тов, явлений и процессов, в совокупности составляющих место и обстановку совершения компьютерных преступлений.

Список литературы

1. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. № 2. С. 114 - 116.
2. Агибалов А.Ю. Виртуальные следы в криминалистике и уголовном процессе: автореф. дис. канд. юрид. наук. - Воронеж, 2010. С. 21.
3. Бахин В.П., В.С. Биленчук, П.Д. Кузьмичев. Криминалистические приемы и средства разрешения следственных ситуаций - Киев: КВШ МВД СССР им. Ф.Э. Дзержинского, 1991. – С. 98.
4. Поляков В.В., Лапин С.А. Программное обеспечение, используемое для совершения компьютерных преступлений // Ломоносовские чтения на Алтае–2013: матер. Междунар. молодежной школы-семинара (Барнаул, 5-8 ноября 2013 г.). – Барнаул: Изд-во Алт. ун-та, 2013. – Ч. 2 . – С. 15-17.
5. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. – Омск: Омская академия МВД России, 2009. С. 243-246.
6. Уголовное дело № 13127428 // Архив суда г. Минусинска. 2005 г.
7. Гавло В.К., Поляков В.В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. 2006. №2. С. 44-48.

ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ УСТАНОВЛЕНИЮ И ДОКАЗЫВАНИЮ ПО ДЕЛАМ О КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЯХ

Л.Г. Суханова, АлтГУ, юридический факультет, магистратура, 2 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Расследование компьютерных преступлений представляет собой сравнительно новое веяние в уголовном судопроизводстве. Расследование и раскрытие преступлений в сфере компьютерной

информации сопряжены с решением важной и сложной задачи - изъятием компьютерной информации и рассмотрением ее с точки зрения доказательства по уголовному делу.

Применительно к процессу доказывания компьютерную информацию можно определить как фактические данные, которые существуют в электронном виде, сохраняются в форме, доступной восприятию ЭВМ или человека либо передаются по телекоммуникационным каналам и на основе которых в определенном законом порядке устанавливаются обстоятельства, имеющие значение для правильного разрешения дела [6].

Криминалистическая характеристика преступлений в сфере компьютерной информации и обстоятельства подлежащие установлению и доказыванию по названным преступлениям тесно взаимосвязаны и во многом совпадают по своему содержанию.

В криминалистическую характеристику преступлений в сфере компьютерной информации входят следующие основные данные: о способах совершения преступления и механизме противоправного деяния; средствах совершения противоправного деяния; обстановке и месте совершения преступления; следах преступления; предмете преступного посягательства; лицах, совершающих данные преступления [3].

При расследовании компьютерных преступлений правоохранительные органы обязаны установить обстоятельства, которые подлежат установлению и доказыванию. Можно выделить следующие такие обстоятельства:

1. имело ли место преступление (либо это правонарушение иного рода);
2. каков объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности);
3. каков предмет преступного посягательства;
4. каков способ совершения преступления;
5. место, время (период) и обстоятельства совершения преступления;
6. размер и вид ущерба, причиненного пострадавшему;
7. кто совершил преступление;

8. если преступление совершено группой лиц, то каковы состав группы и роль каждого соучастника;
9. какие обстоятельства способствовали совершению преступления [1].

Вышеуказанные обстоятельства являются основными и подлежат установлению и доказыванию по всем категориям компьютерных преступлений. Однако имеется определенная специфика обстоятельств, подлежащих обязательному установлению и доказыванию при расследовании компьютерных преступлений в зависимости от состава преступления, предусмотренного соответствующими статьями УК РФ.

Полагаем, что при расследовании неправомерного доступа к компьютерной информации подлежат установлению следующие обстоятельства:

- факт неправомерного доступа к компьютерной информации;
- место несанкционированного проникновения в компьютерную систему или сеть;
- время несанкционированного доступа;
- надежность средств защиты компьютерной информации;
- способ совершения несанкционированного доступа;
- лица, совершившие неправомерный доступ к компьютерной информации;
- виновность и мотивы лиц, совершивших неправомерный доступ к компьютерной информации;
- вредоносные последствия неправомерного доступа к компьютерным системам или сетям;
- обстоятельства, способствовавшие неправомерному доступу к компьютерной информации.

Факт неправомерного доступа к информации в компьютерной системе или сети обычно первыми обнаруживают потерпевшие. Однако они не всегда своевременно сообщают об этом правоохранительным органам. Особенно это относится к руководителям кредитно-финансовых учреждений, которые не желают вызывать у клиентов сомнения в надежности своей деловой репутации. Они также опасаются, что по этому факту начнется проведение проверок, ревизий и экспертиз, могущих раскрыть их финансовые и иные служебные тайны, вскрыть какие-то нарушения.

