АНО ВО
«Российский новый университет»
Тамбовский филиал

392002, г. Тамбов, ул. Пензенская/Карла Маркса, д. 61/175, к. 3, тел. (4752) 77-10-65

С.И. МОЛЧАНОВА

ОСОБЕННОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Учебное пособие для студентов,
обучающихся по направлению подготовки
40.03.01 «Юриспруденция»

Тамбов
2022

УДК 3433
ББК 67.52
М 76

Автор-составитель:
Молчанова С.И., к.ф.н., доцент кафедры уголовно-правовых дисциплин Тамбовского филиала АНО ВО «Российский новый университет», эксперт АНКО «Тамбовский Центр судебных экспертиз»

Рецензент:
Миронова Л.Ю., к.ф.н., декан юридического факультета Тамбовского филиала АНО ВО «Российский новый университет»

М 76. Молчанова С.И. Особенности раскрытия и расследования компьютерных преступлений. Учебное пособие для студентов, обучающихся по направлению подготовки 40.03.01 «Юриспруденция»/Молчанова С.И., 2022 г. –98с.

Учебное пособие составлено в соответствии с требованиями ФГОС ВО и предназначено для студентов, обучающихся по образовательной программе бакалавриата 40.03.01 Юриспруденция для получения ими актуальных прочных знаний по освоению дисциплин «Криминалистика», «Уголовный процесс», «Уголовное право», «Криминология», а также при подготовке к зачетам и экзаменам по данным учебным дисциплинам.

Сегодня, как никогда ранее, актуальна проблема разработки законодательства в сфере борьбы с киберпреступностью. Появляются новые формы и виды преступных посягательств в сфере высоких технологий.

Учебное пособие освещает теоретические основы и методические подходы к расследованию инцидентов информационной безопасности и правонарушений в компьютерной сфере. Основной целью издания является формирование представлений о способах и средствах реагирования на нарушения информационной безопасности.

Пособие может представлять интерес для студентов юридических вузов, практикующих юристов, особенно начинающих, а также для более широкого круга читателей, не имеющих специальной юридической подготовки и опыта работы в проведении расследования киберпреступлений.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На современном этапе развития цивилизации происходит превращение индустриального общества в общество информационное. Повсеместное внедрение современных информационных технологий создает новые возможности для активного и эффективного развития экономики, политики, государства, общества, социального сознания и гражданина. Однако совершенствование технологий приводит не только к укреплению индустриального общества, но и к появлению новых источников опасности для него. Экономика и обороноспособность ведущих государств мира во многом зависят от нормального функционирования глобальных компьютерных сетей. Нарушение их работоспособности может повлечь серьезные последствия, а национальные и международные правовые институты и организационные структуры практически не готовы к адекватному противодействию новым угрозам. Получая преимущества от использования информационных систем, построенных на основе глобальных компьютерных сетей, Россия постепенно входит в зависимость от их нормального функционирования. Данный факт заставляет вырабатывать новые подходы к уголовно-правовой защите интересов личности, общества и государства в этой сфере.

Сегодня, как никогда ранее, актуальна проблема разработки законодательства в сфере борьбы с киберпреступностью. Это прежде всего обусловлено тем, что с первого дня существования всемирного виртуального пространства в него стали проникать правонарушители самых разных мастей, в том числе и злостные преступники. Появляются новые формы и виды преступных посягательств в сфере высоких технологий. Преступники все чаще применяют системный подход к планированию своих действий, используют современные технологии и специальные средства, создают новейшие системы конспирации.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. КИБЕРПРЕСТУПНОСТЬ.

В настоящее время компьютерная преступность превратилась в целую криминальную отрасль, где действуют мошенники, взломщики-хакеры, рэкетиры, педофилы, сутенеры, торговцы людьми и наркотиками и многие другие нарушители законов. Хищения в особо крупных размерах также сегодня стали характерной чертой киберпространства. Первой серьезной попыткой наведения порядка в Интернете явилась специальная Конвенция

по борьбе с киберпреступностью, подписанная в 2001 г. в Будапеште. Сегодня данный акт подписали более сорока государств, среди которых Украина, Литва, Латвия, Польша, Эстония, Молдавия, Чехия, Румыния, Армения[1].

По данным Бюро специальных технических мероприятий (БСТМ) МВД РФ, каждый год (начиная с 2005 г.) в нашей стране фиксируется порядка 15 тыс. преступлений в сфере высоких технологий. Для сравнения: в конце 1990-х годов работники МВД фиксировали 10-12 подобных преступлений в год, которые носили в основном хулиганский характер. Ситуация с каждым годом становится более серьезной. Через Всемирную сеть ежегодно проходят финансовые операции на сумму порядка 3 трлн. долларов США. Представители американской ассоциации по защите авторских прав констатируют, что мировая промышленная индустрия из-за пиратов теряет от 200 до 250 млрд. долларов в год. Участники глобального рынка оценивают ущерб только американских производителей и правообладателей от пиратства в размере 30-35 млрд. долларов[2].

Следует отметить, что желание навести порядок в Интернете путем создания эффективного механизма регулирования посредством права существовало давно.

Конвенция о преступности в сфере компьютерной информации предусматривает тесное сотрудничество правоохранительных органов стран Евросоюза, а также присоединившихся к этому документу государств. Появляется структура, часто называемая интернет-полицией. Каждый участник соглашения назначает свой контактный центр, работающий 24 часа в сутки в течение 7 дней в неделю, чтобы обеспечить оказание неотложной помощи на стадии расследования или судебного разбирательства уголовных преступлений в сфере высоких технологий. Это касается также сбора доказательств в электронной форме по уголовным преступлениям. Такая помощь включает: оказание технической консультативной помощи; обеспечение сохранности данных; сбор доказательств, предоставление законной информации и установление нахождения подозреваемых лиц. Центр каждой страны располагает возможностями для оперативного обмена сообщениями с аналогичным центром другого государства (ст. 35 Конвенции).

Следует подчеркнуть, что Конвенция определяет четкие правила и нормы противодействия преступным посягательствам и устанавливает гарантии для граждан, согласно которым власти не имеют права без достаточных на то оснований вторгаться в их частную жизнь.

---

[1] *Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2. С. 38-41.*

[2] *http://www.crime-research.ru/news/01.09.2006/2794/.*

В Конвенции важное значение уделяется именно защите информации. Отныне по просьбе заинтересованных в преследовании лиц международная полиция сможет осуществлять расследование случаев взлома сервера или незаконного завладения информацией в любой стране мира, откуда бы ни исходило нападение хакеров. Это также коснется борьбы с проявлениями нацизма и расизма в киберпространстве.

Однако неясно, какие теоретико-правовые и практические новеллы содержит этот так называемый Кодекс и что дает он нам для борьбы с киберпреступностью. Что он вкладывает в понятие и особенности рассматриваемого вида преступлений в Интернете? Какие меры должна предпринять Россия для реализации положений Конвенции на своей территории?

Из анализа юридической литературы можно сделать вывод, что главной особенностью киберпреступления (или компьютерного преступления) является использование сетей компьютера для совершения противоправного поступка или преступления в виртуальном пространстве[3]. Следует отметить, что сам термин «киберпреступность» впервые появился в зарубежной печати в начале 60-х годов XX в., когда были выявлены первые случаи преступлений, совершенных с использованием ЭВМ.

Одна из характерных черт исследуемого вида преступлений - это высокая латентность. Следует также отметить устойчивую тенденцию к «организованности» киберпреступлений и выходу их за национальные рамки. Цивилизованные страны совершенно закономерно пытаются найти пути решения этой проблемы. Ведь чем более масштабной она становится, тем более высокий уровень организации государств требуется для ее разрешения. Так, в рамках ООН регулярно проводятся конференции по профилактике и пресечению киберпреступности, вырабатываются механизмы противодействия этому виду преступлений, принимаются универсальные стандарты и нормы, гарантирующие надежное использование компьютерных систем и средств телекоммуникаций. Такая работа ведется давно.

Исходя из анализа научных работ и публикаций, сегодня можно сделать вывод о том, что киберпреступления нужно исследовать со следующей позиции: необходимо рассматривать киберпреступления как такие действия в Интернете, при которых компьютер является либо орудием, либо предметом посягательств в виртуальном пространстве. При этом, в частности, преступное завладение технических средств и их компонентов в сфере

---

[3] *Компьютерные преступления и информационная безопасность. М.: Новый юрист, 2009. С. 16 - 21.*

интернет-коммуникаций должно рассматриваться как один из случаев совершения киберпреступлений[4].

Одновременно киберпреступления можно исследовать как противозаконные действия в сфере автоматизированной обработки информации. В данном случае в качестве главного классифицирующего признака, позволяющего отнести эти преступления в обособленную группу, выделяется общность способов, орудий и объектов посягательств. Иными словами, объектом посягательства здесь выступает информация, обрабатываемая в виртуальном пространстве, а компьютер служит орудием посягательства.

Законодательство многих стран (в том числе и России) развивается именно в рамках последнего подхода, поэтому, на наш взгляд, следует принять указанную формулировку. Будем считать, что к киберпреступлениям относятся такие общественно опасные деяния, которые совершаются с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете.

Изучение показало, что Конвенция о киберпреступности развивает эти подходы и вносит свою лепту в характеристику данных видов преступлений и в международную организованную борьбу с ними.

Надо отметить, что в данном международном акте детально представлены отдельные виды правонарушений, связанных с использованием компьютерных средств.

