УДК 343.3/.7:004 (575.2) (04)

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

И.В. Коваль

Проведен анализ компьютерных преступлений в криминалистическом аспекте. Автором выделяются и предлагаются критерии расследования компьютерных преступлений, описываются особенности расследования преступлений в сфере компьютерной информации.

Ключевые слова: компьютерные преступления; криминалистический аспект; компьютер; расследование.

С появлением современных средств вычислительной техники и телекоммуникаций традиционные преступления – кража, шпионаж, вымогательство – трансформировались в новые формы[1]. В связи с этим в научной литературе появился термин "компьютерные преступления", который подразумевает преступления в сфере компьютерной информации.

Многие ученые видят основную проблему раскрытия понятия, классификации и криминалистической характеристики компьютерных преступлений в сложности и неоднозначности объектов посягательства.

Некоторые исследователи полагают, что компьютерных преступлений как самостоятельной группы преступлений в юридическом смысле не существует и их следует рассматривать лишь как квалифицирующий признак обычных, "традиционных" преступлений. При этом персональный компьютер при совершении преступления выступает в качестве объекта преступления, орудия преступления, средства, на котором подготавливается преступление, или среды, в которой оно совершается. Например, Ю.М. Батурин считает, что "многие традиционные виды преступлений модифицировались из-за вовлечения в них вычислительной техники, и поэтому правильнее было бы говорить лишь о компьютерных аспектах преступлений, не выделяя их в обособленную группу"[2]. В то же время В.Б. Вехов и многие другие криминалисты считают, что под компьютерными преступлениями (с криминалистической точки зрения) следует понимать предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной техники[3].

Е.Р. Россинская полагает что «термин "компьютерное преступление" должен употребляться не в уголовно-правовом аспекте, где это только затрудняет квалификацию деяния, а в криминалистическом, поскольку связан не с квалификацией, а именно со способом совершения и сокрытия преступления и, соответственно, с методикой его раскрытия и расследования»[4]. В отношении "традиционных" преступлений компьютер является лишь средством, а использование компьютерных технологий – одним из способов совершения подобных преступлений, что не является причиной для отдельной квалификации компьютерных преступлений.

Так, В.А. Мещеряков предлагает «при квалификации компьютерных преступлений во главу угла ставить не компьютер, который выступает как орудие преступления (о чем справедливо замечает и Ю.М. Батурин), а информацию, представленную в специальном виде (пригодном для автоматизированного хранения, обработки, передачи и воспроизведения), а также последствия, которые наступили в результате неправомерного завладения ею, уничтожения или генерации со специальными

[1] *Козлов В.Е.* Теория и практика борьбы с компьютерной преступностью. М., 2002. С. 3.

[2] *Батурин Ю.М.* Проблемы компьютерного права. М., 1991. С. 129.

[3] *Вехов В.Б.* Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского. М., 1996. С. 24.

[4] *Россинская Е.Р.* Компьютерные преступления: уголовно-правовые и криминалистические аспекты // Воронежские криминалистические чтения. Вып. 3 / Под ред. О.Я. Баева. Воронеж, 2002. С. 176.

заданными свойствами. Ведь именно информация, представленная в особом (машинном) виде, является объектом преступления, а различную "окраску" преступление приобретает в зависимости от того, в какой сфере человеческой деятельности эта машинная информация использовалась»[1].

Из вышеизложенного следует, что к компьютерным преступлениям в криминалистическом смысле относятся преступления, сопряженные с применением самого компьютера и информационных технологий. Это преступления в сфере компьютерной технологии, так как их совершение невозможно без использования компьютерных средств, а также преступления, которые связаны с несанкционированным доступом к информации и с нарушением правил эксплуатации данного компьютерного средства. Следовательно, преступления можно считать компьютерными, так как и совершены и сокрыты они были с помощью персонального компьютера.

Расследование компьютерных преступлений имеет ряд особенностей, обусловленных спецификой компьютерных средств и технологий.

Существенным условием успешного расследования компьютерных преступлений является своевременный и качественно проведенный осмотр места происшествия. Данные, полученные в ходе осмотра, имеют значение для решения вопроса о возбуждении уголовного дела, уголовно-правовой квалификации деяния, выявления лиц, причастных к совершению преступления, и т.д.[2] При этом специальные познания, необходимые для проведения осмотра места происшествия по делам, связанным с применением компьютерных средств и технологий, являются весьма специфическими. Проведение в таких случаях осмотра лицами, не обладающими достаточными знаниями, влечет возможность не только упущения необходимой информации, но и ее безвозвратной утраты. Данное обстоятельство относится особенно к непосредственному осмотру средств компьютерной техники, так как даже выключение компьютера несет изменения в системной памяти и частных характеристиках файлов. Задачи следственного осмотра заключаются в собирании доказательств. На базе собранных доказательств следователь выдвигает версии о характере расследуемого компьютерного преступления и его участниках, месте нахождения предметов, имеющих доказательственное значение, последствия преступления и т.д. Кроме того, устанавливаются обстоятельства, способствовавшие совершению преступления[3].

Преодолевая средства защиты компьютерных систем, преступник оставляет следы на узлах и устройствах компьютера, периферийных и сетевых устройствах. Подвергшись преступному посягательству, файл данных или прикладного программного обеспечения становится носителем следовой информации. В качестве следообразующего объекта в процессе образования следов на узлах и устройствах компьютера, их сетей может выступать виртуальный объект – система команд компьютера. Для наиболее полного использования в качестве доказательств следов-предметов в виде регистрационных файлов целесообразен, на наш взгляд, переход субъектов хозяйствования на защищенные средства вычислительной техники, так как преодоление средств защиты компьютерным правонарушителем способствует образованию большего количества следов.

