаются на сервере мобильного оператора. Можно получить у оператора мобильной связи распечатку перечня телефонных звонков и текстов смс-сообщений.

В 2002 году изучение и анализ смс-сообщений позволили обезвредить организованную преступную группу, которая в Харькове, Киеве, Запорожье и др. городах Украины при помощи различных мошеннических действий и «театральных» представлений шантажировала состоятельных людей и в течение нескольких лет получала огромные суммы денежных средств.

Многие программы фирмы Microsoft создают резервные копии файлов, файлы-отчеты, хранят информацию о последних проведенных операциях и выполненных программах, а также содержат иную информацию, имеющую значение для расследования. В частности, почтовая программа Microsoft Outlook Express сохраняет в своей базе данных все письма, которые были отправлены, получены или удалены. Браузер Microsoft Internet Explorer сохраняет информацию о местах в сети Интернет, которые посетил пользователь.

Следами, указывающими на посторонний доступ к информации, могут быть такие: переименование каталогов и файлов, изменение размеров и содержимого файлов, изменение стандартных реквизитов файлов, даты и времени их создания; появление новых каталогов, файлов и другие следы.

Наиболее распространенный вид мошенничества в системах интернет-банкинга состоит из трех основных этапов: получение информации для осуществления неправомерного доступа в систему «Клиент-банк», проведение мошеннической операции и перевод денежных средств в наличные.

Для хищения персональных (авторизационных) данных пользователя системы ДБО – дистанционного банковского обслуживания – (логина, пароля и ключей подписи) злоумышленники используют специальное вредоносное программное обеспечение. Чаще всего это – модификации хорошо известных банковских троянов с дополнительными функциями[1].

[1] Комплексное расследование мошенничества в системах интернет-банкинга. [Электронный ресурс]. – Режим доступа: http://www.group-ib.ru/images/media/Group-IB_AntiFraud.pdf.

Новейшие методы и методики судебной экспертизы телекоммуникационных сетей и средств позволяют установить факт несанкционированного доступа к банковской системе, время такого доступа и IP-адрес компьютера, с которого он осуществлялся.

В компьютере преступника часто хранятся экземпляры скопированной с компьютера «жертвы» информации, а также так называемые «скриншоты» (графические изображения экраны монитора компьютера-»жертвы»). Там могут быть обнаружены присланные с компьютера-жертвы значения паролей и «логинов» для входа в определенную информационную сеть, копии украденной электронной корреспонденции и другая информация.

Сегодня для решения проблем борьбы с компьютерными преступлениями криминалистами исследуется технический характер их осуществления. Особое внимание уделено разработке новейших технических средств и приемов обнаружения, изъятия, фиксации и исследования следов преступлений с использованием компьютерных технологий.

Борьба с компьютерной преступностью не ограничивается установлением уголовной ответственности за конкретное совершенное преступление. Сегодня активно осуществляется построение международной системы борьбы с данными видами преступлений, объединяются необходимые кадры, разрабатываются методики, уточняются процедуры взаимодействия с международными структурами и правоохранительными органами других стран (в т.ч. – при помощи телекоммуникационных средств и систем).