САНКТ-ПЕТЕРБУРГСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

С. П. КУШНИРЕНКО

МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Конспект лекций

Санкт-Петербург
2007

САНКТ-ПЕТЕРБУРГСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

С. П. КУШНИРЕНКО

МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Конспект лекций

Санкт-Петербург
2007

УДК 34
ББК 67.52
Кушниренко, С. П.
Методика расследования преступлений в сфере высоких технологий: конспект лекций / С. П. Кушниренко; СПб юрид. ин-т Генеральной прокуратуры РФ. СПб., 2007. 64 с.

Рецензенты

Г. П. РУСОВА, старший прокурор отдела Управления Генеральной прокуратуры РФ в Северо-Западном федеральном округе.

Э. В. ЛАНТУХ, заместитель начальника кафедры криминалистики СПб университета МВД РФ, кандидат юридических наук, доцент.

В конспекте лекций излагаются следующие основные вопросы: понятие преступления в сфере высоких технологий, криминалистическая характеристика, организация начального этапа расследования, особенности тактики следственных действий и использование специальных знаний при расследовании преступлений данного вида.

Работа предназначена для использования в учебном процессе подготовки и повышения квалификации прокурорско-следственных кадров.

Лекция 1

ПОНЯТИЕ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

План

1. Понятие и классификация преступлений в сфере высоких технологий.

2. Криминалистическая характеристика преступлений в сфере высоких технологий.

1

В соответствии с Доктриной информационной безопасности Российской Федерации национальная безопасность страны существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет неуклонно возрастать. Информационная сфера, представляющая собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений, является системообразующим фактором жизни общества. Она активно влияет на состояние политической, экономической, оборонной, социальной составляющих безопасности общества.

Под *информационной безопасностью* понимается состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Эти интересы заключаются в реализации конституционных прав человека и гражданина на доступ к информации и ее использование для осуществления не запрещенной законом деятельности, в защите личной, корпоративной, государственной информации от неправомерного доступа, в безусловном обеспечении законности и правопорядка, в обеспечении незыблемости конституционного строя, суверенитета и территориальной целостности России, ее политической, экономической и социальной стабильности.

Расширение и развитие информационной сферы закономерно влечет за собой появление технических, социальных и правовых проблем. Среди последних наиболее острой является проблема уголовного преследования за преступления, совершаемые в информационной сфере с использованием так называемых высоких технологий.

Как свидетельствует статистика, в последние годы количество преступлений в сфере компьютерной информации неуклонно увеличивается, возрастает их удельный вес по размерам причиняемого вреда в общей доле моральных и материальных потерь от обычных видов преступлений[1]. О динамике и масштабах этих преступных посягательств наглядно свидетельствуют следующие данные: если в Российской Федерации в 1999 г. было зарегистрировано 294 преступления в сфере компьютерной информации, в 2001 г. — 2066, в 2003 г. — 7540, то в 2005 г. уже 10 214 преступлений[2]. В то же время качество расследования так называемых компьютерных преступлений часто остается низким, что объясняется сложной криминалистической структурой, обуславливающей объективные сложности раскрытия и доказывания; недостаточным уровнем подготовки следователей и оперативных работников, отсутствием научно обоснованных методических рекомендаций по выявлению и расследованию этого вида преступлений.

Понятие *преступление в сфере высоких технологий* для уголовного права и криминалистики сравнительно новое. Впервые такой термин стал употребляться в США, а затем и в других странах с высоко развитыми компьютерными технологиями в 60-х гг. XX в. Первым зарегистрированным преступлением было дело А. Конфессоре, который с применением ЭВМ совершил уклонение от уплаты налогов на сумму $ 620 тыс. в 1969 г.

Термин сложился стихийно для удобства обозначения преступлений, орудием или предметом которых стала компьютерная информация или компьютерные средства. В 80-е годы данные преступления достигли такого распространения, что в национальных правовых системах, а затем и на международном уровне были приняты правовые нормы, вводившие уголовную

---

[1] Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации. М., 2004. С. 6.

[2] www.mvdinform.ru

ответственность за их совершение. Такие деяния получили названия «компьютерные преступления», «киберпреступления», «преступления в сфере высоких технологий», «высокотехнологичные преступления», «преступления в сфере компьютерной информации», «сетевые преступления», «машинно-интеллектуальные, или технико-интеллектуальные преступления», в основном подразумевающие одни и те же виды преступной деятельности. Зарубежными исследователями чаще используются понятия high-tech crime, cyber crime, network crime, которые соответственно и переводятся как «преступления в сфере высоких технологий», «киберпреступления». Исследователь проблемы противодействия таким преступлениям В. В. Крылов рассматривает их как часть информационных преступлений, поскольку они имеют один родовой объект — общественные отношения, связанные с информационными процессами сбора, обработки, накопления, хранения, поиска и распространения информации[3].

Наибольшее распространение в отечественной юридической литературе получил термин *компьютерные преступления*. В уголовном праве сделаны попытки уточнить рассматриваемое понятие в связи с изменившейся обстановкой в обработке и передаче информации. Явно наметились три тенденции в подходах к рассмотрению проблемы[4].

1. Расширительное толкование понятия «компьютерные преступления», в соответствии с которым к таковым относятся: посягательства на связи и отношения людей, опосредующих применение и использование компьютерной техники; вещественный элемент отношений компьютерной безопасности (например, компьютеры, коммутационное оборудование, линии связи); надежность персонала компьютерных систем; жизнь гражданского населения — при использовании «интеллектуальных» систем оружия, влекущих разрушение населенных пунктов, оправданных военной необходимостью; «мир» как состояние человечества — развертывание систем управления стратегическим и ядерным оружием, полностью передающих функции принятия решения компьютерам.

---

[3] Крылов В. В. Расследование преступлений в сфере компьютерной информации // Криминалистика / Под ред. Н. П. Яблокова. М., 2002. С. 615.

[4] Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002. С. 30.

2. Компьютерных преступлений как самостоятельного вида не существует, их следует рассматривать лишь как квалифицирующий признак обычных, «традиционных» преступлений. При этом компьютер при совершении преступления выступает в качестве предмета преступления, орудия преступления, средства, на котором подготавливается преступление, или среды, в которой оно совершается.

3. Компьютерные преступления представляют собой самостоятельный вид преступной деятельности, который может и должен квалифицироваться отдельными составами преступлений.

Внутри приведенных течений также есть различные точки зрения, которые можно условно разделить на три группы. Одни ученые под компьютерными преступлениями понимают противоправные деяния, в которых компьютеры (их системы, сети, компьютерная информация) могут выступать как объектом, так и орудием преступного посягательства[5]. Вторые — ограничивают компьютерные преступления только противоправными деяниями в сфере автоматизированной обработки информации, для которых орудием является компьютер, а в качестве объекта посягательства выступает компьютерная информация[6]. Третьи, по нашему мнению, обоснованно полагают, что в строго юридическом смысле термин «компьютерное преступление» весьма уязвим, предлагают заменить его другим, более удачным — «информационное преступление»[7] в силу того, что объектом преступных посягательств «является не техника, а информация, хранящаяся, передаваемая, обрабатываемая этой техникой»[8].

Компьютерные преступления в России были криминализированы в 1996 г. — в УК РФ были включены ст.ст. 272, 273 и 274, предусматривающие преступления *в сфере компьютерной информации* (неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных

---

[5] Воробьев В. В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. … канд. юрид. наук. Н. Новгород, 2000. С. 62.

[6] См.: Селиванов Н. А. Проблемы борьбы с компьютерной преступностью // Законность. 1993. № 8. С. 37.

[7] См.: Крылов В. В. Расследование преступлений в сфере информации. М., 1998. С. 154—169.

[8] Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 1995. С. 81.

программ для ЭВМ и нарушение правил эксплуатации ЭВМ, их систем и сетей). Однако при внедрении высоких технологий практически во все сферы жизни и хозяйства неправомерный доступ к охраняемой законом компьютерной информации перестал быть самоцелью правонарушителей. Компьютерные технологии все чаще становятся не только орудием, но также способом и средством совершения так называемых традиционных преступлений: хищений путем растраты и присвоения, мошенничества, изготовления фальшивых денег и документов, поддельных пластиковых кредитных и расчетных карт, акцизных марок, изготовления и распространения порнографических изображений, контрафактной продукции, хулиганства и многих других.

При широком распространении возможностей глобальных сетей компьютерные преступления стали транснациональными, т. е. не имеющими национальных, административных или ведомственных границ. Использование Интернета является широко применимым способом совершения хищений чужого имущества, распространения порнографии, ложных сообщений об актах терроризма, вымогательства под угрозой блокирования или уничтожения баз данных, принадлежащих крупным корпорациям и общественным организациям, распространения компрометирующих материалов в отношении физических и юридических лиц.

Разнообразие преступлений, совершаемых в отношении электронной цифровой информации и посредством ее использования, равно как и средств компьютерной и иной вычислительной техники, потребовало обобщения криминалистических знаний с целью выработки приемов, методов и средств выявления, расследования и превенции преступлений такого рода. Без преувеличения можно сказать, что преступления, объединенные общностью способов подготовки, совершения и сокрытия, осуществляемых преступниками определенного типа, имеющие специфику места и времени совершения, обусловленные схожей обстановкой, уже выделились в определенную группу. Это обстоятельство поставило перед криминалистами новые задачи определения понятия преступлений в сфере высоких технологий, их криминалистической классификации и рамок данной группы.

На современном этапе важно *классифицировать* рассматриваемые преступления для решения практических задач. Предла-

гаются несколько классификаций по различным основаниям. Например, по последствиям, наступившим в результате совершения деяния и связанным с возможными формами уязвимости компьютерной информации, такими как подверженность физическому уничтожению, возможность несанкционированной модификации, опасность несанкционированного получения информации лицами, для которых она не предназначалась. При этом выделяются три группы последствий: 1) искажение (неправомочная модификация) данных; 2) утечка информации; 3) отказ в обслуживании (нарушение доступа к сетевым услугам)[9]. Соответственно, наносится ущерб целостности, конфиденциальности и доступности информации[10].

Другая классификация включает в себя четыре основных вида преступлений: 1) манипуляции с информационной техникой; 2) незаконное использование машинного времени; 3) кража программ; 4) компьютерный саботаж[11].

В литературе предлагается и ряд других классификаций[12], существенно различающихся по составу рассматриваемых деяний.

В инструктивных материалах Интерпола «цифровые преступления» делятся на три группы: 1) собственно компьютерные преступления (нарушение авторских прав на программное обеспечение, хищение данных, нарушение работы вычислительных систем, хищение компьютерного времени и т. д.); 2) преступления, «связанные с компьютерами» (в основном финансовое мошенничество); 3) сетевая преступность (использование сетей для совершения незаконных сделок — распространение порнографии, торговля наркотиками, уклонение от таможенных пошлин, отмывание денег и т. д.)[13].

В настоящее время особый интерес и практическую значимость представляет классификация, содержащаяся в Конвенции

---

[9] Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях. Международный опыт. М., 2004. С. 64.

[10] См.: Методологические основы обеспечения информационной безопасности объекта // Защита информации: Конфидент. 2000. № 1. С. 75.

[11] Черкасов В. Н. Указ. соч. С. 34.

[12] Батурин Ю.М. Проблемы компьютерного права. М., 1991. С. 138—159; Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия. М., 1996. С. 55—104; Крылов В. В. Расследование преступлений в сфере информации. С. 165—169. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М., 2002. С. 129—143.

[13] Осипенко А. Л. Указ. соч. С. 64.

Совета Европы по борьбе с киберпреступностью 2001 г. (ETC № 185), поскольку уже принято Распоряжение Президента РФ от 15 ноября 2005 г. № 557-рп о ее подписании. Ратификация Россией данной Конвенции потребует корреляции отечественного законодательства с международными нормами. Конвенционные правонарушения подразделяются на четыре вида: 1) преступления против конфиденциальности, целостности и работоспособности компьютерных данных и систем — незаконный доступ, незаконный перехват, создание помех для обмена данными, создание помех для функционирования систем, неправомерное использование аппаратных устройств; 2) компьютерные преступления — фальсификация и подлог, совершаемые с использованием компьютерной техники; 3) преступления, связанные с сетевым контентом — изготовление, распространение и хранение детской порнографии; 4) правонарушения, связанные с нарушением авторского права и смежных прав. Как известно, почти все из перечисленных форм девиантного поведения криминализированы в российском уголовном праве.

