Краснодарский университет МВД России

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Курс лекций

Краснодар
2019

УДК 343.98(075)
ББК 67.523.13
Р24

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Составитель *Н. В. Солонникова*

Рецензенты:
Е. С. Стешич, кандидат юридических наук, доцент (Ростовский юридический институт МВД России);
А. С. Герасименко (Главное упрвление МВД России по Краснодарскому краю).

Расследование преступлений, совершенных в сфере компьютерной информации : курс лекций / сост. Н. В. Солонникова. – Краснодар : Краснодарский университет МВД России, 2019. – 56 с.

Р24

ISBN 978-5-9266-1518-7

Рассматриваются основные положения дисциплины «Расследование преступлений, совершенных в сфере компьютерной информации». Показан алгоритм принятия решения о возбуждении уголовного дела, тактические приемы расследования компьютерных преступлений на первоначальном и последующем этапах.

Для профессорско-преподавательского состава, адъюнктов, курсантов и слушателей образовательных организаций МВД России.

УДК 343.98(075)
ББК 67.523.13

ISBN 978-5-9266-1518-7

Предисловие

Человечество с древности пыталось механизировать вычислительные операции, последовательно создав счеты (500 г. до н. э. – Япония, Китай и Индия), логарифмическую линейку (1622 г.), арифмометры (1630 г.), механический калькулятор (Г.В. Лейбниц, 1673 г.). Прообразом современного компьютера является аналитическая машина английского математика Чарлза Бэббиджа, конструкция которой была разработана в период с 1834 по 1851 г., но ее создание не было завершено из-за низкого технологического уровня того времени.

Жизнь современного человека тесно связана с глобальной сетью Интернет и современными информационными технологиями, развитие которых стимулирует как положительные, так и отрицательные стороны жизни общества. Среди последних – совершение преступлений в сфере компьютерной информации.

Количество преступлений в сфере компьютерной информации растет по мере развития технологий, телекоммуникационных сетей и увеличения числа персональных компьютеров. Такого рода преступления отличаются достаточно высокой латентностью, поскольку о совершенном преступлении правоохранительные органы уведомляются не всегда, особенно если потерпевшая сторона является юридическим лицом. Кроме того, доказательства по данной категории преступлений могут быть уничтожены в одно мгновение. Таким образом, их сложно выявлять, раскрывать и расследовать.

В последнее время наблюдается рост компьютерных преступлений, совершаемых в сфере экономики и денежного обращения, к которым относятся финансовые хищения, мошенничества, подлоги и т. д. Однако, как показывает практика, такие преступления следователи нередко квалифицируют только по статьям Уголовного кодекса РФ, предусматривающим ответственность за традиционное преступление, игнорируя совершение этих преступлений с использованием компьютерных технологий. Это приводит к искажению статистических данных о количестве совершаемых в России преступлений в сфере компьютерной информации.

С увеличением количества пользователей глобальной сети Интернет участились случаи совершения противоправных деяний не только на территории Российской Федерации, но и на территории других государств.

Существуют определенные факторы, которые затрудняют расследование компьютерных преступлений: специальный понятийный аппарат, обилие нормативных актов, определяющих правовой статус и специфические особенности компьютерной информации, отсутствие специализации при расследовании компьютерных преступлений, недостаточная оснащенность правоохранительных органов средствами компьютерной техники и др. Устранение этих факторов способствовало бы повышению качества расследования неправомерного доступа к компьютерной информации. Следовательно, сотрудники правоохранительных органов должны обладать соответствующими знаниями для борьбы с преступлениями, совершаемыми в сфере компьютерной информации.

Цель данного курса лекций – рассмотреть элементы криминалистической характеристики, особенности производства следственных действий на различных этапах расследования компьютерных преступлений.

Тема 1. Особенности расследования преступлений в сфере компьютерной информации на первоначальном этапе

План

1. Криминалистическая характеристика преступлений в сфере компьютерной информации.
2. Особенности возбуждения уголовного дела по преступлениям в сфере компьютерной информации.
3. Особенности тактики производства отдельных следственных действий по преступлениям в сфере компьютерной информации.

1. Криминалистическая характеристика преступлений в сфере компьютерной информации

Технологический процесс не стоит на месте, он развивается достаточно стремительно. Благодаря этому люди получили различные возможности, например, оперативно общаться с абонентом, находящимся в другой точке нашей планеты, произвести заказ того или иного продукта, найти информацию за считаные секунды. Однако, с другой стороны, развитие информационных технологий породило проблемы как для отдельных граждан, так и для целых стран.

Российские нормативные правовые акты содержат нормы уголовной и административной ответственности за несоблюдение требований информационной безопасности. Однако некоторые виды нарушений становятся массовыми и практически обыденными.

В настоящее время при расследовании преступлений в сфере компьютерной информации существуют такие проблемы, как отсутствие единой судебной и следственной практики; отсутствие высокопрофессиональных специалистов в системе МВД, методик расследования преступлений в сфере компьютерной информации; определенные сложности при проведении компьютерной экспертизы.

В гл. 28 УК РФ, предусматривающей ответственность за преступления в сфере компьютерной информации, содержится четыре состава: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

Изучая вопросы расследования преступлений в сфере компьютерной информации, необходимо уяснить сущность и свойства информации как правового понятия.

Информация (лат. informatio – разъяснение, изложение, осведомленность) – некоторые сведения, совокупность каких-либо данных, знаний и т. п.

Под информацией обычно понимаются сведения об окружающем мире и протекающих в нем процессах, воспринимаемые и передаваемые человеком или специальными устройствами.

Согласно Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» информация – это сведения (сообщения, данные), независимо от формы их представления.

В гл. 28 УК РФ «Преступления в сфере компьютерной информации» законодатель использует два термина со словом информация: «охраняемая законом компьютерная информация» и «компьютерная информация».

Согласно примечанию 1 к ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001) указано, что компьютерная информация – это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной для восприятия ЭВМ, или передающаяся по каналам связи.

Признаками компьютерной информации являются:

1) материальный носитель (диск, интегральная микросхема, электрические сигналы и т. д.);

2) форма, доступная для восприятия ЭВМ или передающаяся по каналам связи.

Специфичность такой информации заключается в следующем.

1. Отсутствие жесткой привязки к материальному носителю.

2. Изменяемость. Достаточно просто и быстро преобразовать компьютерную информацию из одной объектной формы в другую либо перенести на другой носитель – как бумажный, так и электронный.

3. Распространяемость.

4. При изъятии (переносе на другой электронный носитель, распечатке на бумажном носителе) компьютерной информации, в отличие от изъятия материального предмета (вещи), она сохраняется в первоисточнике, что затрудняет обнаружение факта ее хищения.

5. Трудность установления авторства.

Если еще пятнадцать лет назад считалось, что преступления в сфере компьютерной информации в России – явление относительно редкое, то в настоящее время доля такого рода преступных деяний, в том числе совершаемых посредством сети Интернет, существенно увеличилась.

Для уяснения специфики такого явления, как Интернет, рассмотрим вопросы адресации и административного устройства сети, виды ее ресурсов.

Ресурсами Интернета являются: электронная почта, сетевые новости, протокол передачи файлов (FTP-протокол), всемирная паутина (www), электронные платежные системы, интернет-радио, интернет-телевидение, IP-телефония, мессенджеры, файлообменные сети, IRC (веб-чаты), поисковые системы, интернет-реклама.

Адрес каждого компьютера в Интернете должен быть определен однозначно.

Для записи адресов используются два равноценных формата: IP (ай-пи) и DNS-адреса.

IP-адрес в Интернете (IP-номер) – уникальный код компьютера в сети Интернет (IP-номер), который состоит из четырех десятичных чисел со значениями от 0 до 255, разделенных

точками (xxx.xxx.xxx.xxx). Такая схема нумерации позволяет иметь в сети более четырех миллиардов компьютеров.

Для удобства компьютерам в Интернете кроме IP-адресов присваиваются также собственные имена. При этом, так же как и в случае с цифровыми адресами, такие имена обладают уникальностью.

В этих целях в 1984 г. была разработана система доменных имен (Domain Name System, DNS).

Доменное имя – обозначение символами, предназначенное для адресации сайтов в сети Интернет в целях обеспечения доступа к информации, размещенной в Интернете.

Первым в DNS-адресе стоит имя реального компьютера с IP-адресом. Далее последовательно идут адреса доменов, в которые входит компьютер, вплоть до домена страны (для них принята двухбуквенная кодировка).

Следует учесть, что преступления, предусмотренные гл. 28 УК РФ, могут совершаться в совокупности с иными преступлениями. Это связано тем, что компьютерная информация может стать предметом преступного посягательства. Компьютерная информация используется для совершения следующих общественно опасных деяний: подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; нарушение авторских и смежных прав; мошенничество и др.

Способы совершения компьютерных преступлений

Первая группа – это способы несанкционированного доступа, дающие возможность несанкционированных подключения, копирования, модификации, блокирования и уничтожения информации.

Указанная группа подразделяется на следующие виды.

1. Способы непосредственного доступа к компьютерной информации, при осуществлении которых информация уничтожается, блокируется, модифицируется, копируется путем введения определенных команд. Доступ может также осуществляться с помощью хищения носителей информации и технических отходов информационного процесса. Различают две формы – физическую и электронную.

Физическая форма представляет собой обследование рабочих столов сотрудников, емкостей с мусором с целью выявления оставленных носителей информации, исследования различной документации и иных бумаг.

Электронный вариант представляет собой просмотр и последующее изучение данных из памяти компьютера.

2. Способы удаленного доступа к компьютерной информации, которые представляют собой опосредованную связь с определенным компьютером (сетевым сервером), находящимся на расстоянии, и имеющейся на нем информацией. Такая связь может быть осуществлена через локальные или глобальные компьютерные сети, иные технические устройства.

Специалисты выделяют следующие способы удаленного доступа:

– применение подслушивающих устройств (закладок);

– мистификация (маскировка под запросы системы);

– считывание данных из массивов других пользователей;

– копирование носителей информации с преодолением мер защиты;

– маскировка под зарегистрированного пользователя («маскарад»);

– использование программных ловушек;

– незаконное подключение к аппаратуре и линиям связи;

– вывод из строя механизмов защиты.