Во-первых, это подлог с использованием компьютерных технологий. Каждая страна обязалась реагировать определенным образом (в случае совершения преднамеренно и без права на это) на ввод, изменение, стирание или блокирование компьютерных данных, влекущих за собой нарушение их аутентичности, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве подлинных, независимо от того, поддаются ли эти данные непосредственному прочтению и являются ли они понятными. Страна может требовать для наступления уголовной ответственности наличия намерения совершить обман или аналогичного злого умысла.

Во-вторых, это мошенничество с использованием компьютерных технологий. В случае совершения этого преступления каждое государство принимает такие законодательные и иные меры, которые необходимы для того, чтобы квалифицировать в качестве уголовного преступления, согласно своему внутригосударственному праву (в случае совершения преднамеренно и без права на это), лишение другого лица его собственности путем любого ввода, изменения, удаления или блокирования компьютерных данных; любого вмешательства в функционирование компьютерной системы с

---

[4] *Компьютерные преступления и информационная безопасность. М.: Новый юрист, 2009. С. 16 - 21.*

мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

В-третьих, это правонарушения, связанные с детской порнографией. Отмечается, что стороны обязаны остро реагировать, согласно их внутригосударственному праву, в случае совершения преднамеренно и без права на это следующих деяний: производство детской порнографической продукции с целью распространения через компьютерную систему; предложение или предоставление в пользование детской порнографии через компьютерную систему; распространение или передача детской порнографии через компьютерную систему; приобретение детской порнографии через компьютерную систему для себя или для другого лица; владение детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.

Анализ показал, что значительное место в тексте Конвенции о киберпреступности отводится также правонарушениям, связанным с нарушением авторских и смежных прав.

Что касается санкций и мер, то указанная Конвенция устанавливает, что каждая сторона принимает такие меры, какие могут быть необходимы для обеспечения того, чтобы к лицам, совершившим уголовные преступления, были применены эффективные, соразмерные и убедительные меры наказания, включая лишение свободы (ст. 13 Конвенции)[5].

Отмечается, что каждое государство делает все возможное для установления юрисдикции в отношении любого правонарушения, предусмотренного в Конвенции о киберпреступности, когда такое правонарушение совершено, в частности: на его территории; или на борту судна, плавающего под флагом этого государства; или на борту самолета, зарегистрированного согласно законам этого государства; или одним из его граждан, если это правонарушение является уголовно наказуемым в месте его совершения или совершено за пределами территориальной юрисдикции какого-либо государства.

Если на юрисдикцию в отношении предполагаемого правонарушения претендует более одного государства, заинтересованные стороны, по мере необходимости, проводят консультации с целью определить наиболее подходящую юрисдикцию для осуществления судебного преследования.

Все это ставит перед Российской Федерацией задачу совершенствования законодательства в сфере борьбы с киберпреступлениями (и в частности, в свете изложенной выше Конвенции о киберпреступности). Наличия в Уголовном кодексе РФ трех статей о преступлениях в сфере компьютерной информации (ст. 272 - 274) и отдельных записей в иных правовых актах об ответственности руководителей информационных систем,

---

[5] *Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2. С. 38-41.*

пользователей информации в Сети, провайдеров, СМИ и т.д. сегодня уже явно недостаточно. Необходимо разработать и принять специальный закон о борьбе с киберпреступностью в нашей стране, а также внести соответствующие дополнения в уже действующее законодательство. Причем все это должно быть увязано с Конвенцией о киберпреступности.

Преступления в сфере компьютерной информации (компьютерные преступления) - это запрещенные уголовным законом виновные посягательства на безопасность в сфере использования компьютерной информации, причинившие существенный вред или создавшие угрозу причинения такого вреда личности, обществу или государству[6].

Специфика преступлений данной группы определяется их объектом и предметом. С одной стороны, закон относит их к преступлениям против общественной безопасности. Поэтому составы компьютерных преступлений следует толковать в том смысле, что эти преступления представляют опасность для охраняемых законом интересов неопределенного круга лиц. С другой стороны, все указанные преступления совершаются путем неправомерного воздействия на компьютерную информацию, что ограничивает объект и указывает на предмет этого преступления.

Единство объекта компьютерных преступлений определяется не тем обстоятельством, что социальные отношения по поводу использования компьютерной информации являются самостоятельной сферой общественной жизни. Сами по себе эти отношения лишены ценностного содержания. Ценностное содержание и значение объекта преступления приобретает лишь компьютерная безопасность. Опасность компьютерных преступлений в том, что они создают опасность жизни и здоровью, имущественным правам и интересам, неприкосновенности частной жизни, иным охраняемым законом интересам личности, общества и государства, Недопустимо применение к человеку уголовной репрессии лишь за нарушение установленного порядка в сфере использования компьютерной информации, если его деяние не причинило и не могло причинить никакого реального вреда. Не будет, например, преступлением в силу ч. 2 ст. 14 УК[7] использование одним несовершеннолетним компьютера другого несовершеннолетнего для игр без согласия последнего, даже если это привело к копированию очень большого объема информации, исчисляемого сотнями мегабайт. С другой стороны, изменение даже одной единицы информации в оборонной или транспортной системе может вызвать серьезные вредные последствия и может влечь уголовную ответственность при неправомерном доступе.

Поэтому представляются обоснованными предложение Г.П. Новоселова de lege ferenda не рассматривать уничтожение, блокирование информации и т.п. в качестве

---

[6] *Иногамова-Хегай.Л.В. Уголовное право РФ. Особенная часть. – М. 2010.*

последствия преступления. Целесообразно было бы определить их в качестве способа посягательства, но это не основано на действующем законе[8].

Видовым объектом компьютерных преступлений является безопасность в сфере использования компьютерной информации - общественные отношения, обеспечивающие безопасное использование ЭВМ, компьютерных систем и сетей, т.е. такое их использование, которое исключает причинение вреда личности, обществу и государству. Непосредственными объектами преступлений в сфере компьютерной информации являются отдельные виды отношений, входящие в содержание данного вида общественной безопасности: неприкосновенность информации, содержащейся в ЭВМ, их системе или сети, и правильная эксплуатации системы, исключающие причинение вреда личности, обществу и государству.

Предметом компьютерных преступлений является компьютерная информация (в ст. 272 и 274 УК - «охраняемая законом»).

Компьютерная информация - это информация в оперативной памяти ЭВМ, информация на иных машинных носителях, как подключенных к ЭВМ, так и на съемных устройствах, включая дискеты, лазерные и иные диски. Цена дискеты не имеет никакого отношения к ценности информации, на ней записанной. Хищение дискеты (кроме грабежа и разбоя) влечет административную ответственность за мелкое хищение, что не исключает ответственности за неправомерный доступ к информации, на ней записанной, если виновный при этом умышленно приобретает доступ к информации на дискете.

Компьютерная информация в системе или сети ЭВМ не может существовать иначе как на конкретных ЭВМ, в эту систему или сеть объединенных. Поэтому, например, перехват информации при ее передаче по каналам связи будет неправомерным доступом к информации в ЭВМ, с которой она передается. Компьютерная информация в ЭВМ, в свою очередь, существует только в виде записей на машинных носителях[9].

Поскольку компьютерная информация не существует иначе как в виде записей на компьютерных машинных носителях, необходимо определить, что следует понимать в этом качестве. При этом следует исходить из употребления слов ЭВМ, компьютер в естественном русском языке. Так, очевидно, не может рассматриваться в качестве компьютера калькулятор, и использование чужого калькулятора без разрешения его хозяина не является преступлением. Не будет компьютером и кассовый аппарат, в том числе и оборудованный

---

[7] *Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 17.06.1996. № 25. ст. 2954.*

[8] *Иногамова-Хегай.Л.В. Уголовное право РФ. Особенная часть. – М. 2010.*

[9] *Слыщенков В.А., Левин А.Е. Охрана программ для ЭВМ: в поисках эффективных правовых решений // Юрист. 2010. № 8. С. 8-15.*

электронным запоминающим устройством. В русском языке слова «ЭВМ», «компьютер» употребляются для обозначения «карманных компьютеров» (например, компьютеров для Windows CE, «ньютонов»), персональных компьютеров и компьютеров более высокого уровня. Компьютерами будут и электронные машины, являющиеся неотъемлемой частью какой-либо технической системы (бортовые компьютеры, компьютеры в автоматизированных производствах и т.п.).

Охраняемая законом компьютерная информация - это любая информация, поставленная под защиту закона в связи с обеспечением вещных и обязательственных прав на ЭВМ и компьютерное оборудование, а также в связи с тайной сообщений (ст. 23 Конституции РФ).

Высказано мнение, что охраняемой законом информацией является лишь документированная информация, образующая информационные ресурсы - «объект права собственности» по Федеральному закону от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации»[10]. Вместе с тем данное преступление не является преступлением против собственности, оно посягает на общественную безопасность. Документированная информация составляет лишь незначительную часть охраняемой законом информации. Например, нарушение работы ЭВМ может быть связано с неправомерным доступом к недокументированной информации, причем опасность этого посягательства ничуть не меньше доступа, например, к документированной информации, предоставляемой информационным агентством. Понятие «документированной Информации» и «информационных ресурсов» предусмотрено не в целях защиты общественной безопасности, а в целях охраны интересов лиц и организаций, предоставляющих информацию на возмездной основе, а также в целях организации документооборота в государственных органах и учреждениях.

По тем же причинам нельзя отожествлять «с охраняемой законом информацией» и «информационные ресурсы ограниченного доступа», указанные в Федеральном законе об информации, информатизации и защите информации.