Представленные виды преступлений в сфере высоких технологий уже восприняты российской криминалистической наукой и послужили основанием для выдвижения новых классификаций, имеющих научное и практическое значение. В частности, *с учетом отечественного законодательства предлагается выделять*:

а) преступления, направленные непосредственно на нарушение нормального функционирования глобальных сетей и подключенных к ним компьютеров;

б) «традиционные» преступления, при совершении которых компьютерные или телекоммуникационные системы используются в качестве необходимых технических средств[14].

Мы разделяем такую точку зрения, не умаляя значения и обоснованности иных мнений по данному вопросу. Представляется, что только дальнейшая разработка и обобщение практики раскрытия и расследования преступлений в сфере высоких технологий приведет, наконец, к принятию более адекватного современным условиям уголовного законодательства в стране.

[14] Там же. С. 67— 68.

Криминалистическая структура преступлений в сфере высоких технологий включает следующие элементы:

предмет посягательства;

орудие посягательства;

физическая деятельность субъекта;

вредные последствия;

место и время совершения преступления;

субъект преступления;

психическая деятельность субъекта.

Основным предметом посягательства является компьютерная информация, определяемая как документированные[15] сведения о лицах, предметах, фактах, событиях, явлениях и процессах, хранящиеся на машинных носителях, в ЭВМ, системе или сети ЭВМ, либо управляющие ЭВМ.

ЭВМ называется комплекс электронных устройств, позволяющий осуществлять предписанные программой (или пользователем) информационные процессы: сбор, обработку, накопление, хранение, поиск и распространение информации. Понимая под системой любой объект, элементы которого находятся в упорядоченной взаимосвязи, систему ЭВМ можно определить как комплекс, в котором хотя бы одна ЭВМ является элементом системы, либо несколько ЭВМ составляют систему. Целью системы является повышение эффективности работы ЭВМ. Сетью ЭВМ являются компьютеры, объединенные между собой линиями (сетями) электросвязи, т. е. технологическими системами, обеспечивающими один или несколько видов передач (телефонную, телеграфную, факсимильную передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания)[16]. К машинным носителям компьютерной информации относятся устройства памяти ЭВМ, периферийные устройства связи, сетевые устройства и сети электросвязи. На материальных носителях информация находится непосредственно в файлах, которые имеют стандартные свойства: тип инфор-

---

[15] В соответствии со ст. 2 Федерального закона «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ документированной информацией (документом) являются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные на материальном носителе с реквизитами, позволяющими ее идентифицировать.

[16] Статья 2 Федерального закона «О связи» от 16 февраля 1995 г. № 15-ФЗ.

мации (текст, графика, программный код, числа и пр.), местонахождение информации на физическом носителе, имя, объем информации, время создания и изменения, атрибуты информации (архивная, скрытая, только для чтения и пр.). При передаче файлов и сообщений (информации) в других формах (в виде сигналов) по системам, например, электросвязи, они не теряют своих индивидуальных свойств. Именно поэтому в числе носителей сведений, составляющих государственную тайну, указаны и физические поля, в которых сведения находят свое отображение в виде символов, образов, сигналов, технических решений и процессов[17].

Компьютерная информация может быть массовой, если она предназначена для неограниченного круга лиц, или конфиденциальной, если принадлежит определенному собственнику или ее распространение и доступ к ней ограничены специальной нормой права, например персональные данные о субъектах, государственная, коммерческая, врачебная тайна и т. п. Доступ к такой информации ограничен и требует специального допуска. В противном случае доступ к такой информации является неправомерным.

Орудием совершения компьютерного преступления могут являться как компьютерные средства и оборудование, так и программное обеспечение, с помощью которого преступники осуществляют неправомерный доступ к охраняемой компьютерной информации.

Не всякий неправомерный доступ образует состав преступления, а лишь такой, при котором наступили вредные последствия для правообладателя информации, затруднившие или сделавшие невозможным для потерпевшего использование информации: уничтожение, блокирование, модификацию или копирование информации.

Уничтожение информации — полная физическая ликвидация информации или таких ее элементов, которые влияют на изменение существенных идентифицирующих информацию признаков. Признаком уничтожения является прекращение существования при условии, что информация не может быть восста-

[17] Крылов В. В. Расследование преступлений в сфере компьютерной информации. С. 617.

новлена и использована по назначению в том виде, в каком она существовала у правообладателя. Уничтожение может осуществляться субъектами, имеющими доступ к этой информации, или в результате программно-технических причин, связанных с нарушением эксплуатации или использованием некачественных технических средств вопреки установленным правилам и инструкциям.

Блокирование — искусственное затруднение доступа пользователей к компьютерной информации, не связанный с ее уничтожением. Оно влечет временную или постоянную невозможность осуществлять какие-либо операции с компьютерной информацией.

Модификация информации означает любые ее изменения вопреки желанию и интересам собственника или правообладателя, порождает отличие информации от той, которую включил в систему и которой владеет правообладатель или собственник. Не является модификацией адаптация программы для ЭВМ или базы данных, т. е. такое изменение, которое осуществляется исключительно в целях обеспечения их функционирования на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Копирование информации — воспроизведение ее в любой материальной форме без явно выраженного согласия собственника или правообладателя.

Нарушение работы ЭВМ, системы ЭВМ или их сети означает создание правонарушителем любой нестандартной (нештатной) ситуации с ЭВМ или ее устройствами, повлекшие уничтожение, блокирование, модификацию или копирование информации.

Физическая деятельность субъектов преступления проявляется в осуществлении ими подготовки, совершения и сокрытия преступления. Непосредственное совершение преступления определяется способом преступной деятельности. Для компьютерных преступлений это:

неправомерный доступ к компьютерной информации, направленный на нарушение конфиденциальности информации — получение возможности знакомиться и осуществлять операции с чужой информацией, находящейся в ЭВМ, системах ЭВМ и их сетях, а также на машинных носителях;

создание, использование и распространение вредоносных программ, приводящих к нарушению целостности или направленных на нарушение конфиденциальности информации;

нарушение порядка использования компьютерно-технических средств, повлекшее нарушение целостности и конфиденциальности информации.

Наиболее распространенными объектами преступного посягательства при *неправомерном доступе к компьютерной информации и базам данных* (ст. 272 УК РФ) являются коммерческие организации, в том числе кредитно-финансовые, государственные учреждения, правоохранительные органы, а также частные лица. Две трети преступлений связаны с незаконным проникновением с использованием удаленного доступа. Почти треть проникновений осуществляется внутри потерпевших организаций — лицами, использующими для этого свое служебное положение, т. е. возможности правомерного доступа к ЭВМ, их системе или компьютерной сети кредитно-финансового или иного учреждения, предприятия, организации в силу выполняемой работы или занимаемой должности. Следует иметь в виду, что правомерный доступ к компьютерному оборудованию не означает правомерности доступа к компьютерной информации, которая предназначается для определенных лиц и выполнения ими соответствующих функций.

Субъекты совершают преступления путем:

модификации компьютерных программ с целью проводки подложных электронных документов для создания резерва денежных средств с их последующим перечислением на счета юридических и физических лиц, обналичиванием и изъятием;

изменения программ по начислению заработной платы и зачисления ее на лицевые счета сотрудников с автоматическим списанием части наличных сумм на свой счет и на счета соучастников;

произведения незаконных начислений денежных выплат с последующим их хищением путем подделки подписи получателей в оформленных платежных документах;

создания файлов с вымышленными вкладчиками, зачисления и проводки по их счетам фиктивных денежных сумм с последующим переводом на свой счет и их хищением;

получения в базах данных кредитно-финансовых учреждений номеров банковских карт и ПИН-кодов с последующим использованием в расчетах денежных средств клиентов банка;

искажения реквизитов электронных платежных документов, касающихся адреса получателя денег, с переводом их на свой счет или счета соучастников;

занижения суммы выручки торговых предприятий путем введения специальных вредоносных программ в контрольно-кассовые аппараты, являющиеся ЭВМ, для совершения налоговых преступлений и хищений;

внесения ложных сведений в электронные базы данных, управляющие учетом, для завышения расхода топлива, сырья, материалов и сокрытия недостачи, образовавшейся в результате хищения;

другими способами.

Основными средствами неправомерного доступа и преодоления информационной защиты являются: хищение ключей и паролей, использование несовершенства защиты информации, использование визуальных, оптических и акустических средств наблюдения за ЭВМ, использование недостатков программного обеспечения, операционных систем, несанкционированное подключение к основной и вспомогательной аппаратуре ЭВМ, внешним запоминающим устройствам, периферийным устройствам, линиям связи и пр. В основном для совершения преступления используются программные (55% случаев) либо комбинированные (программные и технические носители) средства.

Физическая деятельность субъектов при *создании, использовании и распространении вредоносных программ для ЭВМ* (ст. 273 УК РФ) заключается в постановке задачи, определении цели программы, в выборе средств и языка реализации программы, написании текста программы, ее отладке и запуске, а также в ее использовании, т. е. в создании вредоносной программы. Вредоносной является любая программа, специально разработанная или модифицированная для несанкционированного собственником информационной системы уничтожения, блокирования, модификации либо копирования информации, нарушения обычной работы ЭВМ[18]. Создание программ может производиться непо-

[18] Крылов В. В. Информационные компьютерные преступления. М., 1997. С. 42.

средственно на ЭВМ в подвергшейся воздействию компьютерной системе, а также в любом другом месте, где субъект имеет доступ к персональному компьютеру и обладает необходимыми для разработки программы оборудованием, временем и средствами. Наказуемо и использование такой программы, которое заключается в применении разработанной, в том числе и иным лицом, вредоносной программы при эксплуатации ЭВМ и обработке информации. Способом совершения преступления является и распространение вредоносных программ, которое выражается в предоставлении доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных. Оно может осуществляться путем перезаписи на магнитные и иные носители и продажи с рук или через торговые предприятия, сдачи в прокат, взаймы, путем обмена, дарения и т.п. Распространение может осуществляться и сетевыми способами. Характерным является то, что все эти действия могут выполняться одним лицом или разными, как действующими в группе по предварительному сговору, так и индивидуально.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ) совершается путем выполнения действий или бездействия, нарушающих порядок их использования, установленный инструкциями по эксплуатации компьютерного оборудования. Выделяют активный и пассивный способ совершения этого преступления[19]. Правила эксплуатации устанавливаются разработчиками оборудования, а также собственником и владельцем информационных ресурсов. Их нарушение в равной мере недопустимо, если это повлекло вредные последствия в виде уничтожения, блокирования или модификации компьютерной информации. Ответственность за такую деятельность предусматривается только для лиц, имеющих официальный доступ к ЭВМ, их системе или сети.

Для всех преступлений в сфере высоких технологий характерно то, что *место и время* совершения противоправных действий не совпадают с местом и временем неправомерного доступа к информации и наступления вредных последствий. Это означает, что действия, совершаемые в одной местности, могут по-

[19] Скоромников К. С. Расследование компьютерных преступлений // Пособие для следователя. Расследование преступлений повышенной общественной опасности / Под ред. Н. А. Селиванова, А. И. Дворкина. М., 1998. С. 382.

влечь доступ к информации в нескольких других местах, значительно удаленных, а вредные последствия могут наступить в третьем, еще более удаленном от первых двух. Наиболее ярким примером этого могут являться хищения путем незаконного электронного перевода денежных средств со счетов граждан путем использования номеров их банковских счетов с обналичиванием денег через подставных лиц в иной местности. Выявление компьютерных преступлений не всегда означает автоматическое выяснение места его совершения. Между выявлением и поимкой преступника могут существовать барьеры в виде национальных границ между государствами с разными правовыми системами, в которых по-разному определяется понятие компьютерного преступления, и тогда возмездие за содеянное может не наступить.

Субъекты рассматриваемых преступлений весьма специфичны. Способ совершения посягательства, как правило, отражает черты и мотивы преступников. Следственная практика показывает, чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть, тем легче выделить подозреваемого, поскольку круг специалистов, обладающих соответствующими способностями, обычно весьма ограничен.

Анализ уголовных дел свидетельствует о том, что 2/3 киберпреступников имеют высшее или незаконченное высшее техническое образование, 80% из них занимают административные и бухгалтерские должности либо относятся к инженерно-техническому персоналу, каждый третий по роду службы правомерно пользовался служебной компьютерной техникой и постоянно имел свободный доступ к ней. Наряду с этим распространены случаи совершения компьютерных преступлений несовершеннолетними. Например, в Москве был задержан 17-летний учащийся одной из школ, который в домашних условиях создавал и через компьютерные сети распространял опаснейшие вредоносные программы, предназначавшиеся для несанкционированного уничтожения информации и нарушения работы ЭВМ. 78% совершивших компьютерные преступления — мужчины. Все шире распространяется совершение компьютерных преступлений группами, в том числе и организованными. Среди зарегистрированных проявлений — каждое третье преступление совершено организованной преступной группой с распределением ролей и соответствующей подготовкой. Уже зарегистрированы случаи

использования «компьютерных взломщиков» организованными группами, совершающими тяжкие преступления, в том числе финансовые, а также террористическими организациями.