Данный перечень является далеко не исчерпывающим.

Вторая группа – это способы перехвата информации. Перехват – получение разведывательной информации путем приема электромагнитного и акустического излучения пассивными средствами приема, расположенными, как правило, на безопасном расстоянии от источника информации.

Виды перехвата:

– непосредственный;

– электромагнитный;

– аудиоперехват, или снятие информации по виброакустическому каналу (установка подслушивающего устройства – «таблетки», «клопа», «жучка» и т. п. в различные технические устройства, на проводные коммуникационные линии, в различные конструкции инженерно-технических сооружений и бытовых приборов, а также на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать речевые сигналы);

– видеооптический перехват посредством использования различной видеооптической техники.

Третья группа – это злонамеренная вирусная модификация, которая включает следующее:

1) злонамеренную установку вирусных закладных устройств;

2) внедрение вирусных программ для уничтожения или модификации информации;

3) внедрение вирусных программ для уничтожения средств обработки и передачи информации.

Все вредоносные программы можно условно подразделить на следующие виды.

1. «Червь» – программа, которая проникает в компьютерные системы и выполняет какие-либо вполне определенные вредоносные функции или действия. Распространяется через компьютерные и мобильные сети.

2. «Логическая бомба» – программа, представляющая собой набор команд, который срабатывает при определенных условиях или в заранее определенное время («временная бомба»).

3. Троянская программа.

4. Классические компьютерные вирусы. Компьютерный вирус – это вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

5. Программы для получения несанкционированного доступа – это программы, с помощью которых можно удаленно управлять компьютером, осуществлять расшифровку информации, подбор паролей и т. д.

На практике большая часть преступлений в сфере компьютерной информации совершается смешанными способами.

Способы противодействия расследованию

Способ сокрытия следов преступления как один из этапов совершения преступления предоставляет дополнительную информацию о преступнике, обстоятельствах преступления. Сокрытие может осуществляться как «традиционными» способами (например: отказ от дачи показаний, воздействие на потерпевших, свидетелей, подозреваемых), так и специфическими, связанными с компьютерным оборудованием и информацией. К ним можно отнести маскировку местонахождения преступника с по-

мощью ремейлеров, применение устройств, изменяющих данные электронной почты отправителя и др.

Особенности следовой информации

В научной литературе принято выделять три группы следов, образующихся при совершении преступлений в сфере компьютерной информации.

1. Материальные следы, которые в свою очередь подразделяются на следы, рассматриваемые трасологией, следы-вещества (следы краски, тонеров, смазок) и следы-предметы (диски, ленты, кабели, документы на различных носителях и т. д.).

2. Информационные (виртуальные) следы, к которым относят:

– любые изменения компьютерной информации, которые образуются в результате воздействия на форму компьютерной информации, ее файловое представление, файловые атрибуты и реквизиты файлов, совершаемого путем доступа к ней, и которые связаны с событием преступления (находятся на ЭВМ, сетевых устройствах, машинных носителях владельца, собственника компьютерной информации);

– протоколы результатов работы антивирусных и тестовых программ;

– изменения в загрузочной и программной конфигурации компьютера, системном реестре;

– протоколируемые результаты доступа через компьютерные сети, например через Интернет.

При расследовании DoS-атаки следует принимать во внимание, что компетенция подозреваемого в совершении компьютерного преступления в области IT может быть достаточно высокой. Поиск необходимо направить на следы технического характера: инструменты атаки; следы поиска, тестирования, приобретения инструментария; логи – файлы операторов связи, через сети которых проходила атака; следы от контрольных обращений подозреваемого к атакуемому ресурсу в период атаки, чтобы убедиться в ее действенности, и т. п.

При расследовании преступления, предусмотренного ст. 273 УК РФ, можно обнаружить следующие следы: исходный текст или промежуточные варианты вредоносной программы; антивирусное программное обеспечение разных производителей, на котором

злоумышленник тестировал созданную им вредоносную программу; программные средства для управления вредоносными программами; следы контактов с заказчиками, распространителями или пользователями вредоносной программы, а также передачи им экземпляров и документации, оплаты. На компьютере пострадавшего необходимо искать следы вредоносной программы (исполняемый код вредоносной программы, лог антивируса либо следы деятельности вредоносной программы).

3. Интеллектуальные следы, к которым относятся показания потерпевших, свидетелей, подозреваемых или обвиняемых.

Обстановка преступлений в сфере компьютерной информации характеризуется рядом специфических факторов.

Во-первых, интерес представляет изучение сведений о месте совершения данных преступлений. При совершении преступления способом непосредственного доступа место совершения преступления и место постоянного нахождения ЭВМ совпадают. При удаленном доступе местонахождение преступника в момент преступления, местонахождение компьютерного оборудования, на которое осуществляется посягательство, и место наступления вредных последствий могут не совпадать. Чаще всего удаленный доступ осуществляется с компьютерного оборудования, находящегося у преступника дома. В ряде случаев – с ЭВМ, находящейся по месту работы виновного, а также в компьютерных центрах, клубах.

Во-вторых, для большинства вышеуказанных преступлений особенностью обстановки является несовпадение места совершения преступления и места наступления последствий от него, в связи с чем необходимо взаимодействовать с оперативными и следственными подразделениями, расположенными как на территории Российской Федерации, так и на территории других государств.

В-третьих, способ совершения преступления в сфере компьютерной информации зависит от таких факторов, как: особенности компьютеризации объекта и организации информационной безопасности; возможность нарушения целостности компьютерной информации без непосредственного участия человека; уровень квалификации специалистов, в обязанности которых входит защита информации.

В-четвертых, обстановка совершения преступления находится во взаимосвязи с личностью преступника, который выбирает способ совершения преступления с учетом возможной обстановки, а конкретизирует – с учетом реально сложившейся обстановки.

Местом совершения преступлений данной категории могут быть жилые и нежилые помещения, например квартиры, частные домовладения или кабинеты предприятий, учреждений, организаций.

Время совершения преступления зависит от места и способа его совершения. Например, при совершении преступных действий на рабочем месте время их совершения – это время работы предприятия, учреждения, организации. При совершении преступления с помощью компьютерных сетей отмечается их большее количество в вечернее и ночное время. Это связано, например, с льготными тарифами, меньшей загруженностью сети или нахождением преступника по месту жительства после работы.

Характеристика лиц, совершающих преступления в сфере компьютерной информации

Классификация лиц, совершающих преступления в сфере компьютерной информации, проводится по различным основаниям и весьма разнообразна.

Традиционно в отдельную группу выделяют хакеров – лиц, занимающихся поиском способов получения несанкционированного доступа к средствам вычислительной техники и охраняемой законом компьютерной информации. В зависимости от специализации хакеры подразделяются на следующие типы.

1. «Крэкеры» – лица осуществляющие модификацию, блокирование, уничтожение средств защиты компьютерной информации. Эти лица занимаются оборотом контрафактной продукции, промышленным и иным шпионажем, незаконным распространением охраняемой законом компьютерной информации, распространением порнографических материалов в сети Интернет.

2. «Фрикеры» – совершают преступления в области электросвязи с использованием конфиденциальной компьютерной информации и специальных технических средств, разработанных для негласного получения, модификации, блокирования информации с технических каналов электросвязи.

3. «Кардеры» осуществляют незаконную деятельность в сфере оборота пластиковых карт.

Классификация компьютерных преступников по уровню профессиональной подготовки и социальному положению:

а) «хакеры» – лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций;

б) «шпионы» – лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях;

в) «террористы» – лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политического воздействия;

г) «корыстные преступники» – лица, вторгающиеся в информационные системы для получения личных имущественных или неимущественных выгод;

д) «вандалы» – лица, взламывающие информационные системы для их разрушения.

Компьютерные преступления, как правило, совершают мужчины в возрасте от 15 до 45 лет, имеющие опыт работы в области информационных технологий или увлекающиеся ими как хобби. Возможна причастность психически нездоровых лиц.

Цели и мотивы совершения компьютерных преступлений:

– корысть;

– коммерческий шпионаж, диверсия;

– хулиганские побуждения;

– месть (например, за необоснованное увольнение с работы);

– иные цели и мотивы (например, использование глобальных сетей в террористических целях, совершение компьютерных атак по политическим мотивам).

Следует учитывать, что в настоящее время на смену подросткам, распространяющим вирусы ради забавы и самоутверждения, приходят профессиональные киберпреступники, которые предпочитают атаковать конкретные объекты для получения востребованной информации. Действия таких преступников наносят гораздо больший ущерб, чем проделки подростков, и сложнее расследуются. Однако, с другой стороны, совершение преступления технически сложным способом (например, несанкциониро-

ванный доступ в тщательно закрытую систему, подделка информации, установка «логической бомбы» в программе) является фактором, упрощающим расследование, так как круг специалистов, которые имеют достаточную квалификацию и возможности для такой акции, весьма ограничен.

Характеристика потерпевших от преступлений в сфере компьютерной информации

Сведения о потерпевшей стороне могут способствовать получению информации о личности преступника, мотивах совершения преступления и, как следствие, определить круг подозреваемых лиц, поскольку нередко между преступником и жертвой существует взаимосвязь.

Компьютерные посягательства представляют серьезную угрозу для любого располагающего компьютерной техникой физического или юридического лица.

Потерпевшей стороной компьютерных преступлений являются юридические или физические лица.

1. Юридические лица – различного рода учреждения, предприятия и организации:

– компании, обслуживающие работу телефонной, в том числе сотовой связи;

– кредитно-банковские организации;

– фирмы, обслуживающие любые пользовательские службы в Интернете;

– другие лица.

2. Физические лица:

– пользователи услуг систем сотовой связи, интернет-связи и т. д.;

– обладатели авторских прав (ими могут быть и юридические лица);

– другие лица.

Потерпевшие первой группы неохотно сообщают или не сообщают вовсе в правоохранительные органы о фактах компьютерных посягательств. А отказ потерпевших от уголовного преследования позволяет преступникам уходить от уголовной ответственности и создает предпосылки для увеличения числа компьютерных преступлений.