Нельзя ограничивать пределы «охраняемой законом информации» и исключительно программами для ЭВМ и базами данных. Но охрана авторских прав не исключает иных объектов правовой защиты. Неправомерным, например, будет и доступ в отношении текстового файла, не входящего в какую-либо базу данных.

---

[10] *Иногамова-Хегай.Л.В. Уголовное право РФ. Особенная часть. – М. 2010.*

Не ограничивается круг охраняемой законом информации и сведениями, составляющими государственную, коммерческую, профессиональную, личную или семейную тайны.

Объективная сторона компьютерных преступлений характеризуется как действие (бездействие), связанное с использованием компьютерных систем и сетей, причинившее вред личности, обществу и государству или способное причинить такой вред.

Компьютерные преступления имеют материальные составы (исключением является преступление с формальным составом, предусмотренное ч. 1 ст. 273 УК: создание, использование и распространение вредоносных программ для ЭВМ)[11].

Субъективная сторона компьютерных преступлений характеризуется как умышленной, так и неосторожной виной. Некоторые квалифицированные составы преступлений предусматривают только неосторожную форму вины.

Субъект компьютерного преступления - вменяемое лицо, достигшее возраста 16 лет. В ст. 274 и в ч. 2 ст. 272 УК формулируются признаки специального субъекта: лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен НЦБ более чем 100 стран[12].

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы **Q**. Для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

- **QA - Несанкционированный доступ и перехват**
- **QAH** - компьютерный абордаж
- **QAI** - перехват
- **QAT** - кража времени
- **QAZ** - прочие виды несанкционированного доступа и перехвата
- **QD - Изменение компьютерных данных**
- **QUL** - логическая бомба
- **QDT** - троянский конь

---

[11] *Слыщенков В.А., Левин А.Е. Охрана программ для ЭВМ: в поисках эффективных правовых решений // Юрист. 2010. № 8. С. 8-15.*

[12] *Юрлов И.А. Проблемы правового регулирования оборота компьютерных программ // Правовые вопросы связи. 2010. № 2. С. 12 - 14.*

- **QDV** - компьютерный вирус
- **QDW** - компьютерный червь
- **QDZ** - прочие виды изменения данных
- **QF - Компьютерное мошенничество**
- **QFC** - мошенничество с банкоматами
- **QFF** - компьютерная подделка
- **QFG** - мошенничество с игровыми автоматами
- **QFM** - манипуляции с программами ввода-вывода
- **QFP** - мошенничества с платежными средствами
- **QFT** - телефонное мошенничество
- **QFZ** - прочие компьютерные мошенничества
- **QR - Незаконное копирование**
- **QRG** - компьютерные игры
- **QRS** - прочее программное обеспечение
- **QRT** - топография полупроводниковых изделий
- **QRZ** - прочее незаконное копирование
- **QS - Компьютерный саботаж**
- **QSH** - с аппаратным обеспечением
- **QSS** - с программным обеспечением
- **QSZ** - прочие виды саботажа
- **QZ - Прочие компьютерные преступления**
- **QZB** - с использованием компьютерных досок объявлений
- **QZE** - хищение информации, составляющей коммерческую тайну
- **QZS** - передача информации конфиденциального характера
- **QZZ** - прочие компьютерные преступления

Кратко охарактеризуем некоторые виды компьютерных преступлений согласно приведенному кодификатору.

Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений[13]:

QAH – «Компьютерный абордаж» (хакинг - hacking): доступ в компьютер или сеть без нрава на то. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

---

[13] *Юрлов И.А. Проблемы правового регулирования оборота компьютерных программ // Правовые вопросы связи. 2010. № 2. С. 26.*

QAI - перехват (interception): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственною подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

- *«Жучок»* (bugging) - характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;
- *«Откачивание данных»* (data leakage) - отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;
- *«Уборка мусора»* (scavening) - характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины;
- метод следования *«За дураком»* (piggbacking), характеризующий несанкционированное проникновение, как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;
- метод «*За хвост»* (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;
- метод «*Неспешного выбора»* (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно

читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;

- метод «*Поиск бреши»* (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;
- метод «*Люк»* (trapdoor), являющийся развитием предыдущего. В найденной «бреши» программа «разрывается» и туда вставляется определенное число команд. По мере необходимости «люк» открывается, а встроенные команды автоматически осуществляют свою задачу;
- метод «*Маскарад»* (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;
- метод «*Мистификация»* (spoofing), который используется при случайном подключении «чужой» системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

QAT - кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

Изменение компьютерных данных (QD) включает в себя следующие виды преступлений:

QDL/QDT - логическая бомба (logic bomb), троянский конь (trojan horse): изменение компьютерных данных без права на то, путем внедрения логической бомбы или троянского коня.

Логическая бомба заключается в тайном встраивании в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь - заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

QDV - вирус (virus): изменение компьютерных данных или программ, без права на то, путем внедрения или распространения компьютерного вируса.

Компьютерный вирус - это специально написанная программа, которая может «приписать» себя к другим программам (т.е. «заражать» их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере.

Процесс заражения компьютера программой-вирусом и его последующее лечение имеют ряд черт, свойственных медицинской практике. По крайней мере, эта терминология весьма близка к медицинской:

- *резервирование* - копирование FAT, ежедневное ведение архивов измененных файлов - это самый важный и основной метод защиты от вирусов. Остальные методы не могут заменить ежедневного архивирования, хотя и повышают общий уровень защиты;
- *профилактика* - раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение дисков на «непотопляемые отсеки» - зоны с установленным режимом «только для чтения», хранение неиспользуемых программ в архивах, использование специальной «инкубационной» зоны для записи новых программ с дискет, систематическая проверка BOOT-сектора используемых дискет и др.;
- *анализ* - ревизия вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическое использование контрольных сумм при хранении и передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами по меньшей мере на известные виды компьютерных вирусов и в течение определенного времени за ней должно быть организовано наблюдение;
- *фильтрация* - использование резидентных программ типа FluShot Plus, MaceVaccinee и других для обнаружения попыток выполнить несанкционированные действия;
- *вакцинирование* - специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса, для определения заряжения программы или всего диска;
- *терапия* - деактивация конкретного вируса п отраженных программах с помощью специальной антивирусной программы или восстановление первоначального состояния программ путем уничтожения всех экземпляров вируса в каждом из зараженных файлов или дисков с помощью программы-фага[14].

Понятно, что избавится от компьютерного вируса гораздо сложнее, чем обеспечить действенные меры по его профилактике.

QDW - червь: изменение компьютерных данных или программ, без права на то, путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

---

[14] *Юрлов И.А. Проблемы правового регулирования оборота компьютерных программ // Правовые вопросы связи. 2010. № 2. С. 32.*

Компьютерные мошенничества (QF) объединяют в своем составе разнообразные способы совершения компьютерных преступлений:

QFC - компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

QFF - компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.).

QFG - мошенничества и хищения, связанные с игровыми автоматами.

QFM - манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами. В этот вид компьютерных преступлений включается метод Подмены данных кода (data diddling code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

QFP - компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всех преступлений, связанных с использованием ЭВМ.

QFT - телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

Незаконное копирование информации (QR) составляют следующие виды компьютерных преступлении:

QRG/QRS - незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом.

QRT - незаконное копирование топографии полупроводниковых изделий: копирование, без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изде-лия, произведенного с использованием данной топографии.

Компьютерный саботаж (QS) составляют следующие виды преступлений[15]:

QSH - саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

---

[15] *Юрлов И.А. Проблемы правового регулирования оборота компьютерных программ // Правовые вопросы связи. 2010. № 2. С. 37.*

QSS - компьютерный саботаж с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

Компьютерные программы - относительно новый объект охраны, поскольку массовое производство персональных компьютеров, разработка и распространение компьютерных программ для них начались лишь в конце XX в. Российское законодательство в сфере регулирования такого института гражданского права, как авторские права, несмотря на принятие части четвертой Гражданского кодекса Российской Федерации (далее - часть IV ГК РФ), на сегодняшний день не свободно от недостатков и нуждается в дальнейшем совершенствовании[16].

В Концепции развития гражданского законодательства Российской Федерации справедливо отмечается, что российское гражданское законодательство должно соответствовать современному уровню развития техники, стимулируя разработку и широкое использование новых технологий при одновременном обеспечении защиты интересов правообладателей.

На отношения, возникающие при создании и использовании результатов интеллектуальной деятельности, и в частности - программ для ЭВМ, распространяются общие положения ГК РФ. И здесь существует одна важная проблема. Статья 129 ГК РФ говорит нам об оборотоспособности объектов гражданских прав. В связи с принятием части IV ГК РФ в эту статью был введен п. 4, который закрепляет, что результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации **не могут отчуждаться** или иными способами переходить от одного лица к другому, а в гражданском обороте участвуют только права и материальные носители. Получается, что результаты интеллектуальной деятельности как бы «мертвые». Абсурдность данного положения Гражданского кодекса видна сразу. Как могут в гражданском обороте участвовать только права без самих объектов? Российские ученые справедливо указывают на это. В частности, В.С. Толстой справедливо отмечает, что «возможно понять, как происходит процедура передачи прав на интеллектуальный продукт без предоставления самого продукта. Допустим, автор приходит в издательство и сообщает, что у него имеется оригинальная идея, которую он предлагает приобрести. В ответ на просьбу будущего пользователя познакомить его с идеей автор заявляет, что идея его неотчуждаема и он ведет речь только о передаче имущественных (исключительных) прав на нее (и ссылается на п. 4 ст. 129). Прямо говоря, посетитель издательства предлагает кота в мешке. Ситуация на грани абсурда. Любая идея

---

[16] *Юрлов И.А. Проблемы правового регулирования оборота компьютерных программ // Правовые вопросы связи. 2010. № 2. С. 12 - 14.*

может быть отчуждена и на самом деле отчуждается путем описания ее общепринятыми способами и передачи материального носителя с таким описанием. Если идея не отчуждена, не выражена в материальном носителе, она не является предметом правоотношений».