Среди преступников выделяются три основные группы:

лица, владеющие специальными навыками в области управления ЭВМ и ее устройствами, а также специальными познаниями в области обработки информации в информационных системах в целом, знающие финансовые, бухгалтерские, информационные технологии. Ими совершаются хорошо продуманные и тщательно подготовленные преступления, в основном корыстные;

лица, не обладающие серьезными познаниями в области программирования и компьютерной техники, имеющие лишь некоторые пользовательские навыки работы с ЭВМ. Их действия направлены на уничтожение, блокирование, модификацию, копирование ничем не защищенной информации;

лица, имеющие психические отклонения. К их числу относят страдающих различными компьютерными фобиями. Эта категория заболеваний связана с нарушениями в информационном режиме человека под воздействием внешних или внутренних дестабилизирующих факторов как врожденного, так и приобретенного свойства[20].

Как показывают эмпирические исследования, многообразны мотивы *совершения компьютерных преступлений. Среди них корысть, познавательский интерес, хулиганские побуждения, месть, коммерческий шпионаж и другие*[21].

Корыстные цели преследуются преступниками в 55,7% случаев. Среди них преобладают деяния, связанные с распространением вредоносных программ (18,6% изученных случаев). Реже компьютерные преступления совершаются в целях получения безвозмездного программного обеспечения (7,1%) либо последующей продажи похищенного программного обеспечения или иной информации (5,7%). Корыстным мотивом движимы преступники, совершающие преступления в сфере экономической

---

[20] Криминалистика: Учебник / Под ред. Р. С. Белкина. М.,1999. С. 950—951.

[21] См.: Головин А. Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации // http://www.crime-research.org

деятельности — мошенничество, присвоение и растрату, причинение имущественного ущерба путем обмана или злоупотребления доверием, незаконное получение и разглашение сведений, составляющих коммерческую налоговую или банковскую тайну, и др.

Познавательный интерес преобладает у молодых людей, осуществляющих неправомерный доступ к компьютерной информации различных правообладателей: физических лиц, коммерческих структур, государственных учреждений и ведомств. Чем более защищена информация ведомства, тем настойчивее осуществляются хакерские атаки, в том числе по предварительному сговору группами преступников, объединяющихся путем общения через глобальную сеть, иногда даже из разных стран.

Мотивами мести руководствуются 12,9% преступников. Чаще всего пытаются отомстить за недооценку их личности и профессионализма или за необоснованное увольнение с работы.

Например, подлежащая увольнению по сокращению штатов из городского управления жилищно-коммунальных услуг г. Курчатова Г., недовольная этим фактом, решила осложнить работу подразделений городской администрации. Используя свое служебное положение, Г., занимавшая должность инженера-программиста, под разными предлогами получила доступ к ЭВМ пяти ЖЭУ города и уничтожила программу «Квартплата»[22].

Коммерческий шпионаж осуществляется по 10% уголовных дел.

Например, в торговых точках Санкт-Петербурга в 1997 г. распространялась база данных абонентов компании сотовой связи «Дельта-Телеком». Эти данные носили характер коммерческой тайны, в официальных источниках не публиковались и были похищены с электронных носителей информации компании. В результате распространения подобных сведений ряд клиентов компании были вынуждены отказаться от услуг фирмы, так как были нарушены условия конфиденциальности информации. Кроме того, в некоторых городских газетах были опубликованы статьи об утечке сведений об абонентах мобильных телефонов, что существенно подорвало престиж компании.

---

[22] Уголовное дело № 37298. Архив Курчатовского городского суда Курской области.

Вопросы для самоконтроля

1. Раскройте понятие «преступления в сфере высоких технологий».

2. Какие криминалистические классификации преступлений в сфере высоких технологий существуют в научной литературе?

3. Каким образом классифицированы преступления в сфере высоких технологий в Конвенции Совета Европы о киберпреступности?

4. Перечислите элементы криминалистической структуры преступлений в сфере высоких технологий.

5. Дайте криминалистическую характеристику предмета посягательства, субъектов преступления, их физической и психической деятельности, орудий, места и времени совершения преступления.

Лекция 2

Организация начального этапа расследования

План

1. Обстоятельства, подлежащие установлению и доказыванию.

2. Особенности возбуждения уголовного дела.

3. Типичные следственные ситуации и организация начального этапа расследования.

1

Наиболее существенными обстоятельствами, подлежащими установлению и доказыванию *по делам о преступлениях в сфере компьютерной информации, определяющими специфику видов данных деяний, являются следующие.*

По делам о неправомерном доступе к компьютерной информации *установлению и доказыванию подлежат следующие обстоятельства:*

1. Факт доступа к компьютерной информации.

2. Неправомерность доступа к компьютерной информации. Устанавливается правообладатель информации, использование им средств защиты, конфиденциальность информации.

3. Место неправомерного доступа к компьютерной информации — местонахождение информации, подвергшейся «нападению», и место, откуда осуществлялась компьютерная «атака».

4. Время неправомерного доступа и время наступления вредных последствий.

5. Орудия преступления — компьютерные и телекоммуникационные средства, а также программное обеспечение, которые использовались субъектом для неправомерного доступа.

6. Способ совершения неправомерного доступа.

7. Вредные последствия неправомерного доступа, их оценка правообладателем компьютерной информации, характер и размер вреда.

8. Субъект неправомерного доступа, его служебное положение, наличие доступа к ЭВМ, системе ЭВМ или их сети, наличие преступной группы, наличие организованной преступной группы, распределение ролей между ее участниками.

9. Виновность каждого субъекта преступления, форма вины, мотив преступной деятельности.

10. Обстоятельства, характеризующие личность каждого субъекта.

11. Обстоятельства, исключающие преступность и наказуемость деяния.

12. Обстоятельства, смягчающие и отягчающие наказание, предусмотренные ст.ст. 61, 63 УК РФ.

13. Обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания.

14. Причины и условия, способствовавшие совершению преступления. Характеристика обстановки совершения преступ-

ления.

При расследовании *создания, использования и распространение вредоносных программ для ЭВМ* устанавливаются и доказываются такие обстоятельства:

1. Факт и способ создания вредоносной программы для ЭВМ или факт внесения в существующую программу изменений, приводящих к уничтожению, модификации или блокированию информации.

2. Факт использования или распространения вредоносной программы или машинных носителей с такой программой.

3. Вредные последствия, причиненные преступлением, их оценка правообладателем компьютерной информации, характер и размер вреда, наступление тяжких последствий.

4. Физические или(и) юридические лица, потерпевшие от преступления.

5. Место совершения преступления — место создания, использования, распространения вредоносных программ, место наступления вредных последствий содеянного.

6. Время создания, использования, распространения вредоносных программ, время наступления вредных последствий.

7. Орудия преступления — компьютерные и телекоммуникационные средства, а также программное обеспечение, которые использовались субъектом для создания, использования и распространения вредоносных программ.

8. Субъект преступления, наличие преступной группы, распределение ролей между ее участниками.

9. Виновность каждого субъекта преступления, форма вины, мотив преступной деятельности.

10. Обстоятельства, характеризующие личность каждого субъекта.

11. Обстоятельства, исключающие преступность и наказуемость деяния.

12. Обстоятельства, смягчающие и отягчающие наказание, предусмотренные ст.ст. 61, 63 УК РФ.

13. Обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания.

14. Причины и условия, способствовавшие совершению преступления.

15. Характеристика обстановки совершения преступления.

Расследование *нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети* предполагает установление и доказывание следующих обстоятельств:

1. Факт нарушения определенных правил эксплуатации ЭВМ, системы ЭВМ или их сети, способ действия субъекта преступления.

2. Наступление вредных последствий в виде уничтожения, блокирования или модификации охраняемой законом компьютерной информации. Характер компьютерной информации, подвергшейся воздействию. Существенность причиненного вреда собственнику или правообладателю информации. Наступление тяжких последствий.

3. Субъект нарушения правил эксплуатации, его служебное положение, наличие доступа к ЭВМ, системе ЭВМ или их сети, наличие преступной группы, распределение ролей между ее участниками.

4. Виновность каждого субъекта преступления, форма вины, мотив преступной деятельности.

5. Обстоятельства, характеризующие личность каждого субъекта.

6. Место нарушения правил эксплуатации.

7. Время нарушения правил эксплуатации.

8. Обстоятельства, исключающие преступность и наказуемость деяния.

9. Обстоятельства, смягчающие и отягчающие наказание, предусмотренные ст.ст. 61, 63 УК РФ.

10. Обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания.

11. Причины и условия, способствовавшие совершению пре-

ступления.

12. Характеристика обстановки совершения преступления.

2

Поводами *для возбуждения уголовных дел о преступлениях в сфере компьютерной информации являются:*

заявления граждан и организаций, являющихся владельцами и законными пользователями компьютерной информации, подвергшейся преступному воздействию. Заявления должны быть оформлены и зарегистрированы в соответствии с требованиями ст. 140 УПК РФ;

сообщения о совершенном или готовящемся преступлении, полученные из различных источников. Уполномоченное лицо, получившее такое сообщение, составляет рапорт об обнаружении признаков компьютерного преступления в соответствии с требованиями ст. 143 УПК РФ. В основном такими источниками являются данные, полученные в результате проведения оперативно-розыскных мероприятий специализированными подразделениями ФСБ и МВД[23];

теоретически возможна явка с повинной лица, совершившего преступление в сфере компьютерной информации, хотя в следственной практике такие случаи почти не встречаются.

Решение вопроса о возбуждении уголовного дела требует тщательной проверки и оценки имеющихся данных в соответствии со ст. 144 УПК РФ. Исключение составляют случаи задержания правонарушителей с поличным. Тогда уголовное дело должно быть возбуждено немедленно для производства неотложных следственных действий и иных мероприятий, к которым относятся задержание с поличным, личный обыск подозреваемого, осмотр места происшествия, обыск по месту возможного пребывания подозреваемого, где находится используемый им персональный компьютер, изъятие компьютерной техники и информации, имеющей значение для дела.

---

[23] В частности, для выявления преступлений в сфере так называемых высоких технологий и для установления лиц и преступных группировок, занимающихся преступной деятельностью в этой области, создано Управление «К» МВД России.

В ходе предварительной проверки *должны найти подтверждение следующие факты:*

нарушение целостности (конфиденциальности) информации в ЭВМ, системе или сети ЭВМ;

наступление вредных последствий в виде копирования, уничтожения, модификации, блокирования информации, нарушения работы ЭВМ, за исключением дел о создании, использовании и распространении вредоносных программ для ЭВМ;

наличие причинной связи между неправомерными действиями и наступившими последствиями;

крупный размер ущерба или существенность вреда, причиненного в результате преступных действий.

В процессе проверки заявления или сообщения о совершенном компьютерном преступлении необходимо принять меры к установлению таких необходимых для возбуждения уголовного дела данных, как:

время неправомерного проникновения в компьютерные сети (изнутри потерпевшей организации или извне) и доступа к компьютерной информации;

место нахождения информации, на которую была «совершена атака»;

время и место создания, использования и распространения вредоносных программ для ЭВМ;

способы совершения неправомерного доступа или нарушения правил эксплуатации ЭВМ и их последствия;

технические, программные, комбинированные или иные средства, использованные при совершении преступления;

способы преодоления информационной защиты информации у ее правообладателя;

субъект преступления.

В зависимости от ситуации на стадии проверки заявления могут быть проведены различные мероприятия и такое неотложное следственное действие, как осмотр места происшест-

вия. Их цель не только выявить криминалистические признаки совершенного преступления, но и зафиксировать и изъять следы преступления, определить круг свидетелей, подлежащих допросу.

К моменту возбуждения уголовного дела материал проверки заявления содержит следующие документы*:*

заявление или сообщение о совершенном или готовящемся компьютерном преступлении;

рапорт уполномоченного лица об обнаружении признаков преступления;

объяснения заявителя и других лиц, которым известно о совершенном или готовящемся компьютерном преступлении;

правила эксплуатации ЭВМ, системы ЭВМ, сети ЭВМ, инструкции по работе с компьютерными средствами, журналы регистрации сбоев, справки о произошедшем неправомерном доступе в организации и другие документы, относящиеся к совершению компьютерного преступления, его последствиям или субъекту правонарушения;

документы, подтверждающие распространение вредоносных программ через торговые предприятия: приходные накладные, кассовые чеки, инвентаризационные описи, товарно-денежные отчеты и др.;

материалы органов, осуществлявших оперативно-розыскную деятельность по рассматриваемому факту: протоколы проверочных закупок носителей с вредоносными программами, оперативного наблюдения, перехвата и регистрации информации электронной почты, оперативных экспериментов и других оперативно-розыскных мероприятий, проводимых по данному факту; стенограммы прослушивания телефонных переговоров и иных сообщений (радиообмена, пейджинговых, модемных), перехвата информации с иных каналов связи, свидетельствующие о неправомерной деятельности подозреваемых лиц, и др.;

постановление начальника органа, осуществляющего ОРД, о рассекречивании полученной информации;

постановление начальника органа, осуществляющего ОРД, о

представлении результатов ОРД органу дознания, следователю или прокурору[24].