Обстоятельства, подлежащие установлению при расследовании преступлений в сфере компьютерной информации

Обстоятельства, подлежащие установлению по любому уголовному делу, в том числе о преступлениях в сфере компьютерной информации, указаны в ст. 73 УПК РФ. Рассмотрим только особенности, касающиеся расследования преступлений, предусмотренных гл. 28 УК РФ.

Итак, подлежат установлению следующие обстоятельства.

I. Событие совершения преступления (время, место, способ и другие обстоятельства совершения преступления).

1. Необходимо установить факт совершения преступления: неправомерного доступа к компьютерной информации; создания, использования и распространения вредоносных программ; нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Установление факта совершения преступления часто вызывает сложности. Это связано с тем, что незаконное копирование информации часто остается необнаруженным, появление в компьютере вируса обычно списывается на непреднамеренную ошибку пользователя, заполучившего вирус при пользовании Интернетом или при подключении к компьютеру съемных носителей информации. Расследуя преступление в сфере компьютерной информации, необходимо определить, не является ли событие следствием факторов, не имеющих ничего общего с преступным умыслом (климатических условий, природных и техногенных катастроф, технических неполадок).

Факт неправомерного доступа к информации в компьютерной системе или сети обычно первыми обнаруживают сами же пользователи информационной системы. В ряде случаев потерпевшие не сообщают в правоохранительные органы о факте незаконного вмешательства в компьютерную систему, опасаясь подрыва деловой репутации, потери клиентов, распространения сведений их личной жизни или из-за боязни выявления своих преступных действий.

Факты неправомерного доступа могут быть выявлены в ходе проверок, при проведении ревизий или следственных действий по другим уголовным делам.

Вредоносная программа может быть обнаружена и в процессе антивирусной проверки, и когда уже проявились вредные последствия ее действия, и в результате деятельности правоохранительных органов (например, факт распространения вредоносной программы может быть выявлен в ходе проверочной закупки дисков, содержащих вредоносное ПО).

Доказывая факт преступного нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, целесообразно изучить пакет документов об эксплуатации компьютерной системы или сети, обеспечении их информационной безопасности. Правила обычно регламентируют порядок получения, обработки, накопления, хранения, поиска, распространения и представления компьютерной информации, а также ее защиты от неправомерных посягательств.

В большинстве случаев обнаружение нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации в первую очередь становится известным владельцам и пользователям компьютерной системы (сети) вследствие выявления отсутствия необходимой информации или ее искажения, негативно отразившегося на деятельности предприятия. Кроме того, факт совершения преступления может быть установлен в рамках служебной проверки, которая, как правило, проводится службой безопасности объекта.

2. Место совершения преступления.

Местом совершения (окончания) преступлений с материальным составом будет место наступления преступных последствий, а для преступлений с формальным составом – место совершения обозначенных в законе действий. Установление места несанкционированного доступа в информационно-технологическую систему может вызывать некоторые трудности, поскольку по делам данной категории место незаконного доступа и место наступления последствий, как правило, различны. Следует также учитывать, что мест такого несанкционированного доступа может быть несколько. При организации расследования следует учитывать правила ст. 152 УПК РФ.

При обнаружении факта неправомерного доступа к компьютерной информации необходимо установить: месторасположение

всех компьютеров, объединенных в локальную сеть; помещение, где находятся машинные носители с информацией; место хранения информации на электронных и бумажных носителях, полученных преступным путем.

Труднее определить место непосредственного применения технических средств удаленного несанкционированного доступа. Для этого требуется привлекать специалистов соответствующего профиля.

Определение места совершения преступления при расследовании преступлений в сфере сотовой радиотелефонной связи при непосредственном доступе включает обнаружение конкретного объекта у оператора связи (терминала связи, персонального компьютера и др.), посредством которого осуществлен доступ, а при удаленном способе устанавливается конкретный элемент сети сотовой связи, отражающий следы неправомерного доступа и место применения орудий преступления.

3. Время совершения преступления.

Дата и время отражаются в компьютере с помощью программ общесистемного назначения. Их изменение и несовпадение с реальным временем можно установить с помощью специальных программ либо в рамках производства таких следственных действий, как следственный осмотр или проведение компьютерной экспертизы.

При расследовании преступлений, связанных с несанкционированным доступом к сети сотовой радиотелефонной связи, специфика определения времени совершения преступления заключается в получении следующей информации: сведений из учетных данных биллинговой системы в сети сотовой связи, фиксирующих дату, время и продолжительность сеанса связи; данных, отраженных в программном обеспечении центров обслуживания абонентов (дата подключения к сети сотовой связи, период пользования связью и т. д.); отчетов, поступивших от роуминговых партнеров оператора связи.

При определении времени нарушения правил эксплуатации и незаконного доступа к компьютерной информации необходимо также установить и зафиксировать время наступления вредных последствий. Нарушение правил и наступление таких последствий могут произойти одновременно, а также между ними возможен временной интервал.

4. Способ совершения преступления.

5. Другие обстоятельства:

– описание объекта, где совершено преступление: технические и конструктивные особенности помещений, связанные с установкой и эксплуатацией ЭВМ, их сети или системы;

– состав вычислительного комплекса: тип, модель, размер носителей информации и другие характеристики компьютеров; наличие и типы периферийных устройств; состав и аппаратура организации локальной вычислительной сети; наличие, модель и характеристики устройств телекоммуникации; используемое программное обеспечение;

– организация работы со средствами вычислительной техники: состояние охраны; наличие и характеристика охранной сигнализации, вид охранной техники; организация противовирусной защиты; режим доступа к средствам вычислительной техники и машинным носителям;

– предмет преступного посягательства – характеристика информации;

– технические средства, использованные при совершении преступления: скимминговое оборудование, конкретный терминал, банкомат или участок сети и т. п.

II. Виновность и мотивы лиц, совершивших преступление.

Если преступление совершено группой лиц, то каковы роль, характер действий каждого участника, мотив преступления?

III. Характеристика личности обвиняемого.

Помимо традиционных аспектов необходимо установить наличие и уровень специальных познаний обвиняемого в области программирования, функционирования компьютерных систем и сетей. При совершении преступления лицом с использованием служебного положения следует выяснить, каковы его должностные обязанности, с какими служебными действиями связано преступление.

IV. Характер и размер ущерба, причиненного преступлением.

Характер ущерба, причиненного преступлением в сфере компьютерной информации, заключается в уничтожении, блокировании, модификации и (или) копировании компьютерной информации.

Ущерб может носить экономический характер, а также может повредить интересам организации, личности либо государства вследствие утечки конфиденциальных сведений.

V. Обстоятельства, способствовавшие совершению преступления в сфере компьютерной информации.

Такими обстоятельствами могут являться: нарушение установленных правил эксплуатации, режима доступа; использование несертифицированного программного обеспечения; нарушения, связанные со сроками использования паролей, и другие обстоятельства.

2. Особенности возбуждения уголовного дела по преступлениям в сфере компьютерной информации

Наиболее распространенными поводами к возбуждению уголовного дела являются:

1) заявления о преступлении:

– от представителей юридических лиц;

– от граждан;

2) сообщение о преступлении, полученное из иных источников:

– обнаружение уполномоченным лицом признаков состава преступления в рамках производства следственного действия или оперативно-розыскного мероприятия;

– при отработке информации, полученной из оперативных источников;

– по результатам документальных проверок, ревизий, аудиторских проверок; при задержании лица по горячим следам (например, при установке или снятии скиммингового оборудования на банкомат);

– в ходе расследования преступлений других видов;

– из сообщений в газетах, журналах, на телевидении;

3) постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании;

4) явка с повинной (как повод к возбуждению уголовного дела о преступлении в сфере компьютерной информации явка с повинной возможна, но на практике маловероятна).

Итак, при обнаружении признаков состава преступления в сфере компьютерной информации необходимо применить следующий алгоритм действий: получение объяснений, осмотр места происшествия, поручение на производство оперативно-розыскных мероприятий, процессуальное и непроцессуальное взаимодействие со специалистами, назначение и производство экспертиз. Необходимо также получить объяснение у заявителя, в котором должны содержаться: сведения о месте и времени совершения преступления, предмете преступного посягательства и его особенностях (реквизиты электронного документа, адрес электронной страницы и др.); основания, по которым заявитель имеет в собственности или владении компьютерную информацию (письменный договор с провайдером, интернет-карта и т. д.); сведения о причиненном вреде.

В зависимости от совершенного деяния также можно опросить инженеров-программистов, операторов ЭВМ, системных администраторов, инженеров по средствам связи и телекоммуникационному оборудованию, инженеров-электронщиков и других лиц.

В процессе опроса указанных лиц (а также заявителя) необходимо выяснить следующее:

– известны ли им обстоятельства преступления, кто и каким образом обнаружил факт преступного деяния;

– были ли факты хищений либо утраты электронных носителей информации;

– проявлял ли кто-либо интерес к содержимому мусорных емкостей (корзин, пакетов и т. д.);

– совершал ли кто-нибудь из сотрудников какие-либо необоснованные манипуляции с компьютерной информацией и (или) ее носителями;

– были ли потери массивов данных, какова причина утраты;

– срабатывали ли средства защиты компьютерной техники;

– появлялись ли в организации в последнее время посторонние лица, включая сотрудников специальных служб – сантехников, курьеров и т. п.;

– были ли подозрительные звонки, когда звонивший под любым предлогом интересовался данными работников, средствами идентификации и т. п.;

– были ли нарушения правил ведения отчетной документации (например, журналов учета рабочего времени операторов ЭВМ) и кто их допустил;

– были ли сотрудники, которые без видимых причин задерживались на рабочем месте или приходили раньше остальных;

– где еще расположены компьютеры и электронные носители информации;

– проводилось ли по факту преступного деяния служебное расследование;

– выполняются ли установленные инструкцией процедуры по обеспечению компьютерной безопасности.

Как правило, протокол осмотра места происшествия составляется в месте обнаружения следов преступления. В протоколе необходимо отразить: результат осмотра ЭВМ (их системы или сети), электронных носителей и содержащейся на них компьютерной информации; данные, подтверждающие или опровергающие факты, изложенные заявителем (потерпевшим).

