Насонов Олег Геннадьевич

Магистрант НАЧОУ ВПО СГА

Направление: Юриспруденция

Магистерская программа: Уголовный процесс, криминалистика и судебная экспертиза, теория оперативно-розыскной деятельности

Проблемы расследования компьютерных преступлений

Аннотация. Предлагаются алгоритмы ритмов расследования различного вида компьютерных преступлений, указываются проблемы, требующие решения.

Ключевые слова: компьютерные преступления, компьютерный вирус, вредоносные программы.

Важнейшее место в Федеральной программе борьбы с компьютерными преступлениями, безусловно, должны занимать вопросы их расследования.

Практика показывает, что компьютерное преступление, как правило, очень трудно раскрывается, а иногда, даже будучи раскрытым, остается не вполне доказуемым. Это объясняется, главным образом, тем, что наши следователи не имеют достаточного опыта и методик расследования преступлений, совершаемых с использованием ЭВМ.

Такая методика в настоящее время разрабатывается в НИИ проблем укрепления законности и правопорядка Генеральной прокуратуры на основе анализа имеющегося в нашей стране небольшого опыта расследования компьютерных преступлений и изучения зарубежной практики только, к сожалению, по литературным источникам.

В процессе работы по данной теме мы встретились с множеством трудно решаемых проблем. И, прежде всего, это касается самого понятия компьютерного преступления, а отсюда его уголовно-правовой квалификации и криминалистической характеристики. Трудности встретились в рассмотрении

вопросов производства отдельных следственных действий (осмотра места происшествия, назначения судебных экспертиз, проведения следственного эксперимента и других). На некоторых из них и хотелось кратко остановиться.

Очень важным для следователей, которые будут специализироваться на расследовании преступлений в сфере компьютерной информации, является в Федеральном законе «Об информации, информатизации и защите информации» то, что непосредственно в нем даны основные понятия таких терминов, как: информация; информатизация; документированная информация (документ); информационные процессы; информационная система; информационные ресурсы; персональные данные (информация о гражданах); конфиденциальная информация; средства обеспечения автоматизированных информационных систем и их технологий; собственник и владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения; пользователь (потребитель) информации. Их определения узаконены и не могут толковаться иначе [1].

Правильно законодатель сделал и то, что раскрыл понятие компьютерной информации непосредственно в ст. 272 УК РФ, определив ее как информацию на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Таким образом, общим объектом для всех преступлений, указанных в главе 28 УК РФ, является компьютерная информация, а к непосредственным предметам преступного посягательства следует отнести базы или банки данных конкретных компьютерных систем или сетей, их отдельные файлы, а также определенные компьютерные технологии и программные средства их обеспечения, включая средства защиты компьютерной информации. Денежные средства и другие материальные ценности не могут быть непосредственными предметами преступного посягательства этих преступлений. Они являются предметами преступного посягательства иных преступлений.

Означает ли все сказанное, что мы вообще должны отказаться от термина «компьютерные преступления». Думается, он должен сохраниться, поскольку

уже вошел в профессиональный лексикон, который будет обозначать условное наименование не только преступлений, перечисленных в главе 28 УК РФ, но и тех, которые стали логическим продолжением других преступлений, предусмотренных Уголовным кодексом, виновные в совершении которых должны привлекаться к уголовной ответственности по совокупности статей УК РФ. Не было бы излишним изложить понятие компьютерного преступления непосредственно в УК, как это сделано в отношении многих других преступлений [4, с. 50].

В настоящее время наиболее полно разработана методика расследования неправомерного доступа к компьютерной информации. Алгоритм расследования этого преступления построен по следующей схеме:

1. Установление самого факта неправомерного доступа к информации в компьютерной системе или сети.

2. Установление места несанкционированного проникновения в компьютерную систему или сеть.

3. Установление времени несанкционированного доступа.

4. Установление надежности средств защиты компьютерной информации.

5. Установление способа несанкционированного доступа.

6. Установление лиц, совершивших неправомерный доступ к компьютерной информации.

7. Установление виновности и мотивов лиц, совершивших неправомерный доступ к компьютерной информации.

8. Установление вредных последствий неправомерного доступа к компьютерным системам или сетям.

9. Выявление обстоятельств, способствовавших неправомерному доступу к компьютерной информации [3, с. 77].