3

Организация начального этапа расследования зависит от того, какая *следственная ситуация* сложилась к моменту возбуждения уголовного дела. Под следственной ситуацией понимается объективная криминалистическая категория, отражающая положение в определенный момент расследования, характеризующаяся содержанием криминалистически значимой информации и степенью достаточности ее для принятия решений следователем или прокурором. Поэтому на начальном этапе расследования организация сводится в основном к работе с информацией — к ее восприятию, анализу, переработке, оценке, систематизации, синтезу. На основе результатов обработки исходной информации выдвигаются версии, определяются задачи расследования, следователь принимает решения, организует их выполнение и осуществляет контроль за исполнением всеми участниками процесса. В результате он получает новую информацию, которая, в свою очередь, воспринимается, анализируется, перерабатывается, синтезируется, что ведет к постановке новых задач и принятию новых управленческих решений и корректировке прежних. Постоянно по ходу этого процесса следователь прогнозирует расследование в целом, поведение подозреваемого, обвиняемого, заявителя о компьютерном преступлении, свидетелей, других участников расследования, а также возможное недобросовестное противодействие со стороны защиты.

Организация расследования осуществляется с использованием программно-целевого метода, метода мысленного моде-

---

[24] Порядок представления результатов ОРД органу дознания, следователю, прокурору, суду регламентирован Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд, утвержденной совместным Приказом ФСНП РФ, ФСБ РФ, МВД РФ, ФСО РФ, ФПС РФ, ГТК РФ, СВР РФ от 13 мая 1998 г. № 175/226/336/201/286/410/56.

лирования, криминалистического факторного анализа и комплексного подхода[25].

Для начального этапа расследования компьютерных преступлений наиболее типичны следующие ситуации:

собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления и обнаружил лицо, его совершившее;

собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления, но преступник не известен;

преступление выявлено органом дознания в результате проведенной оперативно-розыскной деятельности.

Анализ исходной информации, независимо от ситуации, осуществляется на основе обобщения имеющихся в материале сведений о криминалистических признаках*, указывающих на совершение компьютерного преступления. Это могут быть следующие признаки:*

сбои в работе ЭВМ, системе ЭВМ или локальной вычислительной сети собственника или правообладателя;

уничтожение, блокирование, модификация или копирование компьютерной конфиденциальной информации;

утрата значительных массивов информации или баз данных;

необычные проявления в работе ЭВМ: замедленная или необычная загрузка операционной системы, замедление работы машины с внешними устройствами, неадекватные реакции ЭВМ на команды пользователя и пр.;

копии чужих файлов в файловой системе правообладателя;

файлы с вредоносными программами;

наличие программного обеспечения подбора паролей для неправомерного доступа в Интернет либо иного проникновения в

---

[25] Густов Г. А. Проблемы методов научного познания в организации расследования преступлений: Автореф. дис. … д-ра юрид. наук. М., 1993. С. 28—52.

компьютерные сети, а также содержащего функции по уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

внесение в конструкцию компьютера встроенных устройств, дополнительных жестких дисков, устройств для расширения оперативной памяти, считывания оптических дисков и т. д.;

наличие нестандартных периферийных устройств;

изменения в оперативном запоминающем устройстве, зафиксированные при задержании подозреваемого с поличным в момент работы на компьютере при совершении неправомерного доступа к компьютерной информации;

улики поведения подозреваемого;

другие признаки.

Анализируя указанные признаки, следователь выдвигает общие и частные типовые версии.

Основными из них являются следующие:

имело место компьютерное преступление, правообладатель правильно отразил в заявлении его обстоятельства;

совершено иное преступление, сбой компьютерного оборудования применен для запутывания следов преступления;

имеет место оговор или ложное заявление о преступлении с целью отвести подозрение от себя или избавиться от нежелательного лица;

имеет место заблуждение или ошибка заявителя.

Одновременно выдвигаются типовые частные версии по каждому из обстоятельств, подлежащих доказыванию, в зависимости от того, какие из них не установлены к данному моменту. После этого в результате сопоставления обстоятельств, подлежащих установлению и уже установленных, формулируются задачи расследования и определяются средства их решения, т. е. те следственные действия и иные мероприятия, в результате проведения которых предполагается установить не известные еще обстоятельства совершения преступления. Таким образом формируется план расследования по делу в целом, отдельным эпизодам и обстоятельствам. По мере его выполнения и получе-

ния новой информации вносятся коррективы в имеющийся план, и вновь проводится анализ и формулирование дальнейших задач расследования.

Наиболее важными следственными действиями на начальном этапе расследования компьютерных преступлений являются осмотр места происшествия, компьютерного оборудования и информации, обыск и выемка с целью обнаружения, фиксации и изъятия компьютерной информации и компьютерных средств, относящихся к расследуемому событию. Это ключевой момент расследования, поскольку компьютерная информация является предметом посягательства, неправомерный доступ к ней должен быть своевременно процессуально зафиксирован. Тем более что компьютерная информация может быть легко изменена или уничтожена, что повлечет утрату следов преступления.

Вопросы для самоконтроля

1. Перечислите обстоятельства, подлежащие установлению и доказыванию по делам о неправомерном доступе к компьютерной информации.

2. Каковы поводы и основания возбуждения уголовных дел о преступлениях, совершаемых в сфере высоких технологий?

3. Какие факты проверяются в ходе предварительной проверки?

4. Какие типичные следственные ситуации характерны для начального этапа расследования рассматриваемых преступлений?

Лекция 3

Тактика производства отдельных следственных действий

План

1. Тактические особенности подготовки к изъятию компьютерной информации.

2. Тактика осмотра и обыска места происшествия.

3. Тактика выемки.

4. Тактика допроса.

1

Если у следствия есть основания полагать, что цифровая информация может являться доказательством по уголовному делу, то она *должна изыматься только процессуальными способами,* предусмотренными законом: в процессе производства осмотра, обыска, выемки. Выбор конкретного следственного действия зависит от решения следователя, которое, как правило, обусловлено конкретной ситуацией расследования на момент необходимости изъятия цифровой информации. В бесконфликтной ситуации с собственником или владельцем цифровой информации, когда гражданин или организация потерпели от правонарушения и готовы оказать помощь в установлении истины, целесообразно проводить выемку или осмотр. Такая ситуация чаще всего складывается с организациями, подвергшимися неправомерному доступу к компьютерной информации.

В конфликтной ситуации, особенно при расследовании преступлений в сфере экономики, целесообразно проводить обыск, поскольку гражданин и организация могут оказывать явное или скрытое противодействие, вплоть до преграждения доступа и уничтожения информации и ее носителей.

Задачи подготовительной стадии:

получить наиболее полное представление о характере деятельности объекта, где могут находиться следы преступле-

ния и другие объекты, относящиеся к расследуемому делу, изучить обстановку в организации: отрасль хозяйствования, порядок учета, документооборот, структуру, особенности используемых технологий;

изучить коммуникативные и иные тактико-технические характеристики используемой компьютерной техники и программного обеспечения;

изучить организацию охраны объекта информатизации и конкретной компьютерной информации;

выяснить служебные обязанности лиц, имеющих санкционированный доступ к охраняемой законом компьютерной информации, а также их прямое или косвенное отношение к ценностям (имуществу), которые стали предметом правонарушения.

Для полного, объективного и всестороннего исследования всех обстоятельств совершения преступления следует получить ответы на целый ряд вопросов, касающихся *обстановки в организации*:

1. Сколько компьютеров в организации, в каких подразделениях они находятся (отделах, службах, филиалах, подразделениях и пр.)?

3. Имеется ли локальная сеть (одна или несколько)? Какова размерность сети (сколько ПЭВМ объединены сетью и в каких помещениях они находятся)? Имеются ли у организации филиалы и представительства, по каким адресам, соединены ли в локальную сеть их компьютеры? Связаны ли их сети с сетью основного предприятия?

4. Есть ли в организации компьютеры, имеющие выход в глобальную сеть? В каких помещениях они находятся? Посредством какого провайдера осуществляется выход в глобальную сеть?

5. Какие средства связи и телекоммуникаций используются для работы средств вычислительной техники и информационного обмена (какого типа, общедоступные или конфиденциальные, абонентские номера, позывные, ключи (коды) доступа)?

6. Каков режим и система охраны объекта? Какая организация осуществляет охрану?

7. К какой категории относится обрабатываемая информация (имеются ли данные, составляющие государственную тайну, конфиденциальная информация, персональные данные)?

8. Какие источники электропитания используются (электросеть, автономные, бесперебойные, комбинированные)?

9. Какая операционная система и какое программное обеспечение используется в сети?

10. Какие средства защиты доступа используются в локальной сети (коды, пароли, шифры, программные средства и др.)?

11. Какая документация по функционированию локальной сети ведется в организации? Кто ответственен за ее ведение?

12. Какая часть бухгалтерского учета (какие именно учетно-хозяйственные операции) фиксируется через локальную сеть и где хранятся итоги обработки?

13. Другие вопросы.

Для выяснения перечисленных выше вопросов проводится ряд *следственных действий и иных мероприятий*, в частности:

запрос и изучение схемы документооборота организации, утвержденной приказом руководителя на текущий год или интересующий следствие период;

выемка и изучение документов по локальной сети (технический проект и сопроводительные документы, в которых указываются: количество помещений, охваченных сетью; количество ПЭВМ в каждом помещении, подключенных к сети; схемы мест подключения в каждом помещении; место нахождения сервера; тип машины, которая будет использоваться в качестве сервера, и ее технические характеристики);

анализ показаний свидетелей, потерпевших, подозреваемых, обвиняемых, допрошенных по перечисленным выше вопросам. Свидетельская база должна быть расширена и представлена следующими группами свидетелей: заказчики локальной сети, проектировщики, менеджер сети, операторы и лица, работающие непосредственно с сервером и рабочими станциями, и другие;

выемка и исследование актов проверок независимых контролирующих органов: налоговых, финансовых, экологических, санитарных, пожарных, а также аварийных, аудиторских проверок и других документов.

В этот период тактически правильно должны быть определены не только места проведения следственных действий, но и время с учетом возможного доступа к средствам компьютерной информации, оказания противодействия следственной группе со стороны правонарушителей, полноты загрузки мощностей дей-

ствующего компьютерного оборудования или, наоборот, его отключения и т. д.

Обязательно должен составляться *план* предстоящего следственного действия, в котором учитываются и тактически обоснованно используются полученные данные об обстановке в заподозренной организации. Именно на основе «разведывательных данных» следователь определяет место, время проведения следственного действия, его участников, материально-техническое обеспечение и др. Важно иметь технический план локальной вычислительной сети.

Планирование состава оперативно-следственной группы зависит от обстановки в организации. Кроме следователя, осуществляющего руководство производством следственного действия, *в группу обязательно включаются*:

оперуполномоченный отдела «К» при УСТМ ОВД;

специалист-криминалист прокуратуры или ОВД, прокурор-криминалист;

инженер по видеотехнике;

специалисты (в зависимости от вида и функций носителей цифровой информации, подлежащей осмотру).

При производстве следственного действия *могут присутствовать*:

собственник жилья и проживающее лицо (если следственное действие проводится в жилище);

представители организации, в которой проводится следственное действие: администрации; службы безопасности; персонал, обслуживающий носители цифровой информации; специалисты (операторы ЭВМ, бухгалтеры, контролеры, технологи и другие, в зависимости от задач следственного действия и обстановки) и др.

Техническая подготовка включает обеспечение транспортом, упаковочными материалами, научно-техническими средствами различного назначения, достаточным количеством дискет для копирования информации.

Целесообразно иметь при себе:

портативный компьютер Notebook с соединительными кабелями с различными разъемами или с комбинированным разъемом;

программное обеспечение для копирования информации на месте производства следственного действия;

набор сервисных программ для определения технических характеристик исследуемых компьютеров, исправности отдельных устройств и внешней памяти, а также антивирусные программы;

при необходимости копирования небольших фрагментов информации — комплект дискет, чистых компакт-дисков (CD-R или CD-RW) для записи информации. Необходимый набор сервисных программ следователь или специалист формирует по своему усмотрению в зависимости от категории расследуемых дел, используемого программного обеспечения и оборудования в данном регионе в данный момент времени.