На стадии возбуждения уголовного дела могут изыматься следующие документы и предметы:

– журналы фиксации сбоев в работе компьютерной сети, компьютеров или технических устройств; журналы учета рабочего времени операторов ЭВМ или компьютеров сети;

– документы о проведенных в течение дня операциях и т. п.;

– заключение о результатах служебного расследования, если по факту IT-инцидента оно проводилось, а также собранные специалистами службы безопасности следы преступления: лог-файлы сетевого оборудования организации, копии сетевого трафика, копии содержимого энергозависимых носителей информации и т. п.;

– энергозависимые и энергонезависимые носители информации (ЭВМ, НЖМД, флэш-накопители, аппаратные ключи и т. п.);

– данные журналов (электронных или бумажных) систем контроля доступа в помещения фирмы; данные систем видеонаблюдения за интересующим помещением, участком местности за максимально возможный промежуток времени;

– информация (в электронной и бумажной форме) о попытках незаконного использования компьютера, несанкционированного подключения к сети;

– список лиц, имеющих доступ к компьютерной информации, и список паролей;

– документы, подтверждающие факт распространения вредоносного программного обеспечения (например, кассовый или товарный чек);

– иные предметы и документы, на основании которых можно принять решение по материалу проверки.

При проведении проверки по материалу о преступлении в сфере компьютерной информации значительную работу выполняют оперативные работники, в частности сотрудники отделов «К». По результатам оперативно-розыскных мероприятий составляется обзорная справка, в которой необходимо отразить, каким способом получены сведения о преступлении, перечень проведенных мероприятий по установлению преступника и их результат.

В ряде случаев уголовное дело возбуждается по результатам проведения проверочной закупки, например, дисков с вредоносными программами.

Для решения вопроса о возбуждении уголовного дела следователь в ходе предварительной проверки материала должен получить информацию о предмете посягательства, месте его нахождения и условиях охраны; о характеристиках используемой компьютерной техники; о лицах, которые в силу своих обязанностей работали с предметом посягательства. При необходимости следователь должен изучить порядок учета, отчетности, документооборота, охраны объекта.

В материале проверки должны содержаться следующие необходимые сведения и документы:

1) заявление гражданина или представителя юридического лица или протокол устного заявления о преступлении;

2) рапорт об обнаружении признаков преступления и приложенные к нему материалы, полученные в ходе производства оперативно-розыскных мероприятий, ревизий, документальных и иных проверок;

3) объяснение заявителя;

4) документы (или их копии), подтверждающие права обладателя информации, подвергшейся преступному воздействию, либо отражающие неправомерно совершенную операцию (например, договоры на получение услуг Интернета, электросвязи,

договоры на обслуживание по банковской карте; свидетельство о праве собственности на программу для ЭВМ).

5) протокол осмотра места происшествия;

6) заключение специалиста о производстве предварительного исследования предметов и документов (ЭВМ, электронных носителей информации, распечаток, электронных документов и т. п.);

7) данные о пользователе (владельце, собственнике) ЭВМ (их системы или сети), посягнувшем на охраняемую законом компьютерную информацию;

8) документы, подтверждающие факт распространения вредоносного программного обеспечения, машинных носителей с такими программами, а также контрафактной продукции.

На момент принятия решения о возбуждении уголовного дела по признакам преступления в сфере компьютерной информации, как правило, складываются следующие исходные следственные ситуации.

1. Отсутствует информация о способе совершения преступления и личности преступника.

2. Способ совершения преступления известен, но неизвестна личность преступника.

3. Известны значимые обстоятельства, такие как способ совершения преступления, личность преступника и др.

3. Особенности тактики производства отдельных следственных действий по преступлениям в сфере компьютерной информации

Осмотр места происшествия

Место происшествия по рассматриваемой категории дел – это пространство, в пределах которого осуществлялись преступные действия, наступили вредные последствия, можно обнаружить следы преступления, предусмотренного гл. 28 УК РФ. Местами происшествия могут быть:

1) место обработки информации – предмета преступного посягательства (рабочее место, рабочая станция и т. д.);

2) сервер, сохранивший свидетельства о предмете посягательства или о работе системы за определенный период;

3) место использования технических средств для незаконного доступа к компьютерной информации; место создания, использования, распространения вредоносного ПО; место непосредственного нарушения правил эксплуатации ЭВМ;

4) место наступления вредных последствий, хранения магнитных носителей информации, полученной в результате неправомерного доступа;

5) территория, на которую распространяется зона покрытия (в случае совершения преступления в сфере мобильных коммуникаций).

Помимо «традиционных» участников следственно-оперативной группы при осмотре места происшествия целесообразно привлекать незаинтересованных специалистов, обладающих познаниями в области вычислительной техники, сетевых технологий, систем электросвязи.

Не рекомендуется привлекать в качестве специалистов инженерно-технический состав того объекта, где произошло преступление, так как указанные лица могут быть причастны к совершению преступного деяния.

При выезде на место происшествия целесообразно иметь следующую аппаратуру:

1) ноутбук с жестким диском большой емкости, дисководом, приводом CD-ROM;

2) соединительные кабели;

3) портативный принтер;

4) загрузочные носители с «исследовательским» и сервисным программным обеспечением;

5) внешний винчестер с программным обеспечением;

6) фотоаппарат, видеокамеру;

7) программное обеспечение общего и специального назначения (текстовый и табличный редактор, диагностические программы, программы сбора информации о файловой системе, антивирус, программы определения настроек аппаратуры и программ и ряд других);

8) упаковочный материал в достаточном количестве.

Целью осмотра места происшествия при расследовании преступлений в сфере компьютерной информации является установление конкретного средства вычислительной техники и определенной

компьютерной информации, выступающих в качестве предмета и (или) орудия совершения преступления и несущих в себе следовую информацию.

Алгоритм действий следователя при осмотре места происшествия следующий.

Первый этап

Следует начать с запрещения доступа к средствам вычислительной техники, электронным носителям информации всем лицам, за исключением специалиста. Обязательной охране подлежат все пункты отключения электропитания, находящиеся на месте происшествия.

Второй этап

Осмотр и составление протокола осмотра места происшествия.

Вопрос о специфике отражения фактических данных в протоколе осмотра места происшествия «компьютерного преступления» достаточно полно отображен в научной литературе. Так, в протоколе помимо традиционных данных должны быть указаны:

– технические и конструктивные особенности объекта, связанные с установкой и эксплуатацией средств вычислительной техники, а также его расположение;

– расположение технических средств видеонаблюдения и их состояние на момент осмотра;

– конфигурация специальных технических средств негласного получения компьютерной информации и машинных носителей.

При осмотре средств электронно-вычислительной техники в протоколе подробно описывают: тип (назначение), марку (название), цвет корпуса, заводской номер (серийный, инвентарный или учетный номер изделия), индивидуальные признаки средств вычислительной техники; тип (назначение), цвет и другие индивидуальные признаки соединительных и электропитающих проводов; какие разъемы задействованы и с какими внешними устройствами связаны; положение всех переключателей на всех блоках и устройствах.

Специалист принимает решение о необходимости включения аппаратуры или ее изъятия, при этом целесообразно в протоколе осмотра последовательно отразить все действия специалиста.

Информацию о паролях необходимо внести в протокол осмотра или в приложение к нему.

Осмотру и занесению в протокол подлежат следующие документы и их носители, являющиеся доказательствами подготовки, совершения и сокрытия преступления:

а) учетно-справочная документация по работе со средствами вычислительной техники и компьютерной информацией;

б) документация, отражающая санкционированность доступа (удостоверения личности, электронные ключи доступа, пароли, средства идентификации и аутентификации санкционированного пользователя);

в) учетно-регистрационная и бухгалтерская документация (лицензии, сертификаты, расчетно-кассовые и иные бухгалтерские документы);

г) учетно-контрольная документация;

д) документация, регламентирующая действия обслуживающего персонала (должностные обязанности; инструкции по работе со средствами вычислительной техники, программами для ЭВМ, средствами защиты; инструкции по работе оператора в нештатной (аварийной) ситуации);

е) рукописные тексты с паролями, адресами.

В дополнение к протоколу составляются: схема расположения компьютеров и периферийных устройств в помещении, схема соединения компьютеров в сети, фототаблица.

Осмотр электронного носителя и компьютерной информации в зависимости от ситуации возможно производить как в ходе осмотра места происшествия, так и при производстве отдельного следственного действия.

Осмотр производят по принципу «от общего к частному». Описание электронного носителя начинают с внешних индивидуальных признаков (название, вид, марка, цвет корпуса, размер), затем переходят к осмотру информации, содержащейся на электронном носителе.

В протоколе обязательно указываются все манипуляции со средствами компьютерной техники и их результат.

Описывая компьютерную информацию, следует помнить, что ее основной хранитель – это файл. В протокол подлежат занесению следующие сведения о компьютерной информации.

1. Размер области носителя, занятой под информацию, а также размер области носителя, свободной от записи.

2. Тип операционной системы.

3. Сведения о программах (список программ и их реквизиты; ранее устанавливающиеся, но удаленные программы).

4. Сведения о файлах документов (их список; тип информации (графические, текстовые, табличные и т. д.); местонахождение на носителе; размер хранимой информации; дата, время создания и изменения).

5. Атрибуты файла (архивный, скрытый, только для чтения и т. д.).

6. Статистика текста (формат, количество страниц, наличие выделенных областей).

7. Дополнительные комментирующие свойства (тема, автор, ключевые слова).

8. Наличие или отсутствие вредоносных программ, их название.

9. Название, версия и лицензионность антивирусной программы.

10. Какая именно информация, откуда, куда и каким способом была скопирована, количество копий.

11. О ранее удаленной, поврежденной, скрытой (но восстановленной), защищенной паролем (но расшифрованной) информации указываются: тип сокрытия (удаление, шифрование); какими программными средствами и с какого носителя удалось извлечь информацию, какова степень ее восстановления.

12. О программах особого назначения (криптографических, подбора паролей, удаленного доступа) и вредоносных программах указываются: их название, исполняемые функции, частота, время и направленность использования (если удается установить).