Довольно часто у пользователя программ для ЭВМ возникает вопрос о том, что следует считать началом вступления лицензионного соглашения в силу. Большинство правообладателей в договоре указывают, что договор вступает в силу с момента заключения данного соглашения путем нажатия кнопки «принять» либо «я согласен», однако некоторые правообладатели указывают, что данный договор вступает в силу с момента вскрытия упаковки либо загрузки файла из сети Интернет. Это прямо противоречит сущности договора, определяемой ст. 432 ГК РФ (договор считается заключенным, если между сторонами, в требуемой в подлежащих случаях форме, достигнуто соглашение по всем существенным условиям договора) как взаимное соглашение сторон. В связи с этим возникает проблема: как может быть заключен договор стороной (пользователем), когда она еще не знала ни о существовании, ни о содержании лицензионного соглашения. Хотелось бы отметить, что согласно ст. 1235 ГК РФ лицензионный договор заключается в письменной форме[17].

При рассмотрении данной проблемы возникает один очень важный вопрос: применяется ли к лицензионным договорам Закон РФ «О защите прав потребителей»?

В преамбуле Закона РФ «О защите прав потребителей»[18] говорится, что «настоящий Закон регулирует отношения, возникающие между потребителями и изготовителями, исполнителями, импортерами, продавцами при продаже товаров (выполнении работ, оказании услуг), устанавливает права потребителей на приобретение товаров (работ, услуг) надлежащего качества и безопасных для жизни, здоровья, имущества потребителей и окружающей среды, получение информации о товарах (работах, услугах) и об их изготовителях (исполнителях, продавцах), просвещение, государственную и общественную защиту их интересов, а также определяет механизм реализации этих прав». А ведь отношения по лицензионному договору возникают между правообладателем и пользователем, а не между продавцом и пользователем. Ведь сторонами лицензионного договора являются не продавец (производитель) и покупатель, а лицензиар и лицензиат, и в данном случае «товар» не продается лицензиату, а лишь предоставляется право его использования.

---

[17] Слыщенков В.А., Левин А.Е. Охрана программ для ЭВМ: в поисках эффективных правовых решений // Юрист. 2010. № 8. С. 8-15.

[18] Закон РФ от 07.02.1992 № 2300-1 О защите прав потребителей // Российская газета. № 8. 16.01.1996.

В результате можно сделать вывод, что Закон РФ «О защите прав потребителей» на лицензионные договоры не распространяется.

Следующая группа проблем - проблемы, связанные с копированием программ для ЭВМ. В ст. 1280 ГК РФ законодатель закрепил за пользователями программ для ЭВМ право на создание одной резервной копии. Однако правообладатели в лицензионных соглашениях на использование программ для ЭВМ зачастую прямо запрещают копирование, даже создание резервных копий. Кроме того, многие разработчики программ для ЭВМ и правообладатели устанавливают на материальный носитель помимо самой программы систему защиты, которая в большинстве случаев препятствует и не дает возможности созданию одной резервной копии.

В настоящее время наиболее остро стоит вопрос о распространении компьютерных программ через Интернет, а именно - через файлообменные сети. Посредством файлообменных сетей пользователи могут предоставлять в общий доступ файлы, находящиеся на их компьютерах. Приведем практический пример: существует определенный сервер в Интернете, так называемый торрент-трекер (например, широкоизвестный торрент-трекер HYPERLINK «http://www.torrents.ru/»). На этом торрент-трекере пользователи размещают информацию о различных файлах (компьютерных программах, музыкальных файлах и т.д.), но сами файлы находятся на компьютерах пользователей. В итоге нарушают исключительные права не владельцы сервера (торрент-трекера), а пользователи. В Концепции развития гражданского законодательства Российской Федерации справедливо отмечается, что одним из важнейших вопросов, без решения которого невозможно обеспечить эффективную защиту результатов интеллектуальной деятельности в информационно-телекоммуникационных сетях, является определение условий привлечения к ответственности лиц, обеспечивающих доступ к информационно-телекоммуникационной сети, функционирование ресурсов в сети и размещение на них соответствующих объектов (провайдеров)[19].

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

---

[19] *Юрлов И.А. Проблемы правового регулирования оборота компьютерных программ // Правовые вопросы связи. 2010. № 2. С. 12 - 14.*

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов РФ при создании информационных систем и их эксплуатации;

5) обеспечение безопасности РФ при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Согласно законодательству РФ - защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации.

Правовые механизмы и процедуры, обеспечивающие реализацию конституционных норм в сфере информационных отношений, детализированы в нормах законодательства: ФЗ «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О средствах массовой информации» и других регулирующих отношения по использованию информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством РФ, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации включает:

1. Нарушение требований ФЗ «Об информации, информационных технологиях и о защите информации» влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством РФ требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

В соответствии с предписаниями ФЗ «Об информации, информатизации и защите информации» целями защиты информационной сферы являются:

– предотвращение утечки, хищения, утраты, искажения, подделки информации;

– предотвращение угроз безопасности личности, общества, государства;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные

системы, обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

В результате в этой области можно выделить три основных направления правовой защиты объектов в информационной сфере (правового обеспечения информационной безопасности).

Защита чести, достоинства и деловой репутации граждан и организаций; духовности и интеллектуального уровня развития личности; нравственных и эстетических идеалов; стабильности и устойчивости развития общества; информационного суверенитета и целостности государства от угроз воздействия вредной, опасной, недоброкачественной информации, недостоверной, ложной информации, дезинформации, от сокрытия информации об опасности для жизни личности, развития общества и государства, от нарушения порядка распространения информации.

Защита информации и информационных ресурсов, прежде всего, ограниченного доступа (все виды тайн, в том числе и личной тайны), а также информационных систем, информационных технологий, средств связи и телекоммуникаций от угроз несанкционированного и неправомерного воздействия посторонних лиц.

Защита информационных прав и свобод (право на производство, распространение, поиск, получение, передачу и использование информации; права на интеллектуальную собственность; права собственности на информационные ресурсы и на документированную информацию, на информационные системы и технологии) в информационной сфере в условиях информатизации.

Таким образом, нормы, регулирующие оборот компьютерных программ, нечетко регулируют вопросы, связанные с их созданием, распространением и использованием. В связи с вышеуказанными проблемами законодателю необходимо развивать правовые нормы части IV ГК РФ, направленные на регулирование программ для ЭВМ и музыкальных произведений.

2. ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ.

Под противодействием компьютерной преступности следует понимать систему общесоциальных, специально-криминологических и индивидуальных мер, направленных на выявление, нейтрализацию и компенсацию ее причин и условий. Определяющими целями предупреждения этого типа преступности выступают выработка оптимального механизма социального контроля над преступлениями с использованием компьютерной техники; установление контроля в области высоких технологий и обеспечения информационной безопасности как общества в целом, так и отдельной личности. Важно отметить, что профилактика преступлений, совершаемых в сфере использования компьютерных технологий, в настоящий момент выступает как важный элемент всей системы социального контроля над преступностью, так как она затрагивает в том числе и аспекты предупреждения иных преступлений, например терроризма, расизма, национализма, детской порнографии и т.д. В этой связи в дополнение к Конвенции о киберпреступности от 23 ноября 2001 г. Советом Европы разработан специальный протокол, обязывающий подписавшие его страны «принять необходимые законодательные меры для борьбы с использованием информационных технологий в создании и распространении материалов расистского, враждебного или дискриминирующего содержания»[20].

В материалах X Конгресса ООН по предупреждению преступности и обращению с правонарушителями отмечается: «Для эффективного предупреждения киберпреступности и борьбы с ней необходим согласованный международный подход на различных уровнях. На внутреннем уровне для расследования киберпреступлений требуется надлежащий персонал, специальный опыт, знания и процедуры. Государствам настоятельно рекомендуется изучить механизмы, позволяющие обеспечить своевременную и четкую защиту данных, содержащихся в компьютерных системах и сетях, на тот случай, если данные потребуются в качестве доказательства в процессуальных действиях. На международном уровне для расследования киберпреступлений необходимы оперативные действия, опирающиеся на координацию усилий национальных правоохранительных органов и принятие соответствующего юридического основания»[21].