Как отмечалось выше, место совершения компьютерного преступления неоднозначно, поэтому поиск и фиксация компьютерной информации осуществляется на различных объектах, а именно в местах*:*

непосредственной обработки и постоянного хранения компьютерной информации, ставшей предметом преступного посягательства;

непосредственного использования компьютерного оборудования с целью неправомерного доступа к охраняемым базам и банкам данных или создания, использования и распространения вредоносных программ для ЭВМ;

хранения добытой преступным путем из других компьютеров, компьютерных систем и сетей информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети;

непосредственного нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети;

наступления вредных последствий;

задержания подозреваемого (личный обыск).

2

В ходе осмотров и обысков исследуются служебные и жилые помещения; средства вычислительной техники, носители машинной информации, документы, предметы и иные объекты.

Поскольку для следователя может быть затруднительным обращение с компьютерной техникой и информацией, необходимо привлекать для участия в следственных действиях всевозможных специалистов:

программистов по операционным системам и прикладным программам;

электронщиков;

специалистов по средствам связи и телекоммуникациям;

специалистов по сетевым технологиям;

специалистов в области экономики, финансов, бухгалтерского учета, в том числе лиц, владеющих навыками работы с определенными компьютерными бухгалтерскими, учетными и другими программами;

других специалистов.

Производя осмотр и обыск, необходимо учитывать, что компьютерное оборудование и компьютерная информация, как уже упоминалось, могут быть предметом посягательства, орудием преступления и хранилищем доказательств. В связи с этим их осмотр и обыск должен иметь цель поиска, обнаружения, закрепления и изъятия всех возможных следов*, связанных с указанными функциями объектов. Например:*

информация о незаконных бухгалтерских и финансовых операциях, произведенных в кредитно-финансовой сфере;

программы, отвечающие за проведение электронных платежей по сети Интернет с использованием услуг Интернет-магазинов и виртуальных фирм, а также списки произведенных перечислений с чужих счетов и кредитных карт;

программы для осуществления виртуальной торговли WEB-MANY;

переписка соучастников, касающаяся организации и исполнения преступления;

сведения, составляющие государственную, коммерческую, банковскую тайну;

программное обеспечение и базы данных, правообладателями которых являются иные лица;

личная переписка;

порнографические изображения;

вредоносные программы;

файлы, содержащие конфиденциальную информацию, которой на законных основаниях не может обладать данный субъект;

зашифрованные данные, связанные с совершением преступления.

Немаловажное значение имеет обнаружение и изъятие в помещении, где установлено компьютерное оборудование, «традиционных» вещественных доказательств. *При совершении компьютерных преступлений таковыми могут быть:*

бумажные носители информации (распечатки с принтера, в том числе оставшиеся внутри его);

записи кодов и паролей доступа;

тексты программ и описание программного обеспечения;

записные книжки, в том числе и электронные, в которых могут находиться имена, клички хакеров и соучастников, номера телефонов, банковских счетов, ПИН-коды пластиковых карт;

кредитные карточки соучастников и третьих лиц, с помощью которых обналичивались и изымались денежные средства, похищенные с использованием компьютерных технологий;

вещи и ценности, приобретенные на похищенные деньги;

телефонные счета за пользование провайдерскими услугами;

нестандартные периферийные устройства, устройства доступа в телефонные сети и сети ЭВМ;

документы, должностные инструкции, регламентирующие правила работы с данной компьютерной системой, сетью с пометками сотрудника, свидетельствующие о его ознакомлении с ними;

личные документы преступников.

Если непосредственный доступ к ЭВМ осуществлялся посторонним лицом, целесообразно направить усилия на поиск следов рук на клавиатуре, мониторе, системном блоке, мебели, следов ног на полу, следов орудий взлома, сопровождавшего проникновение преступника в помещение, и пр.

3

В ходе выемки обязательно изымаются документы, необходимые для решения вопроса о нарушении правил эксплуатации ЭВМ:

инструкции производителя по эксплуатации ЭВМ, системы или сети ЭВМ;

правила работы на ЭВМ, установленные фирмой — собственником оборудования;

журналы регистрации сбоев ЭВМ;

журнал ремонта и профилактических осмотров компьютерного оборудования;

материалы служебного расследования факта нарушения правил эксплуатации;

приказ руководителя организации об отнесении сведений к разряду коммерческой тайны;

приказ о назначении лица на должность;

должностная инструкция работника;

документы о соответствующей подготовке лица для работы с оборудованием;

другие документы.

4

Осмотры, обыски и выемки дают богатый материал для дальнейшего расследования. Его дополняют *показания заявителей о совершенном преступлении*. Если заявление поступило от лиц, которым причинен материальный, моральный или иной вред действиями преступников, они признаются потерпевшими по делу. В ходе их допроса выясняется обстановка в организации, способы защиты компьютерной информации и доступа к ЭВМ и локальной сети организации, обстоятельства выявления преступления, последствия преступного посягательства, оценка причиненного вреда. Если преступник не установлен, целесообразно в ходе допроса попытаться выяснить некоторые криминалистические признаки, позволяющие получить сведения о правонарушителе. Например, как часто менялись коды и пароли доступа к информации, на ком лежала ответственность за их смену, имелись ли факты осуществления сотрудниками сверхурочных работ без видимых на то причин, немотивированные отказы от отпусков сотрудников, обслуживающих компьютер-

ные системы или сети, чрезмерный интерес некоторых сотрудников к работе других отделов, к документам или работе компьютеров, появление дискет или лазерных дисков для копирования компьютерной информации, другие случаи подозрительного поведения сотрудников, обслуживающего персонала или посторонних лиц, кто из посторонних лиц проявлял интерес к оборудованию, программному обеспечению и компьютерной информации.

После таких допросов легко определить *свидетельскую базу*, т. е. тех лиц, которые причастны к работе вычислительных систем и сетей. Начинать допросы, безусловно, следует с очевидцев совершенного преступления, т. е. тех, кто непосредственно может свидетельствовать о неправомерном доступе к информации, создании, использовании или распространении вредоносных программ или нарушении правил эксплуатации компьютерного оборудования либо о тех последствиях, которые возникли в результате этих действий. В качестве свидетелей допрашиваются сотрудники потерпевшей организации по обстоятельствам неправомерного доступа: операторы; администраторы сети; работники бухгалтерии и финансового отдела; руководители отделов, где обрабатывается информация, подвергшаяся «нападению»; инженеры-программисты, разработавшие программное обеспечение и осуществляющие его отладку и обслуживание; специалисты, занимающиеся эксплуатацией и ремонтом компьютерной техники; системные программисты; инженеры по средствам связи и телекоммуникационному оборудованию; специалисты, обеспечивающие информационную безопасность; работники охраны и службы безопасности и другие.

Целью их допросов является получение показаний об обстоятельствах, предшествовавших совершению преступления, для установления круга подозреваемых лиц; об обстоятельствах обнаружения факта преступления и наступивших негативных последствиях. Уточняется наличие и функционирование информационной защиты, ее недостатки, иные причины и условия, которые могли быть использованы для совершения противоправных действий.

Если преступник установлен, проводится его задержание, личный обыск, допрос в качестве подозреваемого, обыск по месту жительства и работы, другие следственные действия.

Готовиться к допросу подозреваемого и обвиняемого в ряде случаев целесообразно, заранее получив консультацию специалиста, поскольку совершение компьютерных преступлений по плечу не каждому субъекту, а лишь тем, кто имеет специальную подготовку, соответствующие знания, навыки, оборудование. Знания следователя не всегда могут соответствовать необходимому уровню, поэтому он должен восполнять пробелы за счет привлечения специалиста. Лучше всего получить предварительную консультацию, а затем пригласить специалиста для участия непосредственно в допросе.

В ходе допроса подозреваемого и обвиняемого *выясняются следующие вопросы:*

какое образование имеет подозреваемый или обвиняемый, имеет ли навыки обращения с компьютером, где, когда и при каких обстоятельствах он освоил работу с компьютерной техникой и с конкретным программным обеспечением;

каково место его учебы или работы, должность, работает ли он на компьютере по месту работы, имеет ли правомерный доступ к компьютерной технике и к определенным видам программного обеспечения;

какие операции с компьютерной информацией выполняет на рабочем месте;

имеет ли правомерный доступ к глобальной сети Интернет или иной, работает ли в них;

закреплены ли за ним по месту работы идентификационные коды и пароли для работы в компьютерной сети, кто их устанавливает, как часто они меняются;

если не работает, то какие операции выполняет на своем персональном компьютере либо персональных компьютерах других лиц из своего ближайшего окружения, где и у кого приобрел программы для своей ЭВМ.

На эти вопросы подозреваемые обычно отвечают охотно и даже немного бравируют, стараясь показать свое превосходство над следователем в области знания компьютерного оборудования. Если подозреваемый или обвиняемый пожелает далее отвечать на вопросы, то следует выяснить у него обстоятельства совершенного преступления:

как и кто высказал идею совершения преступления;

как осуществлялась подготовка, выбирался объект «атаки»;

каковы мотивы и цель совершения преступления;

как осуществлен неправомерный доступ к информации, создана вредоносная программа, использовалась ли или распространялась ли она, знает ли создателя вредоносной программы;

знает ли о наступивших вредных последствиях;

другие вопросы.

Несколько отличается тактика допросов подозреваемых в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети. Ими могут быть только лица, имеющие правомерный доступ к компьютерному оборудованию и сети, компьютерной информации. Чаще всего это операторы, программисты, техники-наладчики, сотрудники подразделений, где компьютеризированы функции. При допросе этих лиц следует выяснять:

когда назначен на должность, какое получил образование, какими навыками обладает;

был ли ознакомлен с установленными режимом работы и правилами эксплуатации; в каком документе такое ознакомление отражено, проводился ли официальный инструктаж, кем и как часто, в каких документах фиксировался;

каковы место и время факта нарушения правил эксплуатации, в какой период времени подобным образом эксплуатировалось оборудование;

в чем конкретно выразилось нарушение правил эксплуатации, каковы технические аспекты способа и механизма нарушения правил: совершены действия, не предусмотренные инструкциями; не выполнены предписанные действия; нарушены технологии соответствующих операций;

каковы последствия допущенных нарушений: возникновение нештатной ситуации с компьютером и его устройствами, повлекшей уничтожение, модификацию или копирование информации; выведение из строя компьютерной системы, вызвавшее блокирование информации и нарушение работы организации, учреждения, предприятия, систем управления и связи; вывод из

строя оборудования организации, управляемого компьютерными программами; иное;

место наступления вредных последствий.

В *отношении субъектов преступления* устанавливаются:

персональные данные;

занимаемая должность;

функциональные обязанности, связанные с ответственностью за информационную безопасность и надежность работы компьютерного оборудования, за обеспечение выполнения правил эксплуатации данной компьютерной системы или сети;

нормативные акты, устанавливающие функциональные обязанности субъекта: инструкции и правила по эксплуатации, приказы, распоряжения руководителей, трудовой договор или контракт, дополнительные соглашения и пр.;

образование и специальность;

стаж работы по специальности и на данной должности;

уровень профессиональной квалификации;

данные, характеризующие лицо по месту работы.

Указанная информация устанавливается посредством допросов свидетелей, самого подозреваемого, истребования соответствующих документов из кадрового органа, осмотра эксплуатационных документов на данную компьютерную систему, осмотра компьютера, оборудования к нему, машинных носителей информации, распечаток.

Вопросы для самоконтроля

1. Какие мероприятия осуществляются при подготовке к изъятию компьютерной информации?

2. Какие участники уголовного процесса привлекаются к производству следственных действий?

3. Каковы тактические особенности производства осмотра места происшествия?

4. Каковы тактические особенности обыска и выемки?

5. Каковы тактические особенности допроса подозреваемых и обвиняемых?

Лекция 4

ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ

ПРИ РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ

ПРЕСТУПЛЕНИЙ

П л а н

1. Консультации специалиста.

2. Участие специалиста в следственных действиях и допрос специалиста.

3. Назначение судебных экспертиз.

4. Оценка следователем заключения эксперта.

1

Выявление и расследование компьютерных преступлений на практике часто вызывают значительные трудности для следователей и оперативных работников. Способы совершения таких правонарушений настолько разнообразны и так стремительно меняются в зависимости от появления новых вычислительных средств и информационных технологий, что у лиц, проводящих расследование, появляется острая необходимость в помощи сведущих лиц при поиске следов преступления, их фиксации, закреплении и исследовании. В связи с этим расследование таких преступлений, как никаких других, связано с *использованием специалистов* самых разных отраслей знаний и деятельности: информатики, электроники, программирования, телекоммуникационных систем, криптографии, сетевых технологий, проектирования информационных систем и технологий, формирования банков и баз данных, режима их использования и др.