При осмотре страниц сайтов в протоколе помимо технических средств (ПЭВМ, принтера, модема и т. п.) указываются: операционная система, браузер (например, Internet Explorer или Opera), данные о провайдере, предоставившем доступ в сеть Интернет. Затем описывается пошаговый доступ к страницам интернет-сайта с указанием всех ссылок, к которым следователь должен будет обратиться для осмотра информационного ресурса; указываются электронные адреса страниц; осматривается соб-

ственно содержание страницы; указывается, находится ли информация в свободном доступе или требуется регистрация. К протоколу приобщается твердая копия скриншота страницы сайта.

При осмотре мобильных телефонов указываются наличие или отсутствие SIM-карты, ее номер и оператор, IMEI. После описания внешних признаков целесообразно изучить папки «Сообщения», «Контакты», «Вызовы», «Изображения», «Видео». Контакты могут указываться с формулировкой: «…имеется 134 контакта, абонентские номера с привязкой к именам…». При просмотре сообщений приводится текст сообщения, информация о том, от кого оно получено, дата поступления.

Третий этап – решение вопроса об изъятии предметов и документов и их упаковка.

Правила обращения с вычислительной техникой и носителями информации.

1. Все действия, связанные с режимом работы компьютера, применением криминалистической техники, должны осуществляться либо специалистом, либо под его руководством.

2. Необходимо исключить попадание мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.).

3. Запрещено подвергать диски электромагнитному, механическому воздействию.

4. Необходимо соблюдать допустимые температуры при хранении и транспортировке компьютерной техники и машинных носителей информации (от 0 до +50 °С).

Общие правила изъятия компьютерной техники и электронных носителей информации.

1. Запретить доступ к средствам вычислительной техники и электрощиту всем лицам, за исключением специалиста. Желательно отключить сетевые соединения компьютеров.

2. Выключенные устройства не включать.

3. Сфотографировать или произвести видеосъемку электронных носителей информации, компьютерной техники и периферийных устройств, подключенных кабелей.

4. Сфотографировать изображение на мониторе компьютера, если на момент производства следственного действия он включен.

5. Все, что находится в лотке принтера, следует описать, в случае необходимости – изъять. Если принтер что-либо печатает, необходимо дождаться окончания печати.

6. Компьютерная техника хранится и транспортируется в выключенном состоянии.

7. Упаковку изъятого производить в тару изготовителя либо в коробку, пакет, конверт таким образом, чтобы исключить доступ внутрь.

8. Информацию из оперативной памяти компьютера необходимо изымать путем ее копирования на электронный носитель с использованием стандартных паспортизированных программных средств.

9. Во время изъятия компьютерной техники, электронных носителей не должна изменяться никакая содержащаяся на них информация. В случае необходимости следователь должен представить убедительные доказательства того, что представленная эксперту или суду компьютерная информация не изменялась ни в процессе производства следственного действия, ни при последующем хранении. В противном случае изъятая компьютерная информация может быть признана недопустимым доказательством.

10. Доступ к компьютерной информации и ее исследование в ходе производства следственного действия (обыска, осмотра, выемки и т. п.) допустимы лишь в тех случаях, когда невозможно изъять носитель с информацией и отправить его на экспертизу. Такой доступ и исследование должны производиться компетентным специалистом, который в состоянии понять и объяснить смысл и все последствия производимых им действий. В рассматриваемом случае все действия специалиста и полученные результаты должны быть подробно зафиксированы в протоколе следственного действия.

При решении вопроса об изъятии средств вычислительной техники и электронных носителей следователь должен руководствоваться следующими факторами.

1. Если изъятие не нанесет существенного ущерба нормальному функционированию фирмы, выполнению производственных или иных задач, следует изъять средства вычислительной техники и магнитные носители информации для последующего производства экспертизы в лабораторных условиях.

2. Если изъятие оборудования критично для нормального функционирования организации или имеются основания считать, что отключение каких-либо средств вычислительной техники либо их части может привести к утере доказательственной информации, необходимо проводить детальный осмотр непосредственно на месте происшествия.

Уголовно-процессуальным законодательством предусмотрена возможность не только изъятия компьютерной информации, но и ее копирования. Копирование осуществляется специалистом. При копировании обеспечиваются условия, исключающие возможность изменения или утраты информации. Не допускается копирование информации, если это может воспрепятствовать расследованию преступления. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изъятых электронных носителей или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации составляется протокол.

Допрос

При подготовке к допросу необходимо выполнить следующие действия.

1) изучить материалы дела, определить очередность проведения допросов;

2) предварительно изучить личность допрашиваемого (получить сведения о лице по месту жительства, учебы, работы, досуга);

3) получить консультацию специалиста и составить план допроса.

Расследование преступлений в сфере компьютерной информации сопряжено с необходимостью использования специальной терминологии, зачастую не вполне понятной следователю, но абсолютно ясной допрашиваемому. В связи с этим следователю целесообразно проконсультироваться со специалистом, предварительно согласовав с ним формулировки вопросов, подлежащих выяснению.

Допрашиваемое лицо может употреблять специальные термины, жаргонные понятия. В этом случае следователю необходимо путем постановки уточняющих вопросов постараться раскрыть содержание профессиональных и жаргонных определений.

В случае необходимости следует попросить допрашиваемого составить поясняющую схему, приобщить ее к протоколу допроса.

При допросах необходимо установить: обстоятельства, место и время, способ совершения преступления; мотивы и цели преступных действий; характеристику предмета преступления; последствия преступных действий и размер причиненного вреда; данные о лицах, совершивших преступление; другие обстоятельства, имеющие значение для дела.

В ходе *допроса потерпевших* можно выяснить обстоятельства выявления преступления и его последствия; предварительно оценить причиненный ущерб; узнать о способах защиты информации, порядке организации охраны объекта; получить точные данные о предмете преступного посягательства, а также предварительные данные о личности виновного и ряде других обстоятельств.

При расследовании преступлений, предусмотренных гл. 28 УК РФ, *в качестве свидетелей могут выступать*: программист, администратор, сотрудник, занимающийся техническим обслуживанием, оператор ЭВМ, начальник вычислительного центра, руководитель предприятия, администратор сети, сотрудник компании мобильной связи, работник бухгалтерии и другие лица.

Начинать *допросы свидетелей* целесообразно с лиц, которые обнаружили факт совершения преступления или его последствия.

Формулировка вопросов для выяснения интересующей следствие информации может быть следующей.

При каких обстоятельствах обнаружен факт преступного деяния, каковы последствия и какие меры принимались для их устранения? Производилась ли переустановка операционной системы компьютера после обнаружения инцидента?

Проводилось ли служебное расследование по факту инцидента и каковы его результаты?

Отображались ли вам какие-либо необычные сообщения при работе с системой? Замечали ли вы какие-либо необычные события при работе с компьютером непосредственно до выявленного преступления?

Проявлял ли кто-либо повышенный интерес к компьютерной информации, программному обеспечению, компьютерной технике, способу доступа в помещения или способу доступа к информации?

Появлялись ли на территории посторонние лица?

Были ли сбои в работе программ, компьютерного оборудования, средств защиты компьютерной информации? Имели ли место факты хищения либо утраты электронных носителей информации и отдельных компьютерных устройств?

Как часто проводится антивирусная проверка? Каковы результаты последних проверок, где они отражены?

Как часто обновляется программное обеспечение, где и кем оно приобретается?

Кто, когда и где приобретал компьютерную технику?

Кто из сотрудников работает в сети, каковы их обязанности и права?

Имеется ли защита компьютерной информации?

Как организован доступ организации в сеть Интернет? Какие программные средства удаленного (сетевого) управления установлены на компьютере?

Были ли ранее зафиксированы факты неправомерного доступа к компьютерной информации?

Могли ли возникшие последствия стать результатом неосторожного действия лица или неисправности работы компьютерной техники, сбоев программного обеспечения и т. п.?

Каков характер изменений информации?

Кто является обладателем поврежденной информации?

В ходе проведения допросов подозреваемых, обвиняемых необходимо выяснить следующие обстоятельства.

1. Обстоятельства общего характера:

– наличие среднего профессионального или высшего образования;

– был ли судим; если да, то когда, за какое преступление;

– состоит ли на учете в наркологическом и (или) психоневрологическом диспансере;

– место работы, должность, уровень материального достатка;

– профессиональные навыки и опыт работы с компьютерной техникой и программным обеспечением, уровень владения ими;

– должностные обязанности, связанные с правомерным доступом к компьютерной технике и программному обеспечению;

– перечень конкретных действий с компьютерной информацией, осуществляемых на рабочем месте;

– закреплены ли за ним по месту работы идентификационные коды и пароли для пользования компьютерной сетью;

– наличие компьютера по месту жительства; круг лиц, им пользующихся;

– какова конфигурация компьютера, имеющегося по месту жительства (по месту работы), изъятого при обыске;

– какое программное обеспечение установлено на компьютере; переустанавливали ли операционную систему; если да, то когда;

– какие пароли установлены на вход в операционную систему;

– установлены ли на компьютере антивирусные или защитные программы;

– наличие правомерного доступа к сети Интернет и работы в Интернете;

– какие ники, электронные почтовые ящики, сайты, домашние страницы принадлежат подозреваемому (обвиняемому) в сети Интернет;

– кто настраивал удаленный доступ к сети и (или) доступ для выхода в Интернет;

– услугами каких провайдеров пользовался подозреваемый (обвиняемый) для выхода в Интернет.

2. Обстоятельства, предшествовавшие совершению преступления:

– каковы мотивы и цель совершения преступления;

– когда возникло намерение совершить преступление, кто или что повлияло на это решение;

– почему выбран именно данный объект для преступного посягательства.

3. Обстоятельства совершения преступления:

– место и время совершения преступления;

– способы проникновения в помещение, где установлена компьютерная техника, или способы осуществления неправомерного доступа в компьютерную систему, сеть;

– приемы подбора или хищения ключей и паролей, разрушения и отключения средств защиты;

– источники получения данных о потерпевшей стороне, в том числе о мерах защиты информации;

– какие орудия использовались при совершении преступления;

– способ сокрытия неправомерного доступа;

– использовалось ли для совершения преступления служебное положение и в чем это конкретно выразилось;

– наличие сговора с другими лицами и данные о них; кто инициатор, каким образом распределили роли и почему;

– детали состоявшейся преступной договоренности;

– действия по подготовке преступления;

– раскаивается ли подозреваемый (обвиняемый) в содеянном.