Масштабность угрозы киберпреступности в глобализирующемся мире настоятельно требует объединения усилий всего мирового сообщества. Конвенция о киберпреступности от 23 ноября 2001г. предлагает странам-участницам вносить в национальное законодательство единую систему норм об уголовной ответственности за преступления в сфере

---

[20] *Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. М., 2009. С. 184.*

[21] *Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями: Сб. документов. М., 2001. С. 249.*

кибернетического пространства. По существу, предусматривается два блока деяний: правонарушения, направленные против компьютерной информации (как предмета преступного посягательства), и деяния, предметом посягательств которых являются иные охраняемые законом блага, а компьютерные технологии и информация используются при этом как средство, орудие совершения преступления или составляют другой элемент объективной стороны состава преступления. К первому блоку относятся следующие преступления: противозаконный доступ - ст. 2 (имеется в виду доступ без права на него, совершенный в обход мер безопасности); противозаконный перехват данных - ст. 3; нарушение целостности данных - ст. 4; вмешательство в функционирование системы - ст. 5; противоправное использование устройств - ст. 6 (производство, продажа и т.п. устройств, разработанных или адаптированных для совершения преступлений, предусмотренных ст. ст. 2 - 5, а также паролей, кодов доступа и т.п., с помощью которых может быть получен доступ к компьютерной системе с целью совершения преступлений, предусмотренных ст. ст. 2 - 5). Ко второму блоку относятся: подлог с использованием компьютеров - ст. 7; мошенничество с использованием компьютеров - ст. 8; правонарушения, связанные с детской порнографией, - ст. 9; правонарушения, связанные с нарушением авторского права и смежных прав, - ст. 10. Отдельно говорится об ответственности компании (юридического лица), в пользу которой физическое лицо совершило преступление (ст. 12 Конвенции). Содержание приведенной выше Конвенции в полной мере отвечает реалиям XXI в. Считаем необходимым присоединиться к рекомендациям отечественных исследователей проблемы киберпреступности о необходимости ее ратификации Российской Федерацией[22].

Среди правовых мер профилактики компьютерных преступлений центральное место занимают меры по совершенствованию законодательства. Среди них прежде всего хотелось бы обратить внимание на необходимость декриминализации преступления, предусмотренного ст. 274 УК РФ, так как она криминологически не обоснована (в силу отсутствия должной степени общественной опасности и распространенности названного в ней деяния).

Требует дальнейшего совершенствования содержание диспозиций статей УК РФ, устанавливающих уголовную ответственность за компьютерные преступления. Так, по нашему мнению, нуждается в законодательном закреплении дефиниция предмета компьютерного преступления – «компьютерная информация». Помимо этого, есть необходимость в расширении содержания предмета за счет отнесения к нему также и компьютерных услуг. Требуют уточнения и квалифицирующие признаки компьютерных

---

[22] *Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. Ю.В. Гаврилина. М., 2009. С. 71.*

преступлений. Существует необходимость в закреплении таких квалифицирующих признаков неправомерного доступа к компьютерной информации, как «корыстная заинтересованность», «причинение по неосторожности тяжких последствий».

Следует отметить, что для достижения необходимого результата в деле предупреждения преступлений невозможно ограничиться одними только правовыми мерами сдерживания[23]. Еще на рубеже столетия Генеральной прокуратурой России совместно с МВД, ФСБ, ФСНП и ФАПСИ был разработан план действий, включающий в себя следующие мероприятия:

1. Разработка процедуры взаимодействия правоохранительных и иных заинтересованных министерств и ведомств Российской Федерации, а также обмена информацией в борьбе с использованием высоких технологий в преступных целях.

2. Осуществление анализа прокурорско-следственной практики по делам о преступлениях в сфере высоких технологий и создание на его основе методических рекомендаций для работы на местах.

3. Подготовка методических рекомендаций по выявлению, предупреждению, раскрытию преступлений в сфере высоких технологий.

4. Создание в составе экспертно-криминалистических учреждений подразделений для производства экспертиз по делам о преступлениях в сфере высоких технологий.

5. Осуществление анализа действующего законодательства РФ по рассматриваемой проблеме с целью подготовки по его результатам проекта соответствующих законодательных актов, в том числе о внесении дополнений и изменений в это законодательство.

6. Подготовка проекта закона о дополнении санкций ст. ст. 272-274 УК РФ положениями, позволяющими осуществлять конфискацию технических средств, программного обеспечения и накопленной информации, использовавшихся в преступной деятельности.

7. Создание межведомственного центра для проведения исследований и экспертиз при расследовании преступлений, совершенных с использованием компьютерных и информационных систем, сертификации компьютерных и информационных систем на предмет достоверности и полноты данных протоколов регистрации пользователей и другой служебной информации; обучения сотрудников правоохранительных органов методике изъятия и обеспечения сохранности доказательственной базы таких преступлений.

---

[23] *Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М., 2006. С. 111*

8. Организация обучения необходимого числа сотрудников для решения задач борьбы с преступностью в сфере высоких технологий и оказания помощи правоохранительным органам других стран[24].

Приведенный перечень достаточно полно отражает специально-криминологический уровень противодействия компьютерной преступности. Однако, к сожалению, и по сей день многие из перечисленных мероприятий остались не воплощенными в жизнь.

Подводя итог, отметим, что в России назрела острая необходимость в разработке концепции информационной безопасности с обязательным планированием и программированием мер противодействия компьютерной преступности, которые должны охватывать общефедеральный и региональный уровни. Важной составляющей противодействия рассматриваемому типу преступности выступает виктимологический аспект. Интересен в этой связи опыт некоторых зарубежных государств (ФРГ, Франция, США и др.) по созданию общегосударственной системы уведомлений о готовящихся атаках хакеров. Перспективной является идея о предоставлении налоговых льгот пользователям, осуществившим обновление системы защиты информации.

Роль общепревентивных мер в сфере предупреждении совершения преступлений в сфере информационных технологий более значительна, чем уголовно-правовые запреты по следующим причинам:

- низкая эффективность деятельности правоохранительных органов в выявлении и расследовании преступлений данной категории;

- в свою очередь повышение активности правоохранительных органов в данном направлении создает угрозу правам и свободам граждан;

Правоведами были изучены и виктимологические аспекты проблемы. В.А.Бессонов отмечает 7 групп факторов совершения «компьютерных преступлений»:

- неконтролируемый доступ сотрудников к компьютерам;

- бесконтрольные действия обслуживающего персонала;

- несовершенство программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

- несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по его биометрическим параметрам;

---

[24] *Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия. Курган, 2009.*

- отсутствие лица, отвечающего за режим секретности и конфиденциальности компьютерной информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

- отсутствие системного допуска сотрудников к документации строгой финансовой отчетности, в том числе, находящейся в форме машинной информации;

- отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации. Аналогичные факторы приводит В.Б. Вехов и С.Ю. Бытко[25].

Исходной предпосылкой рассуждений о мерах общей превенции является положение о невозможности для государства регулировать деятельность граждан в сети Интернет.

В настоящее время сеть Интернет представляет огромную компьютерную инфраструктуру, состоящую из более чем 100 млн. хостов, расположенных по всей территории Земли. В настоящее время ни одно государство мира не в состоянии полностью контролировать сеть Интернет (как всю сеть, так и сервера, физически расположенные на его территории). Исключение составляют такие страны, как КНР, КНДР, где на законодательном уровне установлены права пользователей компьютеров по получению информации. Однако и в этом случае нельзя говорить о полном контроле над сетью Интернет, а лишь о потенциально возможном применении к не соблюдающим запретов гражданам мер устрашения.

В сети Интернет не существует абсолютно надежных средств защиты от преступников (это вызвано в первую очередь архитектурными особенностями построения сети). Вот как пишут об этом авторы книги «Компьютерные преступления»: «Лишь немногие организации могут позволить себе полную защиту компьютеров от всех видов риска (если такая вообще возможна!). Поэтому приходится выбирать между стоимостью различных типов защиты и рисками, возникающими при ее отсутствии». Для коммерческих организаций, осуществляющих свою деятельность при помощи сети Интернет, допустимым может являться такой уровень безопасности, при котором затраты преступников на взлом защиты превышают потери от утраты потерпевшим защищаемой информации. Однако для объектов повышенной опасности такой критерий применять нельзя. Поэтому целесообразно законодательно запретить соприкосновение сетей (или одиночных ЭВМ) данных объектов с сетью Интернет. Необходимо развивать ведомственные сети отдельно от общегражданских сетей.

---

[25] *Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. Ю.В. Гаврилина. М., 2009. С. 71.*

Представляется целесообразным законодательно обязать лиц, занимающиеся информационной безопасностью объектов государственной важности, проходить специальную подготовку и сдавать экзамены на допуск к такой ответственной работе. Недостаточная квалификация либо халатность таких лиц является основной причиной крупного ущерба.

Серьезным недостатком в общей превенции преступлений, совершаемых с использованием информационных технологий, является недостаточное внимание представителей органов государства к отечественным производителям ПО. Несмотря на декларируемую в «Доктрине информационной безопасности Российской Федерации» поддержку отечественным программистам на деле получается обратное. Представляется целесообразным на уровне федерального законодательства закрепить преимущество отечественных производителей программного обеспечения при закупках программ государственными организациями.

Эффективность уголовно-правовой охраны общественных отношений обеспечивается, в первую очередь, своевременным выявлением угроз этим отношениям и криминализацией наиболее общественно опасных посягательств, а также декриминализацией деяний, которые утратили свою общественную опасность.

Процесс криминализации (декриминализации) всегда сопровождается оценкой множества обстоятельств. Главным основанием криминализации является общественная опасность деяния. Однако это не единственный фактор. В теории уголовного права нет исчерпывающего перечня обстоятельств, которые порождают необходимость криминализации определенного вида деяний.