Использование специальных знаний при расследовании преступлений в сфере компьютерной информации, так же как и по другим преступлениям, осуществляется в виде неофициальных консультаций специалистов различных отраслей науки и техники, участия специалистов при производстве следственных действий и производства экспертиз.

Неофициальные консультации проводятся, как правило, до возбуждения уголовного дела или на начальном этапе расследования и необходимы для получения общих сведений о действии ЭВМ, их систем и сетей, построения общей модели способа со-

вершения преступления и никак не отражаются в материалах дел. На этой стадии в порядке консультации специалист может дать характеристику компьютерного оборудования и используемого программного обеспечения; описать механизм следообразования; оценить возможности осуществления неправомерного доступа к компьютерной информации; описать возможные способы неправомерного доступа в конкретной ситуации; характеризовать вредные последствия; ответить на другие вопросы, связанные с совершенным или готовящимся посягательством.

2

Для повышения эффективности производства следственных действий при расследовании компьютерных преступлений целесообразно *процессуально привлекать специалистов* для содействия в обнаружении, закреплении и изъятии средств вычислительной техники, носителей цифровой информации и самой информации, применении технических средств для поиска и закрепления следов преступления. Участие специалиста в соответствии с ч. 1 ст. 58 УПК РФ целесообразно: в осмотре места происшествия; осмотре носителей информации и компьютерного оборудования; обыске; выемке; следственном эксперименте; контроле и записи переговоров; проверке показаний на месте; допросах подозреваемых, обвиняемых, потерпевших, свидетелей.

По ходу производства следственных действий специалист может также консультировать следователя по вопросам, связанным с использованием компьютерного оборудования и программного обеспечения; правилам обращения с цифровой информацией, оказывать помощь при постановке вопросов эксперту. Достаточно подробно роль специалиста при производстве обыска, выемки, осмотра рассмотрена в предыдущей лекции. Напомним лишь, что все манипуляции с вычислительной техникой и цифровой информацией рекомендуется выполнять только специалисту во избежание утраты, изменения или блокирования информации, что сделает невозможным ее дальнейшее экспертное исследование.

Новым следственным действием для российского уголовно-процессуального закона является допрос специалиста, который

позволяет непроцессуальную форму участия специалиста в расследовании (например, консультации) перевести в процессуальную, закрепив ее в материалах дела посредством показаний. В ходе допроса специалиста могут выясняться и закрепляться не только обстоятельства, требующие оценки лицом, обладающим специальными знаниями, но и разъяснение специалистом сущности своего заключения, данного в письменном виде.

3

Заключение эксперта по рассматриваемой категории дел является одним из важнейших источников доказательств. Именно экспертные исследования позволяют придать изъятым аппаратным средствам, программному обеспечению и компьютерной информации доказательственное значение, упрощая процедуру юридической оценки собранных по делу материалов. В таких условиях основными задачами следователя являются лишь поиск, фиксация, изъятие с помощью специалистов и представление эксперту необходимых материальных объектов — носителей информации.

Экспертиза компьютерной техники, программного обеспечения и информации еще только начинает формироваться как самостоятельный род судебных экспертиз, но уже определено ее место в классификации экспертиз[26]. Теоретики правомерно, на наш взгляд, относят эти экспертизы к классу инженерно-технических, хотя название является условным и, скорее, традиционным, поскольку указанная экспертиза имеет целью исследование не только средств вычислительной техники (их аппаратной части), но и сетевых технологий, других носителей

---

[26] См., напр.: Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М., 2001. С. 117—136; Вехов В. Б., Попова В. В., Илюшин Д. А. Указ. соч. С. 91—92; Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. М., 2004. С. 254—262; Козлов В. Е. Указ. соч. С. 218—219; Нехорошев А. Б. Компьютерные преступления: квалификация, расследование, экспертиза. Ч. 2. Расследование и экспертиза. Саратов, 2004. С. 104—119 и др. В то же время в научной литературе и в практике экспертных исследований еще встречаются термины: программно-техническая, кибернетическая, информационно-техническая, информационно-технологическая экспертиза и т. п. См., напр.: Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации. М., 2001. С. 61—63; Пособие для следователя. Расследование преступлений повышенной общественной опасности. С. 410—418 и др.

цифровой информации и самой цифровой информации. Поэтому и теоретики и практики все чаще высказывают предложение именовать экспертизу как судебную компьютерную[27]. Такая позиция также представляется уязвимой, поскольку объектами экспертного исследования в настоящее время являются не только компьютерные, но и иные носители цифровой информации, а также сама цифровая информация. Тем не менее термин «компьютерно-техническая экспертиза» широко используется, в том числе и экспертными службами МВД России, Министерства юстиции РФ, ФСБ РФ. В то же время разнообразие решаемых этой экспертизой задач позволяет выделять несколько ее видов:

судебная аппаратно-компьютерная экспертиза — исследует электронные, электрические и механические схемы, блоки, приборы и устройства, составляющие материальную часть компьютерной системы;

судебная программно-компьютерная (экспертиза программного обеспечения) — исследует всевозможное программное обеспечение, как системное, необходимое дополнение аппаратных средств, так и прикладное, определяющееся функциональной ролью компьютерной системы и потребностями конкретного пользователя (например, по делам об экономических преступлениях это чаще всего бухгалтерские, складские, кадровые программы);

судебная информационно-компьютерная — осуществляет поиск, обнаружение, анализ, идентификацию и интерпретацию информации, используемой или подготовленной интересующим следствие пользователем, а также созданной для организации информационных процессов в компьютерной системе;

судебная компьютерно-сетевая экспертиза — анализирует функциональное предназначение компьютерных средств, реализующих ту или иную сетевую информационную технологию; исследует факты и обстоятельства, связанные с использованием сетевых и телекоммуникационных технологий (в том числе Интернет-технологий). Лишь использование специальных знаний в

---

[27] См., напр.: Тушканова О. В. Терминологические проблемы судебной компьютерной экспертизы // Раскрытие и расследование преступлений, сопряженных с использованием средств вычислительной техники. Проблемы, тенденции, перспективы. М., 2005. С. 130—135.

области сетевых технологий позволяет соединить воедино полученные разнообразные объекты как элементы сети, проанализировать сведения об их использовании в преступной деятельности и решить экспертные задачи. Ее подвидом является судебная телематическая экспертиза, объектами которой служат средства телекоммуникаций и подвижной связи как материальные носители информации о факте или событии преступного посягательства;

судебная информационно-технологическая экспертиза — исследует собственно информационно-технологические процессы сбора, накопления, хранения, поиска, актуализации, распространения информации и представления ее потребителю в условиях функционирования автоматизированных информационных систем и сетей, отдельно взятых технических и иных средств обеспечения этих процессов. Ее объектом является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, т.е. информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

Экспертным исследованиям подлежат предметы и документы, имеющие значение для расследования уголовного дела и изъятые в ходе следствия в строго процессуальном порядке путем осмотра, обыска или выемки.

Объекты, представляемые на экспертизу, весьма разнообразны:

компьютеры, их системы и сети, а также их отдельные части и комплектующие, сопроводительная документация к ним;

периферийные устройства: клавиатура, манипуляторы всех видов («мышь», джойстик, трекбол), дисплеи, модемы, сканеры и коммуникационные устройства компьютеров и вычислительных сетей, сопроводительная документация к ним и т. д.;

магнитные носители информации (накопители на жестком магнитном диске — НЖМД, дискеты, оптические диски, карты флэш, стриммерные ленты, видеокассеты и т. п.);

различные коммуникационные устройства (пейджеры, телефонные аппараты, электронные записные книжки, мобильные телефоны и другая бытовая техника, содержащая информацию в электронном виде), непосредственно линии электросвязи и обеспечивающие их устройства, иные электронные носители

текстовой и цифровой информации (контрольно-кассовые машины и т. п.), сопроводительная документация к ним;

документы, изготовленные с использованием компьютерных систем и электронных средств передачи и копирования информации (факсы, ксерокопии и т. д.);

компьютерная информация (программы, тексты) в различном виде;

документация по работе с информацией, информационными системами и оборудованием;

видео- и звукозаписи, визуальная и звуковая информация, в том числе на лазерных дисках;

иные электронные технические средства, множительная техника, средства спецтехники и связи, электронные замки, электронные средства охраны и безопасности экономического субъекта, пластиковые карты различного назначения.

Например, непосредственными объектами информационно-технологической экспертизы могут быть:

проектная документация на разработку и эксплуатацию компьютерных систем и сетей, отражающая процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Так, в ходе расследования одного из уголовных дел о хищении денежных средств с использованием ЭВМ экспертному исследованию подвергалась вся проектная документация на конкретную межбанковскую систему электронных платежей, включающая все стадии разработки, внедрения, эксплуатации, контроля и сопровождения данной системы, в следующей последовательности: стадия постановки задачи; стадия предпроектного исследования; стадия подготовки технического задания (ТЗ); стадия технорабочего проектирования; стадия тестирования (испытания) программного обеспечения, стадия ввода в эксплуатацию; стадия эксплуатации, обеспечения безопасности и контроля; стадия сопровождения. Все эти стадии предусмотрены ГОСТами: 24.601-86 «Стадии и этапы создания и развития АСУ» и 24.602-86 «Состав и содержание работ по стадиям создания», относящимся к АСУ всех видов и назначений;

документированная информация (документ), т. е. зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать (отдельные документы и массивы документов в информационных системах), в том числе конфиденциальная информация;

материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов;

приказы и распоряжения администрации, инструкции, протоколы, договоры, положения, уставы и методики по эксплуатации компьютерных систем и сетей, отражающие порядок формирования информационных массивов и доступа к ним (важнейшими из этих предметов исследования могут быть должностные инструкции сотрудников соответствующих информационных подразделений);

схемы движения информации от источников к потребителю с указанием пунктов ее сбора, контроля, накопления, обработки и использования;

табель распределения выходных данных (перечень пользователей с указанием периодичности, объема и сроков поступления информации), а также другие документы, позволяющие наиболее полно раскрыть сущность информационной технологии данной компьютерной системы или сети (обычно прилагаются к техническому заданию на их разработку);

входные и выходные документы, установленные для данной автоматизированной информационной системы;

словари, тезаурусы и классификаторы;

иные эксплуатационные и сопроводительные документы (особое значение для расследования компьютерных преступлений имеют журналы и другие виды учета работы операторов, регистрации сбойных ситуаций и обращений в компьютерную систему или сеть).

Следователь, установив, что добытые им в ходе следственных действий фактические данные не могут быть непосредственно положены в основу обвинения, поскольку для их интерпретации и использования требуются специальные знания, принимает решение о назначении экспертизы. Такое же решение принимается им, когда показания разных лиц противоречат друг другу или иным доказательствам по делу и установление истины невозможно без обращения к лицам, обладающим специальными познаниями.

Предметом компьютерной экспертизы являются фактические данные, устанавливаемые на основе исследования закономерностей формирования и эксплуатации компьютерных средств, обеспечивающих сбор, обработку, хранение, поиск и распространение информации, и на основе анализа самой компьютерной информации, имеющие значение для дела вследствие пося-

гательства на них, использования в качестве орудия преступления или доказательства по делу.

В связи с этим основными задачами экспертизы можно считать определение статуса объекта, являющегося компьютерным средством, его диагностику, выявление и изучение следовой картины представленного устройства, получение доступа к компьютерной информации и ее всестороннее исследование. Судя по стремительному развитию информационных технологий, их использование в преступной деятельности будет постоянно меняться, поэтому и предусмотреть все возможные объекты исследований в настоящее время невозможно. В связи с этим вполне уместна постановка такого вопроса эксперту, как: «Является ли представленный объект ЭВМ?» или «Содержит ли данное устройство электронную информацию?».

Вопросы для экспертного исследования

По аппаратным средствам:

1. Является ли представленный объект компьютером? Компьютер какой модели представлен на исследование? Каковы технические характеристики его системного блока и периферийных устройств? Соответствуют ли они представленной технической документации?

2. Где и когда изготовлен компьютер и его комплектующие? Имеют ли комплектующие единый источник происхождения? Вносились ли в конструкцию какие-либо изменения? Как могут эти изменения охарактеризовать пользователя (например, адаптация к специфическому пользователю, использование в конкретных целях и т. п.)?

3. Исправен ли компьютер и его комплектующие? Каковы причины неисправности?