Конкретный факт неправомерного доступа к компьютерной информации, как правило, первыми обнаруживают сами пользователи компьютерной системы, но при этом они не всегда, по известным причинам, охотно идут на то, чтобы своевременно сообщить о случившемся правоохранительным

органам. Особенно это относится к руководителям кредитно-финансовых и банковских учреждений, которые не очень-то желают привлекать к себе внимание общественности и вызвать у клиентов сомнения в надежности этих учреждений. И больше всего они боятся того, что по этому факту начнется проведение, проверок, ревизий и экспертиз, которые могут раскрыть их финансовые и иные служебные тайны и вскрыть другие серьезные недостатки [2, с. 38].

Среди организационно-правовых мер в этом направлении мы видим необходимость принятия ведомственных нормативных актов, регулирующих порядок оформления и направления в правоохранительные органы материалов по фактам уголовно-наказуемых нарушений в сфере компьютерной информации, подобно тому, как в свое время поступили природоохранные органы в отношении фактов нарушения экологического законодательства.

Особые трудности для следователей будет представлять установление способа неправомерного доступа к компьютерной информации. Конечно, он может быть установлен путем допросов свидетелей из числа лиц, обслуживающих данную систему, или ее разработчиков, в результате производства следственного эксперимента с целью проверки возможности преодоления средств и методов защиты компьютерной системы одним из вероятных способов, а также путем производства судебных экспертиз, о которых следует сказать особо.

Назначение судебных экспертиз по делам о преступлениях в сфере компьютерной информации необходимо для исследования как технологии процессов сбора, обработки, накопления, хранения, поиска и распространения информации в условиях функционирования автоматизированных информационных систем и сетей, так и самой электронно-вычислительной техники, технических средств связи и их комплектующих, выступающих в качестве вещественных доказательств. Поэтому к основным мы относим два новых вида судебных экспертиз: информационно-технологическая и

информационно-техническая (никогда ранее не рассматриваемые в юридической литературе) [5, с. 212].

Информационно-технологическая экспертиза должна назначаться в тех случаях, когда для возникающих в ходе расследования вопросов требуются специальные познания в технологии информационных процессов, связанной с использованием средств вычислительной техники и связи. К объектам ее исследования можно отнести: проектную документацию на АИС или сеть; программы для ЭВМ; инструкции и методики по эксплуатации АИС; схемы формирования информационных массивов, базы и банки данных и их описания; первичные документы для ввода в ЭВМ и т. д.

Информационно-техническая экспертиза назначается тогда, когда возникает необходимость в ходе следствия в специальных исследованиях непосредственно технической части отдельных узлов, блоков, периферийных устройств, оборудования, составляющих компьютерные системы или сети, которые тоже могут стать вещественными доказательствами. Ее объекты исследования можно разделить на две группы: непосредственно технические средства обработки информации и непосредственно машинные носители информации.

Указанные виды судебных экспертиз пока не проводятся в специализированных экспертных учреждениях, поэтому уже сейчас необходимо определить, кому можно поручать их производство. Нам думается, что в решении этой проблемы должны принять непосредственное участие Гостехкомиссия, Роскоминформ, ФАПСИ, РосАПО, Роскомсоюз, АО «Диалог-Наука» и другие учреждения и организации, тесно связанные с разработкой, внедрением и использованием компьютерных систем и сетей. Видимо, следует говорить о создании специализированных экспертных учреждений в этом направлении.

Завершающим этапом расследования, как известно, является установление обстоятельств, способствовавших преступлению [6].

В настоящее время типичными из них, относящимися к неправомерному доступу к компьютерной информации, мы считаем следующие:

1. Нарушение технологического цикла проектирования, разработки, испытаний и сдачи в эксплуатацию АИС.

2. Совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения.

3. Неприменение в технологическом процессе всех имеющихся средств и процедур регистрации и протоколирования операций, действий программ и обслуживающего персонала.

4. Нарушение сроков изменения паролей и кодов пользователей.

5. Нарушение установленных сроков хранения копий программ и копий информации, а иногда и отсутствие их.

Все это в конечном счете сводится к недостаточной эффективности средств и методов защиты компьютерной информации от неправомерного доступа к ней.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» // Собрание законодательства РФ. 2006. № 31. Ч. 1. Ст. 3448

2. Айсанов Р.М. Неправомерный доступ к компьютерной информации. Уголовно-правовой анализ. М.: Юстицинформ, 2010.

3. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М., Юристъ, 2011.

4. Ефремова М.А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. № 7.

5. Нехорошев А.Б. Компьютерные преступления: квалификация, расследование, экспертиза: в 2 ч. / Под ред. В.Н. Черкасова. Ч. 2. Саратов: СЮИ МВД России, 2004.

6. Россинская Е.Р., Шамаев Г.П. Новый раздел криминалистики: криминалистическое исследование компьютерных средств и систем // Известия Иркутской государственной экономической академии. Т. 6. 2015. № 1.