В.М.Коган называет ряд обстоятельств, которые учитываются при установлении, изменении либо отмене уголовной ответственности за совершение общественно опасных деяний: 1) объективные закономерности жизни общества; 2) материальные ресурсы для реализации уголовно-правового воздействия; 3) социальные последствия уголовного наказания; 4) нравственные представления общества; 5) возможность стимулирования должного поведения уголовно-правовыми средствами; 6) возможность действенного контроля за поведением обязанных лиц; 7) уровень развития науки и техники; 8) общие законы управления. «Попытки классифицировать такого рода обстоятельства показывают, что при наличии общественной опасности, порождающей потребность в уголовно-правовом воздействии, установление, изменение либо отмена уголовно-правового запрета связаны с

его допустимостью в политическом, нравственном и юридическом плане, а также с правовыми, организационными и экономическими возможностями его реализации»[26].

Из приведенных выше мнений можно сделать вывод о том, что большинство ученых подходят комплексно к этой проблеме и включают в круг рассмотрения достаточно обширный перечень необходимых условий для криминализации общественно опасных деяний. В то же время, все эти точки зрения объединяет некоторая неполнота, поскольку акцент делается на объективных факторах криминализации. Неосвещенным остается гуманистический аспект проблемы. Между тем, эти вопросы, по нашему мнению, важны для разработки эффективных уголовно-правовых норм в соответствии с принципами справедливости и гуманизма.

На практике же мы наблюдаем тенденцию к ужесточению уголовной репрессии за подобные посягательства и расширение круга криминализируемых деяний. В различных уголовно-правовых и криминологических исследованиях, которые посвящены преступлениям в сфере компьютерной информации стало традицией формулировать новые составы «компьютерных» преступлений и вносить предложения о необходимости повышения верхних пределов санкций данных норм.

Основополагающим критерием для ужесточения наказания авторы считают значительную общественную опасность таких деяний, однако фактически сводят ее лишь к размеру причиняемого вреда. Кроме того, вызывает сомнение и конкретное определение сроков лишения свободы за совершение деяний в сфере компьютерной информации. По нашему мнению, при определении размера наказания за конкретное деяние необходимо провести сравнительный анализ общественной опасности интересующего нас деяния, и того, которое уже закреплено в УК РФ. После того, как будет установлено, что деяние обладает общественной опасностью, сопоставимой с общественной опасностью какого-то другого преступления, можно сделан вывод о том, что и санкции за совершение таких деяний должны быть сопоставимыми.

Наиболее ярким примером переоценки общественной опасности является повышенная ангажированность вирусных программ. Ряд авторов приравнивает использование компьютерных вирусов к таким преступлениям, как терроризм, и утверждает, что компьютерные вирусы могут роковым образом влиять на здоровье пользователя путем определенной комбинации излучений дисплея. Однако научного обоснования данных выводов не существует.

---

[26] *Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. Ю.В. Гаврилина. М., 2009. С. 75.*

В базе данных антивирусной программы AVP хранятся данные о более чем 90000 компьютерных вирусов. Однако, лишь около 1000 из них заражали реальный компьютер, в настоящее время таких вирусов циркулирует в мире не более 150. Остальные десятки тысяч вирусов являются единичными экземпляры (большинство из них штаммы), которые рассылаются в порядке взаимообмена антивирусными компаниями, которые больше нигде не появляющиеся.

О завышении в общественном сознании общественной опасности создания и распространения вредоносных программ свидетельствует и крайне малое количество уголовных дел, возбужденных по ст. 273 УК РФ. При этом обвиняемые, как правило, занимались распространением компьютерных компакт-дисков, среди которых оказались и диски с вредоносными программами. Лица же, которые непосредственно создавали такие программы к уголовной ответственности не привлекались. Характерно, что вредоносные программы в большинстве своем предназначены для использования в сети Интернет, то есть для тех лиц, которые имеют возможность выхода в сеть Интернет. Как следствие, крайне сомнительным представляется мнение о наличии значительной общественной опасности в действиях продавца компакт-дисков, поскольку в сети Интернет совершенно бесплатно и безнаказанно можно найти большое количество данных программ. Поэтому способ их распространения на компакт-дисках является далеко не основным и не влияет на количество создаваемых компьютерных вирусов.

Существенно затрудняет (иногда делает невозможным) расследование преступлений в сфере компьютерной информации доказывание самого события преступления. Очень часто основными доказательствами вины служат log-файлы, которые создаются рядом программ (например, броузерами Internet Explorer или Opera). Эти файлы содержат в себе полный протокол сеанса работы в сети Интернет, IP-адрес соединений. Большинство злоумышленников знает об этой программной особенности и избавляется от нее путем удаления log-файлов.

На основании вышеизложенного можно сделать ряд выводов. Во-первых, правоохранительные органы могут противодействовать лишь лицам, которые плохо разбираются в современных компьютерных технологиях.

Во-вторых, эффективно противодействовать преступлениям в сфере информационных технологий можно лишь в тех случаях, когда удается установить реальные данные злоумышленника (номер телефона, с которого осуществлялся выход в сеть Интернет, либо если обстоятельства дела указывают на конкретное лицо).

Наиболее распространенным в уголовной практике примером подобного рода является незаконный доступ в сеть Интернет с использованием похищенных паролей. Как

правило, доступ в сеть Интернет осуществляется с телефонной линии и через конкретного провайдера (у которого зарегистрирован похищенный логин и пароль), то естественной привязкой к личности преступника является номер телефона, с которого он осуществляет этот доступ. Провайдер, как правило, самостоятельно определяет номер телефона (у всех провайдеров установлены АОНы) и обращается в правоохранительные органы, которые по известному номеру телефона устанавливают адрес преступника. Данные случаи легко расследуются, и составляют наиболее значительный процент дел о преступлениях в сфере компьютерной информации. Практически все уголовные дела по преступлениям в сфере компьютерной информации были возбуждены именно по этим фактам. Несомненно, прирост дел по ст. 272-274 УК РФ и в дальнейшем будет происходить лишь за счет подобных случаев.

При совершении мошеннических действий с кредитными карточками несложно перевести деньги со счетов других граждан. Самым уязвимым звеном является процедура обналичивания незаконно переведенных денег, то есть именно тот момент, когда возможно увязать незаконные действия с личностью конкретного физического лица.

В-третьих, при совершении ряда посягательств, реализованных исключительно в «виртуальном» пространстве и причиняющих отрицательные последствия неопределенному кругу лиц (например, хакерские атаки на сайты компаний, имеющих свои сервера или страницы в сети Интернет), вероятность установить преступников незначительна и не позволяет говорить о неотвратимости уголовного наказания. В подобных случаях существование норм, устанавливающих уголовную ответственность за такие преступления, является декларацией общего отрицательного отношения института государства к таким поступкам и не оправдывает своего предназначения. Необоснованное ужесточение наказания в таких условиях равносильно признанию государством собственной беспомощности в борьбе с «компьютерными» посягательствами.

В-четвертых, имеется российская и зарубежная статистика, показывающая, что большую часть преступлений в сфере компьютерной информации причиняют действия сотрудников, направленные против своих организаций. По данным комиссии ООН по преступности и уголовной юстиции примерно 90% экономических компьютерных посягательств были совершены работниками самих же пострадавших компаний.

В-пятых, одним из основных факторов, способствующих распространению преступлений, совершаемых в сфере информационных технологий, является повышенная уязвимость программ, используемых большинством пользователей средств компьютерной техники к посторонним воздействиям. Использование известных «дыр» в защите программного обеспечения является основой большинства успешных компьютерных атак.

Показательно, что при постоянном появлении сообщений об обнаружении новых проблем в системах безопасности и способах их устранения (как правило, так называемые патчи (заплатки), большинство пользователей ими пренебрегают, предоставляя преступникам широчайшее поле деятельности.

Возникает ситуация, при которой преступники, использующие «дыры» в программном обеспечении преследуются в уголовном порядке, а производители программ не несут никакой ответственности за допущенные ошибки.

Считаем, что исправление такой ситуации невозможно одними лишь уголовно-правовыми методами. Практика сохранения уголовно-правового воздействия на преступников при отсутствии каких-либо правовых мер к производителям дефектного программного обеспечения, на наш взгляд, порочна, поскольку не стимулирует производителя к созданию безопасных систем и усугубляет проблемы компьютерной безопасности. В России, не имеющей собственных программных продуктов уровня операционных систем массового использования, складывается ситуация, при которой действующее законодательство фактически поощряет западные компании к продолжению распространения ненадежной операционной системы для компьютеров.

В шестых, низкая эффективность раскрытия посягательств в сфере компьютерной информации, как всегда, порождает у государства соблазн максимально усилить контроль за действиями своих граждан в данной сфере. Это осуществляется в процессе развертывании систем тотального перехвата информации в сети Интернет под различными предлогами (возможность использования информационных технологий преступниками, а в последнее время основным козырем становится необходимость воспрепятствования терроризму). Общей чертой данных технических систем является предоставление спецслужбам права следить за деятельностью своих граждан в сети Интернете, то есть права вмешательства в личную жизнь, при ослаблении судебного контроля над такой деятельностью.

