https://rospravosudie.com/court-kutuzovskij-sudebnyj-uchastok-g-syktyvkara-s/act-204954783/ (дата обращение 05.04.2014).
9. Приговор Мирового судьи судебного участка № 79 Дзержинского района города Волгограда Паталашко Н.В., от «14» января 2011 года. [Электронный ресурс]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-79-dzerzhinskogo-rajona-g-volgograda-s/act-202749002/ (дата обращение 05.04.2014).

ЗНАЧЕНИЕ МЕСТА И ОБСТАНОВКИ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКЕ

А.И. Сабылина, АлтГУ, юридический факультет, 1 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Криминалистическая характеристика преступлений в сфере компьютерной информации требует изучения вопроса об обстановке совершения преступлений. Данный вопрос в литературе разработан недостаточно и нуждается в дальнейшем исследовании. Обобщенные знания обстановки преступления позволяют акцентировать внимание следствия на более эффективный поиск и установление обстоятельств, входящих в предмет доказывания [1].

В преступлениях в сфере компьютерной информации местом их совершения обычно является помещение, в котором расположена компьютерная техника с информацией, в отношении которой происходят неправомерные действия, а также места использования компьютерной техники преступником. Принципиальные особенности имеют преступления, связанные с неправомерным доступом к компьютерной информации, совершенные дистанционным образом. Особенностью их является то, что в результате использования информационных сетей (проводных и беспроводных технологий) в одном преступлении одновременно могут быть задействованы множество компьютеров. Соответственно, находиться эти компьютеры могут в пространственно удаленных друг от друга местах и даже в разных государствах [2]. Кроме того, для неправомерного удаленного доступа к компьютерной информации особенностью является то, что территорией места происшествия может быть значительное пространство, включающее

помимо места совершения преступления также места подготовки к нему и места сокрытия следов. Это накладывает отпечаток на тактические приемы и используемую технику проведения осмотра места происшествия, обыска и других следственных действий и оперативно-розыскных мероприятий. В частности, по привлечению дополнительных сотрудников правоохранительных органов, использованию специальных программно-аппаратных средств фиксации, изъятия и исследования компьютерной информации. С учетом этого правильное определение границ, например, для осмотра места происшествия, способствует более быстрому раскрытию преступления [3]. В целях эффективного расследования место происшествия по данным делам можно рассматривать как комплекс взаимосвязанных мест:

Наиболее криминалистически значимую информацию представляют следы, оставленные преступником в первой точке, то есть в месте нахождения и непосредственно в самой ЭВМ (портативные, домашние, рабочие и иные компьютеры, используемые при подготовке, совершении и сокрытии преступлений), с которой совершалось преступление. Помимо виртуальных здесь могут иметься традиционные следы, например, следы пальцев рук на клавиатуре, микрочастицы тканей и иные следы жизнедеятельности преступника, которые его персонифицируют.

Другая группа мест локализации следов компьютерных преступлений включает, используемые в преступлении серверы провайдеров, VPN- и прокси-серверы (компьютеры - посредники на которых почти всегда остаются следы неправомерного удаленного доступа к компьютерной информации или проявления сетевого вредоносного программного обеспечения), сетевые шлюзы и маршрутизаторы. Для этих мест характерно наличие таких следов, как лог-файлы, которые привязаны к конкретному IP-адресу. Они могут фиксировать сеансы сетевой связи и включают в себя сведения о логине и пароле, дате, времени и продолжительности соединения, сведения об ЭВМ нарушителя (программное обеспечение, его конфигурация, настройки брандмауэра и браузера), IP адрес компьютера, MAC-адрес сетевой карты, выделенный для определенного сеанса связи, информацию об отправленных и полученных во время соединения, пакетах (время отправки, приема, размер, тип, IP адрес получателя или отправителя и иное).

К местам происшествия нужно отнести также места нахождения ЭВМ, используемых для совершения преступления при наличии сетевого соединения с ними со стороны преступников. Это ЭВМ пользователей, не подозревающих о том, что в отношении них совершено компьютерное преступление, а их компьютеры используются для совершения преступлений. К подобному способу сокрытия своей личности прибегают наиболее опытные и высококвалифицированные преступники, чтобы запутать следствие. В данном случае компьютеры-посредники выбираются по принципу не обеспеченности должной защищенности. Следы на «промежуточных» ЭВМ могут быть оставлены в лог-файлах, ведущихся различным программным обеспечением, протоколах соединений (наиболее важными из них будут те, что отражают соединение с компьютером предполагаемого преступника), хранилищах определенных категорий файлов (похищенных с ЭВМ пользователей, списков паролей, баз данных, вредоносного программ и т.д.).