Обыск и выемка

В процессе подготовки к обыску (выемке) в помещении необходимо:

– определить время производства обыска и меры, обеспечивающие конфиденциальность обыска;

– установить наличие, вид, количество вычислительной техники, а также устройств автономного или бесперебойного питания в обыскиваемом помещении;

– изучить данные о лицах, могущих находиться или проживающих в обыскиваемом помещении;

– подготовить соответствующую аппаратуру для считывания и хранения изъятой информации, упаковочный материал;

– определить состав участников данного следственного действия (целесообразно пригласить, как минимум, специалиста и оперативных работников)

– провести инструктаж.

Порядок производства обыска (выемки).

1. В обыскиваемое помещение необходимо войти быстро и неожиданно, чтобы предотвратить уничтожение информации на ЭВМ.

2. Не допускать лиц, находящихся в квартире (помещении), к ЭВМ и источникам питания.

3. Предложить добровольно выдать предметы, запрещенные к свободному гражданскому обороту, деньги и ценности, добытые преступным путем, а также компьютер и носители информации, использовавшиеся для преступных целей. Если происходит добровольная выдача ЭВМ и (или) электронных носителей

информации, необходимо акцентировать внимание понятых на этом факте и уточнить у виновного, с какими именно преступными целями использовалась аппаратура, о чем сделать соответствующую запись в протокол.

4. По согласованию со специалистом можно включить компьютер, записать его характеристики и операционную систему, указать, имеется ли пароль при входе в систему, описать вид рабочего стола компьютера и вынесенные на него иконки запускаемых приложений, а также указать другие данные, о которых упоминалось при рассмотрении вопроса о производстве осмотра. Целесообразно привлечь виновного к даче пояснений в процессе осмотра ЭВМ и носителей информации.

5. Осуществить мероприятия, направленные на поиск тайников.

6. Следует обращать внимание на традиционные источники доказательственной информации: специальную литературу (рекламные проспекты, справочники и каталоги по компьютерной технике, пособия и учебники по обработке, защите, передаче и негласному получению компьютерной информации), распечатки компьютерной информации, документы о соответствующем профессиональном образовании, свободные образцы почерка, бланки и фрагменты документов, исходные тексты программ для ЭВМ, черновики и иные образцы для сравнительного исследования.

7. Особое внимание рекомендуется обращать на записи паролей, логинов, электронных адресов, алгоритмы входа и работы в компьютерных системах и сетях.

При производстве обыска можно руководствоваться рядом рекомендаций для производства осмотра места происшествия.

Рассмотренные следственные действия (осмотр, допрос, обыск и выемка) наиболее специфичны и типичны при расследовании преступлений в сфере компьютерной информации.

Назначение и производство судебных компьютерно-технических экспертиз

Судебная компьютерная экспертиза (СКЭ) – самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических, который проводится в целях определения статуса объекта как компьютерного средства, выявления и изучения его следовой картины в расследуемом преступлении, а также полу-

чения доступа к информации на носителях данных с последующим всесторонним ее исследованием.

Судебная компьютерная экспертиза подразделяется на несколько направлений:

1) аппаратно-компьютерная экспертиза (проведение исследования (в основном диагностического) технических (аппаратных) средств компьютерной системы);

2) программно-компьютерная экспертиза (исследование программного обеспечения);

3) информационно-компьютерная экспертиза (поиск, обнаружение, анализ и оценка информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе);

4) компьютерно-сетевая экспертиза (исследование сетевых и телекоммуникационных технологий).

До вынесения постановления о назначении экспертизы рекомендуется проконсультироваться с экспертом (специалистом) по поводу ее целей, формулировки вопросов, характера предоставляемых материалов.

Объектами экспертизы являются компьютеры, периферийные устройства, системное программное обеспечение, текстовые и графические документы, изготовленные с использованием компьютерных средств, сетевые аппаратные средства, мобильные телефоны, интегрированные системы и др.

Примерный перечень вопросов, решаемых в рамках компьютерной экспертизы.

1. Вопросы по исследованию аппаратных средств.

Относится ли представленное на исследование устройство к аппаратным компьютерным средствам?

Если да, то к какому типу (марке, модели)? Каковы его технические характеристики и параметры?

Каково функциональное предназначение представленного аппаратного средства?

Какое первоначальное состояние (конфигурацию, характеристики) имело аппаратное средство?

Каково фактическое состояние (исправен, неисправен) представленного аппаратного средства? Имеются ли в нем отклонения

от типовых (нормальных) параметров, в том числе физические дефекты?

Каковы причины изменения функциональных (потребительских) свойств в начальной конфигурации представленного аппаратного средства?

Является ли представленное аппаратное средство носителем информации?

Какой вид (тип, модель, марку) имеет представленный носитель информации?

2. Вопросы по исследованию программных средств.

Какова общая характеристика представленного программного обеспечения, из каких компонент (программных средств) оно состоит?

Каков состав соответствующих файлов программного обеспечения, каковы их параметры (объемы, даты создания, атрибуты)?

Какое общее функциональное предназначение имеет программное средство и является ли оно вредоносным?

Имеются ли в программном средстве отклонения от нормальных параметров (например, свойства инфицирования, недокументированных функций)?

Имеет ли программное средство защитные возможности (программные, аппаратно-программные) от несанкционированного доступа и копирования?

Подвергался ли алгоритм программного средства модификации по сравнению с исходным состоянием?

Какой вид имело программное средство до его последней модификации?

С какой целью было произведено изменение каких-либо функций в программном средстве?

Направлены ли внесенные в программное средство изменения на преодоление его защиты?

Каким способом были произведены изменения в программе (преднамеренно, воздействием вредоносной программы, ошибками программной среды, аппаратным сбоем и др.)?

3. Вопросы по исследованию информации (данных).

Как отформатирован носитель информации и в каком виде на него записаны данные?

Каковы характеристики физического и логического размещения данных на носителе информации?

Какие свойства, характеристики и параметры (объемы, даты создания и изменения, атрибуты и др.) имеют данные на носителе информации?

Какого вида информация (явная, скрытая, удаленная, архив) имеется на носителе?

Каким образом организован доступ (свободный, ограниченный и пр.) к данным на носителе информации и каковы его характеристики?

Какие свойства, характеристики имеют выявленные средства защиты данных и какие возможны пути ее преодоления?

Каково содержание защищенных данных?

Какие данные о собственнике (пользователе) компьютерной системы (в том числе имена, пароли, права доступа и пр.) имеются на носителях информации?

Каково первоначальное состояние данных на носителе (в каком виде, какого содержания и с какими характеристиками, атрибутами находились определенные данные до их удаления или модификации)?

Каким способом и при каких обстоятельствах произведены операции (блокирование, модификация, копирование, удаление) с определенными данными на носителе информации?

Какая имеется причинная связь между действиями с данными (вводом, модификацией, удалением и пр.) и имевшим место событием (например, нарушением в работе компьютерной системы, в том числе сбоями в программном и аппаратном обеспечении)?

4. Вопросы комплексного исследования компьютерной системы (при экспертизе целостной компьютерной системы).

Является ли представленное оборудование компьютерной системой?

К какому типу (марке, модели) относится компьютерная система?

Какой состав (конфигурацию) и технические характеристики имеет компьютерная система?

Какое функциональное предназначение имеет компьютерная система?

Имеет ли компьютерная система какие-либо отклонения от типовых (нормальных) параметров, в том числе физические (механические) дефекты?

Существуют ли в компьютерной системе недокументированные (сервисные) возможности? Какие это возможности?

Какие носители информации имеются в представленной компьютерной системе?

Какая система защиты информации имеется в представленной компьютерной системе? Каков тип, вид и характеристики этой системы защиты? Каковы возможности по ее преодолению?

Какова стоимость производственных и эксплуатационных дефектов компьютерных средств?

Итак, компьютерная экспертиза может дать ответ на вопросы об установлении времени и последовательности совершения пользователем определенных действий; исследовать программы для ЭВМ на предмет их принадлежности к вредоносным, к средствам нейтрализации защиты, к инструментам для осуществления неправомерного доступа к компьютерной информации, к специальным техническим средствам, предназначенным для негласного получения информации; выполнить поиск на электронном носителе документов, изображений, сообщений и иной информации, относящейся к делу, в том числе в неявном виде; определить степень функциональности программ, принципа действия, вероятного их источника. Однако компьютерная экспертиза не отвечает на вопросы об установлении личности пользователя, это задача следователя.

Вышеуказанный перечень вопросов не является обязательным. В каждом конкретном случае формулировки и сущность вопросов могут значительно отличаться.

С целью избежать ошибок при формулировке и выборе вопросов целесообразно осуществлять процессуальное и непроцессуальное взаимодействие с соответствующим специалистом, особенно при составлении постановления о назначении экспертизы.

По делам о преступлениях в сфере компьютерной информации целесообразно назначение комплексных экспертиз, например, технической экспертизы документов, экономической, бухгалтерской, товароведческой экспертизы.

Тема 2. Особенности расследования преступлений в сфере компьютерной информации на последующем и заключительном этапах расследования

План

1. Процессуальный порядок привлечения лица в качестве обвиняемого по уголовным делам в сфере компьютерной информации.

2. Особенности тактики производства отдельных следственных действий на последующем и заключительном этапах расследования преступлений в сфере компьютерной информации.

1. Процессуальный порядок привлечения лица в качестве обвиняемого по уголовным делам в сфере компьютерной информации

Процессуальный порядок привлечения лица в качестве обвиняемого установлен гл. 23 УПК РФ и не имеет специфики при расследовании преступлений в сфере компьютерной информации.

При вынесении постановлений о привлечении лица в качестве обвиняемого в совершении преступлений, предусмотренных гл. 28 УК РФ, следователь должен учитывать ряд особенностей, связанных со спецификой конструкций ст. 272–274 УК РФ.

Так, в описательно-мотивировочной части постановления о привлечении лица в качестве обвиняемого в совершении преступления, предусмотренного ст. 272 УК РФ, следователь должен указать следующее.