Преступления в сфере компьютерной информации сформулированы в главе 28 УК РФ и включают в себя, как уже говорилось, четыре состава преступления: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных систем (ст. 274 УК РФ) и неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

Неправомерный доступ к компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их

сети, наказуем, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Таким образом криминообразующими (свидетельствующими о достаточной для уровня преступного степени общественной опасности) признаками деяния выступают: 1) неправомерность действий лица, которое осуществляет доступ к чужой информации, на ознакомление с которой оно права не имеет; 2) состоящие в причинной связи с таким поведением лица, наступившие негативные для владельца информации последствия (хотя бы одно из пяти перечисленных выше). Исхода из того, что при неправомерном доступе серьезно нарушаются права лица на обладание информацией и часто причиняется ущерб и самой этой информации, следует признать, что основание для криминализации отклоняющегося поведения, действительно, имело место. Создание новой нормы было необходимо, поскольку другие существующие уголовно-правовые нормы не в полной мере охватывают неправомерный доступ к информации (в частности, в отдельных случаях к виновным возможно применение составов нарушения неприкосновенности частной жизни - ст. 137 УК РФ; нарушения тайны переписки или иных сообщений - ст. 138 УК РФ; незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну - ст. 183 УК РФ; государственной измены и шпионажа - ст. ст. 275,276 УК РФ).

В равной степени можно констатировать наличие основания для криминализации таких действий, как создание, использование и распространение вредоносных программ для ЭВМ. Их общественная опасность очевидна и перерастает ту, которая характерна для административного правонарушения, поскольку лицо не просто предпринимает действия, которые могут причинить вред правоохраняемым интересам других лиц, но делает это целенаправленно, осознавая, что создаваемая или распространяемая программа ведет к несанкционированным и негативным для владельца информации последствиям.

Считаем, что при осуществлении российской криминализации названных двух компьютерных преступлений, в основном, соблюдались и принципы криминализации: достаточной общественной опасности криминализируемых деяний, их относительной распространенности, возможности позитивного воздействия уголовно-правовой нормы на общественно-опасное поведение, преобладания позитивных последствий криминализации, неизбыточности уголовно-правового запрета, своевременности криминализации.

Российский законодатель использует в анализируемом составе несколько криминообразующих признаков сразу: 1) нарушение правил пользования ЭВМ, системой ЭВМ или их сетью - в этом суть отклоняющегося поведения, которое, как мы видели выше, лишено точных границ; 2) последовавшие в результате этого уничтожение, блокирование

или модификация охраняемой законом информации; и 3) причинение существенного вреда. Таким образом, о наличии состава преступления должны свидетельствовать сразу два возможных последствия: первого порядка - в отношении информации, и второго порядка - существенный ущерб, принадлежность и содержание которого в законе не обозначены. В каких отношениях должны находиться между собой названные последствия? Каким образом должна устанавливаться на практике причинная связь? Сколько ее видов должно быть констатировано? Очевидно, должна быть причинная связь между нарушением правил пользования ЭВМ и последствиями первого порядка - в отношении информации. Однако неясно, уничтожение, блокирование или модификация охраняемой законом информации должны стать причиной существенного ущерба, или последний должен быть причинен в результате того же нарушения правил?

Не следует забывать, что после установления причинной связи необходимо установить не менее сложную виновную связь, и, следовательно, с известной корректировкой вновь ответить на те вопросы, которые были поставлены нами выше.

Компьютерные преступления в российском уголовном законодательстве ныне включают в себя преступления трех первых категорий степени тяжести. Неквалифицированный неправомерный доступ к компьютерной информации и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети - преступления небольшой тяжести; эти же преступления с отягчающими обстоятельствами, а равно создание, использование и распространение вредоносных программ для ЭВМ - преступления средней тяжести; квалифицированный состав ст. 273 УК РФ - тяжкое преступление. Таким образом, компьютерные преступления не представлены только особо тяжкими преступлениями. Диапазон наказаний, которые могут быть назначены за компьютерные преступления в России, - достаточно широк: штраф в качестве основного или дополнительного наказания (ст. 272, ч. 1 ст. 273 УК РФ), лишение права занимать определенные должности или заниматься определенной деятельностью (ч. 1 ст. 274 УК РФ), обязательные работы , (ч. 1 ст. 274 УК РФ), исправительные работы (ст. 272 УК РФ), ограничение свободы (ч. 1 ст. 274 УК РФ), арест (ч. 2 ст. 272 УК РФ), лишение свободы (по всем простым и квалифицированным составам, кроме ч. 1 ст. 274 УК РФ). Считаем, что такое разнообразие видов наказаний должно восприниматься, как положительная тенденция, поскольку непосредственно позитивно влияет на дифференциацию и индивидуализацию ответственности.

При решении проблем пенализации следует принимать во внимание характер действий виновного и характер тех последствий, которые наиболее вероятны. Большую наказуемость, или строгость санкций должно влечь отклоняющееся поведение, связанное с насилием, и (или) причиняющее вред жизни или здоровью людей. Это положение особой

аргументации не требует, оно достаточно аксиоматично. Тем не менее, в российском уголовном законодательстве не являются редкостью случаи, когда такое девиантное поведение карается гораздо менее строго, нежели деяния, насильственного характера не носящие, и порождающие последствия другого вида. Сказанное в полной мере можно отнести к составу, предусмотренному ст. 273 УК РФ.

Особое значение имеет координация деятельности субъектов борьбы с компьютерной преступностью в ее предупредительном, карающем и правовосстановительном аспектах. Взаимодействие должно быть основано на четком распределении межведомственных и внутриведомственных компетенций подразделений, осуществляющих борьбу с компьютерной преступностью. Например, следует четко определить поле деятельности в этой сфере подразделений ФСБ и МВД. Так, исключительно подразделения ФСБ должны обеспечивать информационную безопасность объектов их контрразведывательного обеспечения. В свою очередь, к компетенции МВД могут быть отнесены хищения посредством совершения преступлений в сфере компьютерной информации. Межведомственная и внутриведомственная координация деятельности подразделений, осуществляющих борьбу с компьютерной преступностью, и их компетенция должны быть определены как на уровне закона, так и ведомственными и межведомственными документами.

Важно усиление сотрудничества подразделений, осуществляющих борьбу с компьютерной преступностью и субъектами информационного оборота. Объединенное противодействие компьютерным преступлениям может состояться только на основе эффективной и высокопрофессиональной работы подразделений по борьбе с компьютерными преступлениями. Деятельность этих подразделений необходимо обеспечить соответствующей правовой, материальной и кадровой поддержкой государства. Эффективная и высокопрофессиональная деятельность правоохранительных органов должна сочетаться с принципами конфиденциальности, доверительного взаимодействия и гарантиями сохранности государственной, банковской, коммерческой тайны и других ценных сведений.

Учитывая объективно и субъективно сложившуюся на тот момент времени общественно-политическую обстановку, 7 октября 1998 года Управление «Р» было преобразовано в Управление по борьбе с преступлениями в сфере высоких технологий (сокращенно УБПСВТ). В его структуре были выделены три подразделения[27]:

Отдел по борьбе с преступлениями в сфере компьютерной информации;

---

[27] *Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М.: ООО Издательство «Юрлитинформ», 2005. С. 145.*

Отдел по борьбе с преступлениями в сфере телекоммуникаций;

Отдел по борьбе с незаконным оборотом радиоэлектронных (РЭС) и специальных технических средств (СТС).

На уровне областных Управлений органов внутренних дел Российской Федерации до 1999 года были созданы аналогичные структурные подразделения -отделы БПСВТ, имеющие в своем составе три отделения. Первоначально, в их штате, в основном, находились оперативные сотрудники, имевшие техническое образование, что негативно сказывалось на качестве раскрытия и расследования компьютерных преступлений. Кардинально ситуация изменилась в лучшую сторону лишь к 2000 году, когда подразделения на местах были полностью укомплектованы лицами, имеющими высшее и среднее специальное юридическое образование.

В 2002 году Управление БПСВТ было упразднено, а его штаты, структура и материально-техническое обеспечение были переданы Управлению специальных технических мероприятий (УСТМ) МВД России. В настоящее время эти подразделения называются Отделы «К» (по борьбе с компьютерными преступлениями) при УСТМ. В них сохранены профильные отделения по трем направлениям борьбы с компьютерными преступлениями.

Основная тяжесть работы по расследованию компьютерных преступлений падает на специализированные подразделения. Они созданы на уровне Главных и Областных управлений органов внутренних дел всех субъектов Российской Федерации. Следователи органов внутренних дел, входящие в состав таких подразделений, тесно взаимодействуют со специализированными органами дознания - Отделами «К» и ОБЭП. Функции и задачи подразделений «К» МВД России:

Борьба с преступлениями в телекоммуникационных сетях: с радиоэлектронными устройствами - «двойниками»; незаконными междугородними и международными переговорными пунктами, работающими в режиме подмены абонентского номера.

Выявление и пресечение преступлений, связанных с осуществлением электронных платежей в теле- коммуникационных сетях, в т.ч. с использованием пластиковых карт.

Борьба с незаконным оборотом радиоэлектронных средств (РЭС) и специальных технических средств (СТС), в т.ч. выявление и пресечение каналов их контрабандного ввоза, незаконного изготовления, сбыта и использования.

Организация и осуществление радиоэлектронного противодействия незаконно действующим РЭС и СТС.

Ведение мониторинга открытых глобальных и локальных компьютерных сетей, сетей проводной, спутниковой и подвижной радиосвязи, а также персонального радиовызова

абонента (пейджинга) общего пользования с целью добывания информации о правонарушениях и правонарушителях.

Борьба с незаконным оборотом объектов интеллектуальной собственности на электронных (машинных) носителях.

Борьба с преступлениями в сфере компьютерной информации:

- неправомерным доступом к охраняемой законом (конфиденциальной) компьютерной информации (ст. 272 УК РФ);

- созданием, использованием и распространением вредоносных программ для ЭВМ или машинных носителей с такими программами (ст. 273 УК РФ);

- нарушением правил эксплуатации ЭВМ, систем ЭВМ или их сетей (ст. 274 УК РФ).