Большую роль играет ЭВМ потерпевшего по количеству и значимости электронно-цифровых следов-последствий преступления. Здесь содержатся следы в виде вредоносного программного обеспечения (программы-шпионы, собирающие информацию об ЭВМ жертвы, программы типа «троянский конь» (их управляемая часть), программы-крипторы и иные), следов его самоликвидации, изменений в системных реестрах и log-файлах, сведений об изменении, модификации, копировании, удалении файлов, появления новых файлов специфического содержания [4].

В отдельную группу нужно выделить банки, банкоматы, магазины, в которых осуществляются покупки или происходит обналичивание денежных средств, добытых преступным путем. Следует отметить, что следы этой группы мест имеют повышенное значение при высокотехнологичных способах совершения преступлений. Ретроспективная методика расследования, берущая свое начало с поиска следов с ЭВМ потерпевшего, может натолкнуться на обрывы звеньев следовой цепи действий преступника, например, применившего сокрытие следов преступления путем использования VPN, Tor, анонимных прокси-серверов. Обычно в такой ситуации следствие встает в тупик, так как нет возможности прояснить картину преступления дальше. Именно здесь играют

свою роль следы действий преступника или членов его группы при обналичивании денежных средств. У следствия появляется возможность выяснить главное – кто совершил преступление по оставленным в банке, банкомате, магазине традиционным следам, позволяющим персонифицировать личность.

Состояние обстановки является другим важным аспектом и достаточно сильно влияет на поведение участников преступлений в сфере компьютерной информации. Судебно-следственная практика показала, что для совершения преступлений в сфере компьютерной информации преступники в большинстве случаев тщательно к ним готовятся [6]. Они наводят справки и изучают режим работы на объекте, содержащем предмет преступного посягательства, собирают данные о находящихся там средствах и технологиях. Наибольший интерес вызывают характеристики имеющихся программно-аппаратных средств, прежде всего – используемых средств технической защиты информации. Подготовка нередко связана с изучением и приспособлением к выявленной обстановке. С этой целью в обстановку могут вноситься изменения, например, путем внедрения в операционную систему компьютера, принадлежащего жертве преступного посягательства, вредоносной программы для снижения защиты компьютера и открытии возможности осуществления неправомерного удаленного доступа к нему по информационной сети. Так, в результате несанкционированной установки специального программного обеспечения в компьютер одной из организаций г. Минусинска преступником была получена возможность неоднократного неправомерного доступа к ее информационным ресурсам [7]. Установка данной программы снизила уровень защищенности компьютера организации, сделав его уязвимым для массового неправомерного доступа. В данном случае, обстановка для совершения преступления была изменена на благоприятную. В противном случае, когда встречаются незапланированные барьеры, например, сбой в работе программного обеспечения, преступник может воздержаться от реализации задуманного или спонтанно изменить план действий. Важность учета благоприятной и неблагоприятной обстановки до совершения преступления настолько велика, что некоторыми авторами выделяется в качестве самостоятельного элемента криминалистической харак-

теристики и называется причинами и условиями, способствующими совершению преступления.

На первоначальную обстановку преступления влияет наличие и состояние средств защиты компьютерной информации. К названным выше факторам необходимо добавить состояние по соблюдению требований информационной безопасности, сложившаяся на объекте межличностная обстановка и т.д. Для обстановки, в которой возможно совершение рассматриваемого преступления, наиболее свойственно следующее: низкий технический уровень защиты компьютерной информации и слабый контроль за ней, атмосфера невнимательности к случаям нарушения требований информационной безопасности и т.п. Нужно отметить, что в провинциальных городах влияние этого фактора более выражено, что необходимо учитывать для повышения эффективности расследования и предупреждения рассматриваемых преступлений [8].

Даже опытные компьютерные преступники не всегда правильно оценивают обстановку совершения преступления. Выполнив масштабные технические и организационные мероприятия по его подготовке, они могут не придать значения неучтенным или новым факторам и обстоятельствам. Так, преодолев основные средства защиты предмета посягательства и получив доступ к искомой компьютерной информации, преступники не обращают внимание на наличие программ, не препятствующих их дальнейшей деятельности, но ведущих подробную фиксацию их действий. Нередко встречается такая ситуация преступления, когда преступники, неожиданного добившись или получив благоприятные условия для совершения преступления, например, в результате удачного стечения обстоятельств, могут изменить способ совершения преступления, слишком упростив или усложнив его. В результате такой «самодеятельности» преступники забывают, не успевают или пренебрегают сокрыть неспрогнозированные ранее следы преступления.

Таким образом, преступник в сфере компьютерной информации оставляет следы в различных местах, как виртуального мира, так и материального. Поэтому при расследовании преступлений в сфере компьютерной информации необходимо изучать систему различного рода взаимодействующих между собой объек-

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