1. Каким законом охраняется компьютерная информация.

Например: «…имея умысел, направленный на неправомерный доступ к охраняемой законом, а именно Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», компьютерной информации, принадлежащей Ю...».

2. Способ совершения преступления.

Возможно использование, например, следующей формулировки: «5 мая 2016 года Р. через неустановленную следствием

интернет-программу скачал на свой персональный компьютер «Асер» компьютерную программу – программное обеспечение «Jungle Flasher», заведомо предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, с целью последующего ее использования для неправомерной модификации компьютерной информации игровой консоли «Xbox 360» и получения за данную услугу денежного вознаграждения».

Формулировка может также быть следующей: «М. в период с 12 часов 15 минут по 12 часов 38 минут 25 августа 2017 года, находясь по адресу: г. Краснодар, ул. Садовая, 45, имея навык обращения с компьютерным и сетевым оборудованием, используя принадлежащую ей электронно-вычислительную машину марки «Сони», используя IP-адрес 111111, выделенный ей ООО «Марка», имея умысел, направленный на неправомерный доступ к охраняемой законом, а именно Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», компьютерной информации, принадлежащей Ю., зная логин электронной почты yjuj6768@mail.ru, ввела логин и путем подбора пароля для получения доступа к электронному почтовому ящику указанной почты, принадлежащему легальному пользователю Ю., осуществила неправомерный доступ к содержимому данного электронного почтового ящика, в котором находилась охраняемая законом компьютерная информация».

3. Наступившие последствия.

Возможно использование такой формулировки: «…блокировал работу абонента… в глобальной сети Интернет, что выразилось в невозможности работы законного пользователя в период времени несанкционированного выхода в Интернет, с использованием пароля и логина, принадлежащих…».

В описательно-мотивировочной части постановления о привлечении лица в качестве обвиняемого в совершении преступления, предусмотренного ст. 273 УК РФ, следователь должен указать следующее.

1. Способ совершения преступления.

Возможно использование, например, такой формулировки: «10 октября 2018 года С., находясь на своем рабочем месте в ООО «МИР», по адресу: г. Анапа, ул. Красная, 5, используя вверенную ему для исполнения своих должностных обязанностей электронно-вычислительную машину «Асус», создал компьютерную программу «Форма», позволившую добавить функцию «подмена номера» в конфигурации формы базы данных «микрофинансовая организация» программного обеспечения «1С:Предприятие» и доработки программного кода обработки. Реализуя свой преступный умысел, С. распространил вредоносное программное обеспечение «Форма» путем предоставления доступа к нему сотрудникам ООО «МИР» сетевым способом».

2. Наступившие тяжкие последствия.

Возможно использование следующей формулировки: «Полученные результаты работы данной вредоносной компьютерной программы, а именно парольно-логиновые комбинации и иные реквизиты держателей банковских карт, используемые при совершении платежей через сеть Интернет, Н. посредством интернет-сервиса… позволяющего обмениваться сообщениями в однократном режиме, передавал за денежное вознаграждение неустановленным пользователям сети Интернет».

В описательно-мотивировочной части постановления о привлечении лица в качестве обвиняемого в совершении преступления, предусмотренного ст. 159.6 УК РФ, следователь должен указать следующее.

1. Способ совершения преступления.

Возможно использование, например, такой формулировки: «Б., находясь по адресу: г. Москва, пер. Акимовский, 234, путем ввода компьютерной информации в электронные устройства хранения и обработки компьютерной информации банковской организации, используя принадлежащий потерпевшей А. мобильный телефон, а также сим-карту с абонентским номером 9898977777 посредством направления СМС-сообщения на единый абонентский номер… по услуге денежных переводов, действуя умышленно и незаконно, перевела со счета банковской карты ПАО «Сбербанк России» №… принадлежащие А. денежные средства

на счет банковской карты ПАО «Сбербанк России» №… зарегистрированной на имя Б., тем самым похитила денежные средства в размере 4 000 рублей, принадлежащие А.».

2. Наступившие последствия.

Например: «…путем ввода компьютерной информации – СМС-сообщения на номер 900 в функционирование информационно-телекоммуникационной сети оператора сотовой связи «МТС» осуществил перевод денежных средств в сумме 50 000 рублей с расчетного счета банковской карты № 2323666 на счет электронного кошелька системы «Киви», находящегося в его пользовании».

2. Особенности тактики производства отдельных следственных действий на последующем и заключительном этапах расследования преступлений в сфере компьютерной информации

Следственный эксперимент

На последующем этапе расследования для установления криминалистически значимой информации, направленной на выявление всех обстоятельств по уголовному делу, а также конкретных лиц, причастных к его совершению, возникает необходимость в производстве следственного эксперимента. При этом в связи с особенностью рассматриваемого состава, а именно обнаруженными компьютерно-техническими следами и высокой технической квалификацией лиц, совершающих указанные преступления, проводятся эксперименты, целью которых является следующее:

– проверка возможности проникновения в помещение (через двери, окно, с отключением и без отключения сигнализации);

– проверка возможности подключения компьютерной техники и совершения непосредственного доступа к компьютерной информации;

– проверка возможности проникновения в закрытые зоны путем подбора паролей, идентификационных кодов и установления периода времени для данного подбора;

– проверка возможности подключения к компьютерной сети;

– проверка возможности электромагнитного перехвата;

– установление периода времени, необходимого на подключение к компьютерной сети;

– установление периода времени, необходимого на отключение технических средств защиты информации;

– установление промежутка времени, необходимого для модификации, копирования компьютерной информации;

– проверка возможности совершения определенных операций с компьютерной информацией в одиночку;

– проверка возможности совершения определенных операций с помощью конкретной компьютерной техники за определенный промежуток времени и др.

Тактические приемы проведения следственного эксперимента:

– проведение опытов в определенном режиме;

– многократность проведения опытов (при необходимости);

– проведение опытов в условиях, максимально приближенных к тем, при которых имели место событие, факт, явление;

– проведение опытов поэтапно (при необходимости);

– принятие во внимание изменившихся и не поддающихся реконструкции условий;

– варьирование условий и обстановки (изменение скорости, темпа и т. д.).

К числу обязательных участников следственного эксперимента относятся: следователь или оперативный работник, которому поручено производство этого следственного действия; специалист в области компьютерной техники; понятые в количестве не менее двух человек. Понятых следует приглашать из числа лиц, владеющих компьютерной техникой. К числу необязательных участников закон относит подозреваемого, обвиняемого, свидетеля, специалиста, переводчика, педагога, защитника.

В целях фиксации показаний с использованием видеосъемки необходим специалист-оператор. В определенных случаях необходимо также участие специалиста-криминалиста.

Максимальное сходство условий проведения следственного эксперимента с условиями, в которых происходило совершение преступления, обеспечивается следующим:

а) реконструкцией обстановки для производства опытов, что позволит достичь максимального сходства между опытной и реальной обстановкой совершения преступления;

б) использованием подлинных или сходных по техническим характеристикам (аналогичных) предметов компьютерной техники, программно- и технически совместимого периферийного оборудования, тех же версий программного обеспечения и т. п., о которых говорил обвиняемый;

в) учетом изменившихся и не поддающихся реконструкции условий;

г) воспроизведением (моделированием) субъективных, психофизиологических факторов.

При совершении неправомерного доступа к компьютерной информации внешние условия обстановки чаще всего не имеют такого принципиального значения, как при совершении других преступлений. Поэтому при оценке результатов следственного действия необходимо учитывать в первую очередь степень совпадения и соответствия технических характеристик и параметров используемой компьютерной техники, состояние и версии программного обеспечения, тип операционной системы, общую конфигурацию компьютера и пр. Однако погодные условия могут оказывать влияние на результаты опытов по проверке возможности осуществления перехвата информации.

Рассматриваемое следственное действие проводится в том же темпе и при той же продолжительности действий.

Многократность проведения однородных опытов. Количество повторений определяется в зависимости от наступления результатов. При этом не имеет значения, будут ли они положительными или отрицательными.

Изменение условий проведения опытов. В тех случаях когда следствие не располагает точными данными об условиях, каких-либо параметрах проверяемого события, необходимо изменять условия проведения опытных действий. Следует иметь в виду, что опытные действия в измененных условиях также повторяются многократно.

Иногда опытные действия целесообразно проводить в измененных условиях – худших, по сравнению с теми, которые существовали на момент проверяемого события. Такие опытные дей-

ствия проводятся после экспериментальных, осуществленных в условиях, максимально сходных с теми, которые имели место на момент проверяемого события. Результаты таких действий усиливают достоверность первых опытных действий.

Соответствие профессиональных навыков лица, осуществляющего опыты, профессиональным навыкам непосредственного участника исследуемого события. Если непосредственный участник исследуемых событий не может принять участие в следственном эксперименте, то лицо, заменяющее его, должно подбираться из числа обладающих такими же профессиональными навыками.

Обеспечение безопасности участников следственного действия. Следователь обязан обеспечить безопасность всех участников следственного действия. Если есть информация о том, что обвиняемый может оказать противодействие проведению эксперимента, то необходимо подготовить и проинструктировать следственную группу, предусмотреть применение средств защиты, оружия, специальных средств.

На процессуальном уровне обеспечение реальной безопасности связано с реализацией требований о неразглашении данных предварительного следствия. Следователь предупреждает лиц, присутствующих при производстве следственного действия, о недопустимости разглашения сведений, полученных в процессе опытов, без его разрешения.

К числу наиболее распространенных тактических рекомендаций можно отнести:

– удаление посторонних лиц с места проведения следственного действия;

– проведение следственного действия в такое время, когда исключено присутствие посторонних лиц;

– обеспечение надлежащей охраны присутствующих лиц;

– обеспечение оцепления места проведения следственного действия;

– сокрытие фабулы дела и анкетных данных лица, чьи показания проверяются;

– наличие резерва сил для быстрого и эффективного реагирования на экстремальную ситуацию, которая может сложиться при проведении следственного действия, и т. п.

Принимая решение о производстве следственного эксперимента, следователь обязан тщательно продумать ход его проведения. Особое внимание необходимо уделить сохранности программного обеспечения и иной компьютерной информации, которая может являться доказательством по делу.