4. Каковы технические характеристики представленной локальной вычислительной сети? Соответствуют ли ее конфигурация и технические характеристики представленной технической документации?

5. Каковы технические характеристики представленных объектов (электронной записной книжки, контрольно-кассовой машины, сотового телефона и т. п.)? Соответствуют ли они представленной технической документации? Имеются ли неисправности? Каковы их причины?

По программному обеспечению:

6. Какая операционная система использована в компьютере?

7. Каково содержание информации, хранящейся на внутренних и внешних магнитных носителях? Какие программные продукты там находятся? Каково их назначение? Каков алгоритм их функционирования, способы ввода и вывода информации? Когда производилась их инсталляция?

8. Являются ли данные программные продукты лицензионными?

9. Какие изменения вносились в программу? Как они видоизменили программу? Вносились ли изменения, направленные на преодоление защиты информации?

10. Использовались ли ограничения доступа к информации? Какие именно? Каково содержание скрытой информации? Предпринимались ли попытки неправомерного доступа к информации? Какие именно?

11. Есть ли в компьютере скрытые или удаленные файлы? Возможно ли восстановление удаленных файлов? Каково содержание восстановленных файлов?

12. Каков механизм утечки информации из локальной вычислительной сети?

13. Не вызваны ли сбои в работе компьютера действием вредоносной программы?

14. Можно ли установить автора программы? Не написана ли программа определенным лицом?

По носителям информации:

15. Каков тип представленного носителя? Каковы его технические характеристики?

16. Какая информация записана на носителе? Имеется ли скрытая информация? Каково ее содержание?

17. Имеются ли механические повреждения? Возможно ли восстановление информации? Каково ее содержание?

18. Возможно ли изменение информации на носителе?

По информации:

19. Имеется ли на представленных носителях информация? Каково ее функциональное назначение? Каково содержание информации, хранящейся на внутренних и внешних носителях?

20. Имеется ли на представленных носителях информация, соответствующая данному образцу?

21. Возможно ли восстановление стертых файлов? Каково содержание восстановленных файлов?

22. Представить информацию, содержащуюся на конкретных носителях, в человекочитаемой форме.

23. Каким образом организована база данных? Какая информация содержится в базе данных? Когда она обновлялась последний раз? Имеется ли в ней запись конкретного содержания? Возможно ли внести в базу данных новую информацию? Каким образом?

24. Когда производилась последняя корректировка файла?

25. Возможно ли внести изменения в информацию на представленном носителе?

По документам:

26. Является ли представленный документ распечаткой информации, содержащейся на магнитных носителях?

27. Какие аппаратные средства и какое программное обеспечение использованы для изготовления представленного документа?

28. Каков способ изготовления представленного документа?

29. Был ли изготовлен данный документ на представленной компьютерной технике?

По информационным технологиям:

30. Соответствуют ли процессы сбора, обработки, накопления, хранения, поиска и распространения информации, установленные проектной и эксплуатационной документацией, информационной технологии в данной компьютерной системе или сети? Если нет, то какие конкретно отклонения от нее допущены?

31. Кем именно нарушены технологические требования в процессе эксплуатации данной компьютерной системы или сети?

32. Кто из должностных лиц должен был обеспечить соблюдение установленной технологии электронной обработки данных?

33. Какие организационно-технологические меры защиты компьютерной системы, предусмотренные эксплуатационной документацией, были приняты?

34. Какие вредные последствия связаны с нарушением установленной технологии электронной обработки информации?

35. Является ли указанное отклонение от технологии обработки данных причиной наступивших последствий?

36. Каковы причины нарушения установленной обработки компьютерной информации? Какие меры необходимо принять для их устранения?

Это далеко не полный перечень вопросов, разрешаемых компьютерной экспертизой. Аппаратные средства и программное обеспечение меняются буквально ежедневно, поэтому предусмотреть все вопросы, которые могут встать перед следователем, невозможно.

Основная рекомендация при формулировании вопросов: обязательная предварительная консультация с экспертом или специалистом. Это поможет точно сформулировать вопросы и правильно использовать специальную терминологию, поскольку имеются случаи, когда следователь своеобразно понимает некоторые термины или руководствуется своими знаниями как пользователя ПЭВМ, не имея профессиональной подготовки работы с компьютерными средствами. Специалист может дать консультацию по определению принципиальной возможности производства экспертного исследования для установления фактов и обстоятельств, интересующих следствие, а также, какие объекты, материалы, сведения и сравнительные образцы для исследования, материалы уголовного дела необходимо представить эксперту.

В процессе расследования преступлений в сфере компьютерной информации может возникнуть необходимость производства и других видов экспертиз. Чаще всего это криминалистические (трасологическая, дактилоскопическая, почерковедческая, видеофоноскопическая, технико-криминалистическая экспертиза документов, автороведческая и др.), материаловедческие (полимерных материалов и изделий из них), инженерно-технические (радиотехническая)[28].

Так, при необходимости установления тождества конкретного принтера по листингу (распечатке), может быть назначена *криминалистическая экспертиза.* Необходимость в ней может возникнуть также для установления подлинности пластиковых (кредитных) карточек. Такая экспертиза назначается с целью восстановления информации на поврежденных частях магнитных носителей.

---

[28] Вехов В. Б., Попова В. В., Илюшин Д. А. Указ. соч. С. 84—90.

При расследовании компьютерных преступлений в соответствии со ст.201 УПК РФ часто назначаются *комплексные экспертизы*, поскольку анализ компьютерной информации, компьютерных средств и программного обеспечения, равно как и документов, изготовленных с помощью компьютерной техники, не является самоцелью, а призван решить сразу комплекс задач, т. е. исследовать представленный объект с разных сторон (например, компьютерно-техническая и судебно-бухгалтерская, финансово-экономическая, инженерно-экономическая, автороведческая, фоноскопическая, видеофоноскопическая, технико-криминалистического исследования документов, психологическая и другие). Так, при исследовании финансового документа, изготовленного с использованием компьютерной техники, следствие могут интересовать сведения о его экономической сущности (содержании), лицах, державших в руках документ, последовательности нанесения на документ текста, подписи, оттиска печати, подлинности подписи на документе, об авторе текста, о техническом устройстве (принтере, факсе, ксероксе, его типе или конкретном экземпляре), на котором он изготовлен, о соответствии его файлу, представленному на магнитном носителе, соответствии копии документа оригиналу и т. д.

При необходимости назначения комплексного экспертного исследования эксперты разных специальностей включаются в состав одной комиссии и совместно решают поставленные вопросы, каждый в рамках своей компетенции. Из членов комиссии назначается ведущий эксперт. В его обязанности входит:

координация работы остальных членов экспертной комиссии;

переписка со следователем, его консультирование;

уточнение экспертных задач, выработка плана исследований и постановка частных задач перед экспертами-участниками в соответствии с их специальными знаниями;

хранение объектов экспертизы, их передача от одного эксперта другому;

сбор, сопоставление и обобщение результатов исследований, проведенных всеми членами экспертной комиссии;

проведение координационных совещаний экспертов;

составление синтезирующей части заключения и формулирование итоговых выводов.

Если представленный объект может быть исследован экспертами различных специальностей независимо друг от друга, целесообразнее назначать *комплекс экспертиз*. Это актуально в случаях, когда в регионе не имеется многопрофильных экспертных учреждений и сложно собрать комиссию экспертов для совместной работы. Комплексные исследования значительно увеличивают сроки проведения экспертизы.

Перед назначением комплексной экспертизы или комплекса экспертиз по одному объекту следует проконсультироваться с экспертом: не может ли проведение одних исследований сделать невозможным проведение других (например, опыление дактилоскопическими порошками системных блоков компьютеров или поверхностей дискет приведет к порче дисководов или носителей информации, а значит, информацию нельзя будет считать и использовать в деле, в то же время, если сначала исследовать компьютеры и дискеты, следы пальцев рук эксперта могут наложиться на следы рук преступника или стереться, что не позволит эксперту провести дактилоскопическую идентификацию личности).

Для проведения носящих комплексный характер экспертных исследований в сфере компьютерной информации приглашаются высококвалифицированные специалисты в области информатики, вычислительной техники и программирования, а также в области традиционных видов криминалистической экспертизы, экономической, финансовой, бухгалтерской и товароведческой экспертиз.

Среди вопросов, которые могут быть поставлены на разрешение комплексной *судебно-бухгалтерской и программно-компьютерной экспертизы* можно выделить следующие:

1. Возможен ли несанкционированный скрытый доступ к программному обеспечению с целью внесения изменений, влияющих на результаты расчетов и отчетность?

2. В положительном случае каков механизм совершения таких изменений, куда и какие изменения были внесены, каковы их последствия?

3. Кто из работников организации (банка), обслуживающих и эксплуатирующих эти средства, имеет указанные выше возможности?

4. Каков размер материального ущерба, причиненного организации?

5. Какие нарушения правил, регламентирующих ведение бухгалтерского учета и отчетности, могли способствовать образованию ущерба?

6. Какая операционная система использована в конкретном компьютере?

7. Не вносились ли в программу данного системного продукта какие-либо коррективы, изменяющие выполнение операций (указать каких)?

8. Возможно ли получение доступа к конфиденциальной финансовой информации, имеющейся в данной сети? Каким образом может быть осуществлен этот доступ?

Для проведения исследования подобной комплексной экспертизы представляются:

материалы уголовного дела;

протоколы допроса лиц, проходящих по уголовному делу;

первичные бухгалтерские документы по отделу текущих счетов;

носители информации, в том числе содержащие тексты программ, а также резервные копии информации на ЭВМ отдела текущих расчетов за определенный период при наличии соответствующего оборудования в экспертных учреждениях.

Экспертам также предоставляются:

данные о структуре файлов автоматизированной системы учета банковских операций;

инструктивные материалы по сопровождению программного обеспечения автоматизированной системы учета банковских операций;

носители, отражающие состояние файлов автоматизированной системы учета банковских операций за определенный период времени (когда производились незаконные начисления денег на счет преступника);

журнал учета-передачи смен и сбойных ситуаций (за определенный период);

Инструкция о счетах и вкладах в иностранной валюте и рублях № 8;

Инструкция по бухгалтерскому учету операций Банка для внешней торговли № 30;

акт обеспечения безопасности проведения операций по счетам граждан типа «В» и защите информации от несанкционированного доступа при обработке на ЭВМ за определенный период;

устав банка, приказы, распоряжения, служебные записки, акты проверок, функциональные обязанности и другие документы, регламентирующие служебную деятельность сотрудников вычислительного центра.

Идентификационная задача может быть решена с помощью *комплексной компьютерно-технической и судебно-авторовед-ческой экспертизы,* позволяющей проверить, не написана ли данная компьютерная программа конкретным лицом.

4

Поскольку заключение эксперта — это один из источников доказательств, предусмотренных ст. 74 УПК РФ, не имеющий каких-либо приоритетов, оно оценивается наряду со всеми другими доказательствами.

Прежде всего, при оценке заключения компьютерно-технической экспертизы проводится *проверка соблюдения требований закона* при назначении экспертизы. Так, должны быть проверены компетентность эксперта и его незаинтересованность в соответствии со ст.ст. 69, 70 УПК РФ. Если экспертиза проводится в государственном судебно-экспертном учреждении, должно быть проверено отсутствие заинтересованности в исходе дела руководителя данного учреждения. В противном случае производство экспертизы не может быть поручено данному учреждению, а начатая экспертиза немедленно прекращается в соответствии с требованиями ст. 18 Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации» от 31 мая 2001 г. № 73-ФЗ. Должно быть проверено соблюдение прав участников процесса, предусмотренных ст.ст. 195, 198 УПК РФ. В частности, с постановлением о назначении компьютерно-технической экспертизы должен быть ознакомлен подозреваемый (обвиняемый) и ему необходимо разъяснить его права заявлять отводы эксперту, просить о назначении эксперта из числа указанных им, представлять дополнительные вопросы эксперту, с разрешения следователя присутствовать при производстве экспертизы и давать объяснения эксперту. В то же вре-

мя вопросы обвиняемого обязательны для эксперта только в случае, если их включит в постановление следователь. Если же ходатайство обвиняемого остается без удовлетворения, следователь обязан вынести об этом мотивированное постановление. После проведения экспертизы следователь обязательно знакомит с заключением обвиняемого, который имеет право дать свои объяснения и заявить возражения, а также просить о постановке дополнительных вопросов эксперту либо о назначении дополнительной или повторной экспертизы. Эти требования закона выполняются и в том случае, если экспертиза проведена до привлечения лица в качестве обвиняемого. Право знакомиться с заключением экспертизы появляется у него после предъявления обвинения. Ни тактически, ни процессуально неверно переносить предъявление обвиняемому заключения эксперта на момент ознакомления с материалами уголовного дела после окончания расследования. Такое решение часто приводит к неполноте исследования обстоятельств дела и нарушению принципов уголовного судопроизводства.