Установить факт неправомерного доступа к компьютерной информации можно и в процессе проведения проверочных мероприятий в стадии возбуждения уголовного дела либо в ходе проведения ревизий, судебных экспертиз, иных следственных действий по уголовным делам, находящимся в производстве следователей, а также при проведении оперативно-розыскных мероприятий [2].

Интерес представляет специфика обстоятельств, которые подлежат установлению и доказыванию по делам, связанным с созданием, использованием и распространением вредоносных компьютерных программ. Причем, создание (включая изменение существующей программы) вредоносной программы означает любую деятельность, направленную на написание вредоносной программы. Создание вредоносной программы - не только творческая деятельность ее автора, но и техническая помощь, оказанная ему другими лицами. Созданием вредоносной программы будет и написание вредоносной программы, лишенной свойства новизны. Создание программы является оконченным преступлением с момента получения объективной формы представления. Под использованием вредоносной программы необходимо понимать ее непосредственное использование для несанкционированного уничтожения, блокирования, модификации, копирования информации, нарушения работы ЭВМ, их системы или сети [7]. Распространение вредоносной программы означает как распространение ее с помощью средств связи, так и простую передачу ее другому лицу в любой форме (в том числе и в виде записи на бумаге).

Распространение машинных носителей вредоносной программы означает передачу носителя другому лицу, включая копирование или дозволение копирования программы на носитель другого лица.

Особенностью неправомерного доступа к компьютерной информации, а также создания, использования и распространения вредоносных программ для ЭВМ является то, что место непосредственного совершения противоправного деяния (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат противоправного деяния) могут не совпадать [4].

Проблемным вопросом является определение места происшествия, поскольку при совершении одного преступления их может быть несколько: рабочее место, место постоянного хранения или резервирования информации, место подготовки преступления и др. [5].

Чаще обнаруживается место непосредственного использования результатов неправомерного доступа к компьютерной информации, особенно связанного с хищением денежных средств. При обнаружении неправомерного доступа к информации в компьютерной системе или сети следует выявить все места, где расположены компьютеры, имеющие телекоммуникационную связь. Следует установить место хранения информации на машинных носителях, добытых в результате неправомерного доступа к компьютерной системе или сети [8]. При расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети необходимо обращать внимание на факт преступного нарушения таких правил. Следует не забывать, что под правилами эксплуатации компьютерной системы следует понимать как правила, которые могут быть установлены компетентным государственным органом, так и правила технической эксплуатации и правила работы с программами, установленные изготовителями ЭВМ и иного компьютерного оборудования, правила, установленные разработчиками программ, сетевыми администраторами, а также правила, установленные владельцем компьютерной системы или по его полномочию.

Необходимо прежде всего установить факт существования конкретных правил эксплуатации ЭВМ на данном объекте. Они могут касаться порядка создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю компьютерной информации, защите ее на любой стадии информационного процесса [3]. Результаты анализа компьютерной преступности позволяют прогнозировать усложнение борьбы с нею ввиду того, что способы совершения компьютерных преступлений с каждым годом усложняются и приобретают все более изощренный характер. Более того, совершенствуются навыки преступников, применяемая ими техника, системы связи и передачи информации. Это ведет к увеличению количества преступлений. Изучение вопроса о способе совершения преступ-

лений в сфере компьютерной информации, личности преступников, совершающих такие преступления, а также исследование других обстоятельств, подлежащих установлению и доказыванию, является чрезвычайно важным для достижения цели своевременного выявления, раскрытия и предупреждения компьютерных преступлений.

Список литературы

1. Вехов В.Б. Компьютерные преступления. Способы совершения методики расследования. - М., 1996. - 182 с.
2. Гавло В.К., Поляков В.В. Следовая картина и ее значение для расследования преступлений, связанных с неправомерным удаленным доступом к компьютерной информации // Российский юридический журнал. 2007. №5 (57). С. 146-152.
3. Гаврилин Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие. - М.: ЮИ МВД РФ, 2003. - 245 с.
4. Поляков В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. 2007. Т. 310. № 1. С. 212 – 216.
5. Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С.45-47.
6. Сарапулов А.А. Теоретико-прикладные проблемы доказательств о преступлениях в сфере компьютерной информации // Правовые вопросы связи. 2011. № 1. С. 8-10.
7. Уголовное право Российской Федерации. Особенная часть: Учебник под ред. Л.В. Иногамовой-Хегай, – М.: Инфра-М: Контракт, 2005. – 559 с.
8. Шурухнов Н.Г. Расследование неправомерного доступа к компьютерной информации: учеб. пособ. – М: Московский университет МВД России, 2004. – 351с.