Комплекс подготовительных мероприятий, как правило, осуществляется в два этапа: до выезда (выхода) на место проведения следственного эксперимента и по прибытии на него.

К подготовительным мероприятиям до выезда на место проведения следственного эксперимента относятся:

– определение задач, условий, содержания и способов производства опытов;

– установление места, времени, очередности опытных действий;

– предварительное ознакомление с обстановкой на месте проведения эксперимента;

– определение состава участников;

– подготовка необходимого реквизита и технико-криминалистических средств;

– проведение реконструкции обстановки или отдельных предметов (при необходимости);

– составление плана проведения следственного эксперимента.

К подготовительным мероприятиям, осуществляемым по прибытии на место проведения следственного эксперимента, относятся:

– выяснение наличия изменений в обстановке за время, прошедшее после предварительной реконструкции;

– новая реконструкция обстановки (при необходимости);

– проверка соответствия условий эксперимента условиям события, которое проверяется;

– разъяснение прав, обязанностей и инструктаж участников эксперимента;

– проверка наличия и готовности реквизита и технико-криминалистических средств;

– установление средств связи и сигналов между участниками эксперимента;

– принятие мер по охране места проведения опытных действий (при необходимости).

Приведенные рекомендации по подготовке к производству следственного эксперимента при расследовании преступлений в сфере компьютерной информации носят общий характер и должны уточняться в зависимости от конкретного эксперимента. Тактические особенности варьируются в зависимости от вида и целей следственного эксперимента.

Проверка и уточнение показаний на месте

При расследовании преступлений, совершенных в сфере компьютерной информации, одним из эффективных способов исследования доказательств, содержащихся в показаниях свидетелей, потерпевших, подозреваемых, обвиняемых, является проверка и уточнение показаний на месте. Данное следственное действие предусмотрено ст. 194 УПК РФ.

Проверка и уточнение показаний на месте на последующем этапе расследования неправомерного доступа к компьютерной информации может и должна проводиться в следующих случаях:

– когда обвиняемый не знает точного адреса помещения (дома, квартиры), из которого осуществлялся опосредованный доступ к компьютерной информации (например, обвиняемый находился там вместе с соучастниками непродолжительное время), но может указать маршрут следования;

– когда обвиняемые говорят о помещении, из которого осуществлялся непосредственный доступ, но информация о месте расположения помещения различается;

– когда обвиняемый говорит о помещении, из которого осуществлялся непосредственный доступ к компьютерной информации, но описание не соответствует действительности (тому помещению, в котором проводился осмотр места происшествия);

– когда обвиняемый говорит об определенном расположении помещений, однако их расположение на месте происшествия иное;

– когда обвиняемый дает показания об определенном расположении, конфигурации и составе компьютерной техники, однако их расположение на месте происшествия иное.

Возможно проведение указанного следственного действия и в иных ситуациях.

Перед проведением проверки и уточнения показаний на месте необходимо провести комплекс подготовительных мероприятий, который включает следующее.

1. Определение цели проверки показаний на месте.

2. Сбор и анализ информации, необходимой для целенаправленного проведения следственного действия. При подготовке целесообразно проанализировать протоколы следственных действий, ознакомиться с результатами проведенных оперативно-розыскных мероприятий. Целесообразно рассмотреть вопрос о дополнительном допросе лица, чьи показания проверяются.

3. Детальный допрос лица, показания которого будут проверяться.

4. Выявление подлинных мотивов согласия подозреваемого или обвиняемого на участие в проверке показаний на месте.

5. Изучение личности субъекта, чьи показания надлежит проверить.

6. Предварительное изучение места проведения следственного действия, если оно известно заранее.

7. Определение порядка движения и составление плана проверки показаний на месте. При проведении проверки следователь может предложить лицу, чьи показания проверяются, выполнить те или иные конкретные действия в определенных местах. Например, показать, каким образом преодолевалась техническая, физическая и интеллектуальная (программная) защита компьютерной информации, осуществлялся неправомерный доступ к ней и т. п.

8. Определение времени проведения проверки и уточнения показаний на месте обусловлено необходимостью уменьшения опасности вмешательства посторонних лиц, создания безопасных условий для участников следственного действия.

В отдельных случаях, исходя из тактических соображений, проверку следует проводить немедленно после получения согласия обвиняемого (например, продемонстрировать способ несанкционированного входа в компьютерную сеть), так как в последующем он может отказаться от этого.

9. Приглашение понятых. Если проверка проводится в нескольких местах или с несколькими проверяемыми, то целесообразно приглашать разных понятых. В случае их последующего вызова в суд для допроса в качестве свидетелей важнейшую роль будет играть степень объективности восприятия и запоминания ими всех обстоятельств наблюдавшихся действий.

10. Подбор участников следственного действия находится в прямой зависимости от того, чьи показания проверяются (свидетель, потерпевший, обвиняемый), его намерений и т. д., однако в

любом случае приглашаются специалист в области компьютерной техники и специалист, который бы обеспечил видеосъемку. В необходимых случаях для участия в проверке могут приглашаться педагог, переводчик, защитник и др.

11. Подготовка технических и транспортных средств (например, средств связи, освещения, фиксации хода и результатов следственного действия; компьютерной техники, которая использовалась при совершении преступления или находилась на месте происшествия).

12. Обеспечение реальной безопасности участников проверки.

13. Инструктаж участников проверки включает разъяснение им их прав и обязанностей, целей и задач следственного действия, порядка его производства.

Тактические приемы проверки показаний на месте следующие:

1) добровольное согласие лица, показания которого решено проверить;

2) детализация и уточнение показаний на месте их проверки;

3) проведение проверки показаний с каждым лицом в отдельности (при проверке показаний нескольких лиц);

4) предоставление лицу, показания которого проверяются, свободы движения и выбора маршрута;

5) сочетание в ходе проверки показаний рассказа и демонстрации действий проверяемого лица;

6) проведение на месте поисковых действий с целью обнаружения следов преступления;

7) сравнение следователем показаний проверяемого лица с обстановкой конкретного места и собранными доказательствами.

Благодаря специфике проверки и уточнения показаний на месте при расследовании преступлений в сфере компьютерной информации можно получить новые доказательства причастности лица к расследуемому преступлению, выявить новые эпизоды противоправной деятельности, сопоставить результаты проверки с ранее данными показаниями. Такое сопоставление позволяет сделать вывод о правдивости или ложности показаний, причастности конкретных лиц к совершенному преступлению, определить их роль в совершении неправомерного доступа к компьютерной информации. Можно также выяснить причины и условия, способствовавшие совершению преступления, и принять эффективные меры по их устранению.

Литература

1. Конвенция о преступности в сфере компьютерной информации ETS № 185: заключена в г. Будапеште 23.11.2001. Доступ из справочной правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собр. законодательства РФ. 1996. № 25, ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Рос. газ. 2001. 22 дек.

4. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ. Доступ из справочной правовой системы «КонсультантПлюс».

5. О полиции: федер. закон от 07.02.2011 № 3-ФЗ // Собр. законодательства РФ. 2011. № 7, ст. 900.

6. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 // Рос. газ. 2013. 13 дек.

7. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации: приказ МВД России от 29.06.2005 № 511 // Рос. газ. 2005. 30 авг.

8. Абравитова Ю.И., Рослякова О.А., Шихов П.И. Расследование преступлений в сфере компьютерной информации и высоких технологий: курс лекций. 2-е изд., перераб. и доп. СПб.: Санкт-Петерб. ун-т МВД России, 2014.

9. Криминалистика: учеб. / ред. О.В. Челышева; сост. А.В. Бачиева и др. СПб.: Санкт-Петерб. ун-т МВД России, 2017.

10. Криминалистика: учеб. для студ. вузов / под ред. А.Ф. Волынского, В.П. Лаврова. 2-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА: Закон и право, 2015.

11. Чижевский В.С. Комментарий к Уголовному кодексу Российской Федерации (постатейный) с практическими разъяснениями официальных органов и постатейными материалами. 2-е изд. М.: Книжный мир, 2017.

12. Михайлов Б.П. и др. Особенности противодействия киберпреступности подразделениями уголовного розыска: учеб.-метод. пособие для студ. вузов, обучающихся по специальности «Юриспруденция» / под ред. Б.П. Михайлова, Е.Н. Хазова. – М.: ЮНИТИ-ДАНА: Закон и право, 2016.

13. Гаврилин Ю.В. и др. Преступления в сфере компьютерной информации: квалификация и доказывание: учеб. пособие. М.: Книжный мир, 2003.

14. Расследование и раскрытие преступлений, совершенных посредством SMS-сообщений: метод. рекомендации / сост. Н.А. Жукова и др. – М.: ДГСК МВД России, 2014.

15. Гаврилин Ю.В., Победкин А.В., Яшин В.Н. Следственные действия: учеб. пособие для вузов. М.: Книжный мир, 2006.

16. Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016.

17. Шаталов А.С. Предварительное расследование: учеб.-метод. пособие. 2-е изд. стереотип. М.: Берлин: Директ-Медиа, 2016.

18. Степанов О.А. и др. Актуальные проблемы противодействия преступлениям в сфере высоких технологий. М.: Академия управления МВД России, 2013.

19. Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: дис. … д-ра юрид. наук. М., 2009.

20. Информационные системы и технологии в профессиональной деятельности сотрудников органов внутренних дел: учеб. пособие / сост. К.М. Бондарь. Хабаровск: Дальневосточный юрид. ин-т МВД России, 2013.

Оглавление

Учебное издание

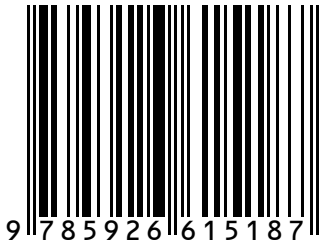
РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Курс лекций

Составитель
Солонникова Нина Валерьевна

Редактор *М. В. Краснобаева*
Компьютерная верстка *С. В. Коноваловой*

ISBN 978-5-9266-1518-7



Подписано в печать 19.11.2019. Формат 60х84 1/16.
Усл. печ. л. 3,3. Тираж 70 экз. Заказ 850.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.