Заключение эксперта оценивается следователем исключительно на основании анализа и сопоставления всех имеющихся материалов дела и доказательств. Это обстоятельство требует определенных знаний и опыта, поэтому рекомендуется поручать расследование подобных дел следователям, уже имеющим опыт либо прошедшим специальную подготовку. В случае неясности или неполноты заключения эксперт может быть допрошен или перед ним ставятся дополнительные вопросы. Если же у следователя возникают сомнения в выводах эксперта или они противоречат другим доказательствам, уголовно-процессуальным законом предусмотрена проверка заключения путем назначения повторной экспертизы, поручаемой другому эксперту, или дополнительной экспертизы в соответствии со ст. 207 УПК РФ.

Немаловажно при оценке заключения и выяснение факта соблюдения такого процессуального требования, содержащегося в ст.ст. 80, 191 УПК РФ и ст. 25 Федерального закона «О государственной судебно-экспертной деятельности в РФ», как соответствие заключения экспертизы установленной законом форме. Содержание заключения должно отражать весь ход экспертного исследования: экспертный осмотр, сравнительное исследование, эксперимент, примененные методики исследования, оценку результатов и изложение выводов.

Заключение оценивается и с точки зрения научной обоснованности *применяемых методик исследования и правомерности их применения. Для компьютерно-технической экспертизы это одно из наиболее уязвимых мест. Поскольку экспертиза находится в процессе становления, а методики разработаны недостаточно и внедрены не повсеместно в государственных экспертных учреждениях, первоочередной задачей остается решение вопросов стандартизации и паспортизации методик. Пока в судебной и следственной практике нет случаев исключения из доказательств заключений экспертов в связи с применением неопробированных (непаспортизированных) или недостаточно обоснованных методик, но это связано не с их безупречностью, а с отсутствием опытных и сведущих в вопросах высоких технологий следователей, судей и защитников. Обвиняемые также пока не решаются опротестовывать заключения экспертиз, что можно объяснить особенностями психологических качеств их личности (молодой возраст, недостаток жизненного и правового опыта, своеобразное признание исключительности их интеллектуальных возможностей и пр.). Не известны и случаи опровержения выводов эксперта в связи с неполнотой исследования или применением не всех возможных приемов и методик. Указания следователя или суда о применении конкретных методов экспертного исследования по рассматриваемому виду экспертиз фактически отсутствуют, но если таковые будут заявлены, выполнение их обязательно для эксперта.*

Важное значение имеет проверка подлинности и достаточности *объектов исследования. Это для компьютерно-технической экспертизы самая большая проблема и наиболее уязвимое место. Из изученных материалов уголовных дел в большинстве случаев ставились защитой под сомнение выводы экспертизы именно в связи с исследованием недоброкачественных в процессуальном смысле объектов. Объяснение этому очень простое: следователи до настоящего времени не обладают навыками работы с компьютерной техникой и информацией, поэтому изъятие происходит с грубыми тактическими нарушениями: изымаемые объекты подробно на месте не осматриваются и в протоколах никак не отражаются их индивидуальные признаки; осмотр информации при изъятии носителей часто не про-*

водится вообще, что не мешает следователям признавать объекты вещественными доказательствами.

Так, в Санкт-Петербурге по одному из дел о мошенничестве с использованием «виртуальной торговли» в квартире преступника при обыске изъяты три винчестера. Из протокола обыска не ясно, в каком состоянии и где именно они обнаружены. Зато в кабинете следователя они осмотрены в период с 17.05 час. до 17.15 час. и даже без участия специалиста. Дословно устанавливающая часть протокола сведена к следующему: «Накопитель на жестком магнитном диске «Винчестер» представляет из себя параллелепипед высотой 23 мм, шириной 101 мм и длиной 146 мм, выполненный из металлополимерного сплава. Марка: Cavar 312001. Объем: 1281,9 МБ, серийный №: WD S/N: WT 3021505698». Вопреки всем требованиям закона эти объекты были признаны следователем вещественными доказательствами и без проверки и оценки включены в приговор как доказательства виновности.

Представляется, что эксперт, выполняющий исследование, должен обращать внимание и на безупречность изъятия объектов, которое может осуществляться в рамках осмотра, обыска или выемки, и на правильность упаковки, транспортировки, хранения. Последнее вызывает наибольшую тревогу, поскольку именно при хранении чаще всего следователи «компрометируют» будущие объекты исследований. Многие из них пытаются самостоятельно без соблюдения процессуальных требований осмотреть и исследовать информацию, некоторые используют изъятые компьютерные средства в служебных или личных целях, что приводит к изменению или даже уничтожению информации, а также ставит под сомнение неизменность изъятого объекта. Анализ практики показывает, что именно такая версия защиты (внесение изменений в компьютерную информацию после ее изъятия у пользователя) преобладает по делам, где проводилась компьютерно-техническая экспертиза. Часто эта экспертиза проводится при недостаточных материалах. Эксперты редко пользуются правом участия в следственных действиях, истребования дополнительных материалов уголовного дела, которые следователь обязан предоставить при необходимости для исследования. Они должны проверять правильность исходных данных, указываемых в постановлении следователя или определении суда о назначении экспертизы, и обращать внимание следователя или суда, что такая возможность нереальна. Если же исходные данные не установлены достоверно, возможно заключение по нескольким вариантам в зависимости

от исходной ситуации.

Не остается в стороне и оценка логической обоснованности хода и результатов экспертизы *при оценке ее заключения. Она складывается из анализа последовательности стадий идентификационного и диагностического процессов исследования, ее логической обусловленности и обоснованности выводов на промежуточных этапах и конечного вывода в целом.*

Немаловажна проверка относимости результатов к расследуемым обстоятельствам. *Очень часто формальная постановка вопросов следователями не позволяет определить эксперту, каково значение выводов экспертизы для доказывания по делу, что значительно снижает возможности экспертного исследования, поскольку затрудняет использование экспертом всех имеющихся средств для обнаружения фактов, относящихся к делу.*

Обязательно должен быть решен вопрос о доказательственном значении заключения эксперта. *Заключение редко бывает прямым доказательством, т. е. однозначно устанавливает совершение преступления конкретным лицом. Чаще оно относится к косвенным доказательствам и должно соответствующим образом быть соотнесено с другими доказательствами, имеющимися в деле. Очень распространены вероятностные заключения, которые также могут быть успешно использованы в процессе доказывания.*

Ярким примером доказательственного значения результатов компьютерно-технической экспертизы может служить дело о незаконном подключении «двойников» к сотовой связи, расследованное Главным следственным управлением при ГУВД Краснодарского края. Группа студентов из Ливана и Палестины организовала подпольную телефонную станцию путем незаконного подключения «двойников» к сотовой связи по номерам фирмы «ИСТ». Звонки производились в 44 страны Европы, Азии, Ближнего Востока и Америки. В ходе расследования компьютерно-техническая экспертиза дала вероятностное заключение, установившее возможность кодировки изъятого телефонного аппарата (МТР) на номер сотового телефона фирмы «ИСТ» 4911130 и перекодировки этого аппарата по найденной у преступников схеме на любые известные им шифр-коды, в том числе и на изъятые у обвиняемых. Безусловно, оно имело доказательственное значение наряду с другими доказательствами: обнаружением в комнате общежития двух сотовых телефонов «НОКИЯ» и адаптеров к ним, а также записи, содержащие шифр-коды и схемы перекодировки телефонов; заключением судебно-почерковедческой экспертизы о вы-

полнении этих записей членами преступной группы; показаниями свидетелей; опознаниями преступников лицами, пользовавшимися услугами подпольной станции, но ранее не встречавшимися.

Заключение компьютерной экспертизы может быть использовано на всех стадиях уголовного процесса, в том числе в оперативных и тактических целях.

Следственные и судебные органы все чаще ставят вопросы на разрешение компьютерной экспертизы. Не всегда это связано с совершением так называемых компьютерных преступлений. Стремительное развитие общества в направлении к повсеместной информатизации и развитию высоких технологий сделало возможным использование ПЭВМ во всех отраслях жизни, поэтому правоохранительные органы вынуждены работать с компьютерными средствами и информацией по делам любой категории. Именно в связи с этим, видимо, следует признать, что компьютерная экспертиза становится универсальной и в ближайшее время встанет вопрос о расширении проведения комплексных экспертиз во многих традиционных исследованиях.

Вопросы для самоконтроля

1. В какой форме используются специальные знания при выявлении и расследовании преступлений, совершаемых в сфере высоких технологий?

2. Каково значение для расследования консультаций специалиста?

3. Для участия в каких следственных действиях привлекаются специалисты?

4. Какова роль специалиста, участвующего в следственных действиях?

5. Значение заключения специалиста для расследования.

6. Каковы цель и тактика допроса специалиста?

7. Классификация компьютерной экспертизы.

8. Перечислите основные объекты компьютерной экспертизы.

9. Назовите основания и порядок назначения комплексных экспертиз, назначаемых при расследовании преступлений, совершаемых в сфере высоких технологий.

10. По каким критериям осуществляется следователем оценка экспертного заключения?

Доктрина информационной безопасности Российской Федерации. Утв. Президентом Российской Федерации 9 сентября 2000 г.

Об информации, информационных технологиях и о защите информации: Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ.

Конвенция Совета Европы о киберпреступности 2001 г.

Андреев Б. В., Пак П. Н., Хорст В. П. Расследование преступлений в сфере компьютерной информации. М., 2001.

Батурин Ю. М. Проблемы компьютерного права. М., 1991.

Быстряков Е. Н., Иванов А. Н., Климов В. А. Расследование компьютерных преступлений. Саратов, 2000.

Вехов В. Б. Компьютерные преступления: Способы совершения и раскрытия. М., 1996.

Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации: Науч.-практ. пос. 2-е изд. М., 2004.

Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002.

Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации: Учеб. пос. / Под ред. Н. Г. Шурухнова. 2001.

Данилова Н. А., Николаева Т. Г., Кушниренко С. П., Пристанскова В. Д. Использование специальных знаний в уголовном судопроизводстве (уголовно-процессуальный и криминалистический аспекты). СПб., 2005.

Захарцев С. И. Оперативно-розыскные мероприятия. Общие положения. СПб., 2004.

Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М., 2002.

Крылов В. В. Расследование преступлений в сфере информации. М., 1998.

Крылов В. В. Расследование преступлений в сфере информации. М., 1998.

Крылов В. В. Расследование преступлений в сфере информации. М., 1998.

Курс криминалистики / Под ред. О. Н. Коршуновой, А. А. Сте-панова. Т. 3. Криминалистическая методика. СПб., 2004.

Кушниренко С. П., Панфилова Е. И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях: Учеб. пос. 3-е изд., перераб. и доп. СПб., 2003.

Мазуров В. А. Компьютерные преступления: классификация и способы противодействия: Учеб.-практ. пос. М., 2002. 148 с.

Методика расследования преступлений: Схемы. СПб., 2003.

Методологические основы обеспечения информационной безопасности объекта // Защита информации: Конфидент. 2000. № 1.

Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002.

Нехорошев А. Б. Компьютерные преступления: квалификация, расследование, экспертиза: В 2 ч. Уголовно-правовая и криминалистическая характеристика. Саратов, 2003.

Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. М., 2004.

Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пос. / Под ред. Ю. В. Гаврилина. М., 2003.

Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. М., 2004.

Расследование преступлений о нарушении авторских и смежных прав. Особенности. М., 2001.

Рогозин В. Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Учеб. пос. / Под ред. А. А. Закатова. Волгоград, 2000.

Рогозин В. Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Учеб. пос. / Под ред. А. А. Закатова. Волгоград, 2000.

Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М., 2001.

Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений. М., 2004.

Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 1995.

СОДЕРЖАНИЕ

Светлана Петровна КУШНИРЕНКО,
канд. юрид. наук, доцент

МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Конспект лекций

Редактор *Н. В. Бибикова*
Компьютерная правка и верстка
Т. И. Павловой

Подписано к печати 19.03.2007 г. Бум. тип. № 1.
Гарнитура "Times New Roman Cyr". Ризография. Печ. л. 4,0.
Уч.-изд. л. 4,0. Тираж 500 экз. (1-й завод 1—250). Заказ 1838.
Свободная цена

Редакционно-издательский отдел
Санкт-Петербургского юридического института
Генеральной прокуратуры РФ

191104, Санкт-Петербург, Литейный пр., 44

Отпечатано с оригинал-макета в печатно-множительном отделе
Санкт-Петербургского юридического института
Генеральной прокуратуры РФ