В силу специфики расследования дел о компьютерных преступлениях возникает необходимость проводить часть исследований по обнаружению, фиксации и изъятию следовой информации компьютерных систем непосредственно на месте происшествия. Это может быть обусловлено невозможностью изъятия компьютерных систем для проведения экспертизы в лабораторных условиях, из-за наличия у следователя оснований полагать, что имеющая доказательственное значение информация, содержащаяся в компьютерных системах, может быть утеряна или изменена при их отключении в процессе изъятия, или изъятие нанесет существенный ущерб выполнению производственных, финансовых и иных задач. При всех этих действиях производится поиск информации в компьютере, тактика которого должна исключать уничтожение или повреждение искомой информации, помочь следователю правильно разобраться в сложном информационном массиве, найти требуемое и зафиксировать изъятую информацию.

По мнению Х.А. Андриашина, перед началом осмотра или обыска необходимо в первую очередь принять меры к предотвращению возможного повреждения или уничтожения информации. Принять меры по контролю за бесперебойным электроснаб-

[1] *Мещеряков В.А.* Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж, 2001. С. 15.

[2] *Гаврилов М.В.* Осмотр при расследовании преступлений в сфере компьютерной информации / М.В. Гаврилов, А.Н. Иванов. М.: Юрлитинформ, 2007. С. 3.

[3] *Козлов В.Е.* Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия-Телеком, 2002. С. 179.

жением компьютера для предупреждения случайного выключения машины в момент осмотра. Удалить всех посторонних лиц с территории, на которой производится осмотр или обыск, и прекратить дальнейший доступ на нее. Исключить возможность контакта с компьютерами и их периферийными устройствами всех пользователей. Если на объекте находятся взрывчатые, легковоспламеняющиеся, едкие вещества, посторонние источники электромагнитного излучения и другие вещества и аппаратура, способные привести к аварии электронно-вычислительной техники – эвакуировать их. К участию в осмотре или обыске необходимо привлечь специалистов в области информатики и вычислительной техники. Кроме того, к участию в осмотре места происшествия или компьютера желательно привлечь специалиста-криминалиста, поскольку на аппаратных средствах зачастую оказываются следы рук, металлообрабатывающих инструментов, ручной пайки на внутренних элементах компьютерных средств[1]. Тактические особенности поиска компьютерной информации зависят от функционального состояния компьютерной системы и ее периферийных устройств на момент осмотра или обыска. Если компьютер на момент начала осмотра оказался включен, необходимо оценить информацию, изображенную на дисплее. Прежде всего, определить, какая программа исполняется на данный момент. В случае работы стандартного программного продукта не приступать к каким-либо манипуляциям на входе без предварительного визуального осмотра технических средств. Для исследования компьютеров, их комплектующих и содержащейся в них компьютерной информации назначается компьютерно-техническая экспертиза. Исследование фактов и обстоятельств, связанных с проявлением этих закономерностей, по заданию следственных и судебных органов в целях установления объективной истины по уголовному делу составляется предмет компьютерно-технической экспертизы.

Одним из основных элементов криминалистической характеристики, особенно важным при расследовании преступлений в сфере компьютерной информации, является способ совершения и сокрытия преступлений. К способам использования вычислительной техники для достижения преступной цели можно отнести:

1) подбор паролей, ключей и другой идентификационной информации;

2) подмена IP-адресов[2] – метод атаки, при котором злоумышленник подменяет IP-адреса пакетов, передаваемых по Интернету или другой глобальной сети, так, что они выглядит поступившими изнутри сети, где каждый узел доверяет адресной информации другого;

3) инициирование отказа в обслуживании и воздействии на сеть или отдельные ее части с целью нарушения порядка штатного функционирования;

4) анализ трафика, т.е. его прослушивание, расшифровка с целью сбора передаваемых паролей, ключей и другой идентификационной информации;

5) сканирование – метод атаки с использованием программ, последовательно перебирающих возможные точки входа в систему (например, номера TCP-портов[3] или телефонные номера) с целью установления путей и возможностей проникновения;

6) подмена, навязывание, уничтожение, переупорядочивание или изменение содержимого данных, передаваемых по сети, и другие типы атак и диверсий[4].

Широкое распространение и внедрение компьютеров во все сферы жизни общества привело и к тому, что изменился сам характер многих преступлений и их расследование. Процесс информатизации общества наряду с положительными последствиями имеет и ряд отрицательных сторон. Так, например, объединение компьютеров в глобальные сети, с одной стороны, дало возможность большому количеству людей приобщиться к огромному массиву накопленной в мире информации, а с другой – породило проблемы с охраной интеллектуальной собственности, помещаемой в сеть и хранящейся в ней. Для достижения, прежде всего, корыстных целей преступники стали активно применять компьютеры и специальную технику, создавать системы конспирации и скрытой связи в рамках системного подхода при планирования своих действий. Очевидно, что рассматриваемые проблемы не могли не затронуть и сферу деятельности правоохранительных органов. Возникла необходимость в разработке подходов к исследованию новых видов преступлений, методов их расследования и профилактики.

---

[1] Информатика и математика для юристов: учеб. пособие для вузов / Под ред. проф. Х.А. Андриашина, проф. С.Я. Казанцева. М: ЮНИТИ-ДАНА, Закон и право, 2001. С. 478.

[2] Сетевой адрес узла в компьютерной сети.

[3] Идентифицируемый номером системный ресурс, выделяемый приложению, выполняемому на некотором сетевом хосте для связи с приложениями, выполняемыми на других сетевых хостах.

[4] Криминалистика: учебник / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. 3-е изд., перераб. и доп. М.: НОРМА, 2008. С. 905.