Особое значение в борьбе с компьютерной преступностью имеет стадия предварительного расследования преступлений в сфере информационных технологий.

Особенности производства неотложных следственных действий при расследовании преступлений, совершаемых в сфере информационных технологий (осмотр, обыск, выемка, судебная экспертиза) Практика борьбы с компьютерной преступностью в Российской Федерации ставит перед правоохранительными органами страны ряд проблемных теоретико-прикладных вопросов, нуждающихся в комплексном разрешении с участием практических работников и представителей юридических, технических и иных отраслей науки.

Для классификации следов преступлений, совершаемых с использованием информационных технологий, которые могут быть обнаружены, зафиксированы и изъяты при проведении следственных действий, мы считаем возможным применить традиционное подразделение следов на следы-отображения, следы предметы и следы-вещества.

Доказательства, связанные с компьютерными преступлениями, и изъятые с места происшествия, могут быть легко изменены, как в результате ошибок при их изъятии, так и в процессе самого исследования. Представление подобных доказательств в судебном процессе требует специальных знаний и соответствующей подготовки. Здесь нельзя недооценивать роль экспертизы, которая может дать квалифицированный ответ на поставленные вопросы.

Однако экспертиза требует определенного времени на ее проведение, а при изъятии компьютерной техники существенным фактором, позволяющим сохранить необходимую доказательную информацию, является неожиданность и оперативность. Именно поэтому изъятие компьютеров и информации приходится проводить силами работников, которые в настоящее время проводят следственные действия. В данном случае следователь не застрахован от ошибок, обусловленных недостаточностью специальных познаний, что потом умело используется защитой в суде.

Производство следственных действий по делам рассматриваемой категории должно осуществляться с участием специалиста в сфере разработки и использования современных информационных технологий. Практика расследования данного вида преступлений показала, что позитивную роль играет участие специалиста в следственном осмотре, обыске и выемке.

Остановимся на некоторых действиях, связанных с осуществлением собирания доказательств из отдельных компьютеров, а также из группы компьютеров, входящих в состав локальной вычислительной сети (ЛВС).

3. ОСОБЕННОСТИ РАБОТЫ С ЭЛЕКТРОННЫМИ НОСИТЕЛЯМИ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ.

К следственным действиям, которые по делам о преступлениях, совершаемых с использованием средств электронно-вычислительной техники, отличаются наибольшей спецификой, относятся:

- осмотр места происшествия;
- осмотр средства вычислительной техники;
- осмотр машинного носителя информации (МНИ);
- осмотр машинного документа;
- обыск и выемка;
- назначение экспертиз.

Проводятся они в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом некоторых особенностей.

Осмотр места происшествия

Следственный осмотр представляет собой обнаружение, восприятие, изучение и фиксацию следователем объектов, имеющих значение для дела, их признаков, свойств, состояния и взаиморасположения. Объектами осмотра по делам данной категории являются место происшествия и его обстановка, отдельные компьютерные средства и комплектующие, иные предметы, документы. Путем осмотра обнаруживается и исследуется значительная часть важнейших следов преступления. Результаты осмотра позволяют следователю правильно определить направление расследования компьютерного преступления, составить себе представление о механизме происшествия, о личности преступника. От качества проведенного осмотра во многих случаях зависит успех расследования. При расследовании

компьютерных преступлений производятся, как правило следующие виды следственного осмотра:

- осмотр места происшествия или помещений, не являющихся местом происшествия;

- осмотр предметов (компьютеров и их комплектующих);

- осмотр документов (описаний к компьютерным системам, производственной документации, документов финансовой отчетности).

Осмотр места происшествия по делам, связанным с использованием информационных технологий - неотложное следственное действие, направленное на установление, фиксацию и исследование обстановки места происшествия, следов преступления и преступника, отобразившихся в компьютерном устройстве или вычислительной сети и иных фактических данных, позволяющих в совокупности с другими доказательствами сделать вывод о механизме компьютерного преступления и иных обстоятельствах расследуемого события.

В соответствии со ст. 177 ч.3 УПК РФ следователь вправе производить осмотр не только в месте производства следственного действия, но и по месту производства следствия, если для осмотра потребуется продолжительное время или осмотр на месте затруднен. В этих случаях в протоколе указываются первые слова текста, последние фразы, отмечается, что данное сообщение скопировано на электронный носитель, указывается ее внешний вид, способ упаковки, вид и текст описка печати. Последующий подробный осмотр изъятой корреспонденции проводится по месту проведения следствия с участием понятых (по возможности тех же) и отражением в протоколе сохранности печати и удостоверительных подписей на упаковке, в которую были помещены машинные носители компьютерной информации.

В случае, если после осмотра следователь придет к выводу о нецелесообразности препятствовать переписке, он может дать указания о направлении ее соответствующему адресату, а также вовсе отменить арест, при этом одновременно уведомляются суд, принявший решение о наложении ареста и прокурор.

Известно, что место происшествия может не совпадать с местом преступления. При этом подразумевается, что преступление могло быть совершено как в месте обнаружения следов, так и в ином месте. Это особенно характерно для преступлений в сфере использования информационных технологий.

Осмотр предметов.

Осмотр компьютерных средств позволяет устанавливать состояние предмета, наименование и назначение, выявить индивидуальные признаки компьютера, дискеты или оптического диска, его дефекты и особенно признаки, свидетельствующие о том, по какому

назначению он использовался и как интенсивно, а также признаки, указывающие на связь предмета, с расследуемым событием. В процессе осмотра компьютерных средств следователь должен сосредоточить свои усилия на выявлении тех следов и признаков, которые впоследствии станут объектами экспертного исследования. Все это возможно только при участии специалиста.

Осмотр документов.

Документы являются источниками и носителями значимой для уголовного дела компьютерной информации. Осмотр документов имеет своей целью выявление и фиксацию таких их признаков, которые придают документам значение вещественных доказательств, а также установление удостоверенных документами или изложенных в них обстоятельств и фактов, имеющих значение для дела. Сделать это необходимо и потому, что программисты часто не надеются на свою память и оставляют записи о паролях, изменениях конфигурации системы, особенностях построения информационной базы компьютера на бумаге.

При осмотре места происшествия в ***состав следственно - оперативной группы*** (СОГ) в зависимости от конкретной следственной ситуации должны входить следующие лица:

- следователь, специализирующийся на расследовании уголовных дел рассматриваемой категории - руководитель СОГ;

- специалист-криминалист, знающий особенности работы со следами преступлений данной категории;

- специалист по СВТ;

-сотрудник Гостехкомиссии России (в случае совершения преступления в отношении юридического лица и/или наличия специальных средств защиты информации и СВТ) или оперативно-технического подразделения правоохранительного органа;

- специалист по сетевым технологиям СВТ (в случае наличия на месте происшествия периферийного оборудования удаленного доступа или локальной компьютерной сети);

- специалист по системам связи (при использовании для дистанционной передачи данных каналов электросвязи);

- оперативные сотрудники (ОУР, ОБЭП, налоговой полиции, ФСБ);

- участковый инспектор, обслуживающий данную территорию;

- инспектор отдела вневедомственной охраны (в случае, когда место происшествия или СВТ, находящееся на нем, являются охраняемыми объектами).

При необходимости для участия в осмотре места происшествия могут быть приглашены и другие незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики, бухгалтеры со знанием СВТ, специалисты

спутниковых систем связи, операторы компьютерных систем и сетей - сотовых, пейджинговых, Интернет и др. - и т.д.).

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано, ***необходимо предварительно провести следующую работу:***

1. С учетом сложившейся следственной ситуации, наметить круг лиц, участвующих в осмотре;

2. Определить последовательность действия лиц при осмотре места происшествия;

3. Пригласить соответствующих квалифицированных специалистов;

4. Перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности;

5. Провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области СВТ и компьютерных технологий, разъяснить их права и обязанности.

Цель осмотра места происшествия - установление конкретного СВТ, выступающего в качестве предмета и/или орудия совершения преступления и имеющего следы преступной деятельности. При производстве следственного действия целесообразно использовать тактический прием «от центра - к периферии», где «центром» (отправной точкой осмотра места происшествия) являются СВТ, находящиеся на месте осмотра.

По прибытию на место происшествия, следователь должен проделать следующую работу:

1. Удалить с места происшествия всех посторонних лиц и организовать его охрану, если этого не было сделано. Обязательной охране подлежат такие объекты:

- территория места происшествия;

- все СВТ, находящиеся на территории (в помещении);

- пункты отключения электропитания СВТ, находящиеся в здании (учреждении, организации, на территории).

Следователю необходимо знать, что к изменению или уничтожению информации (следов) может привести не только работа за пультом управления СВТ (клавиатурой), но и включение-выключение СВТ или разрыв соединения между ними. Поэтому, если на момент производства следственного действия какие-либо СВТ и иные электротехнические приборы и оборудование были включены или выключены, то они должны оставаться в таком состоянии до момента окончания осмотра их специалистом.

2. Опросить потерпевшего, материально ответственное лицо и очевидцев (операторов СВТ) об изменениях, внесенных в обстановку, о категории обрабатываемой

информации (общедоступная или конфиденциальная), а также о действиях потерпевшего до прибытия СОГ. Вопросы необходимо конкретизировать по мере детального осмотра места происшествия, поиска следов и других вещественных доказательств.

В протоколе осмотра следует отразить следующие фактические данные:

- наименование и назначение объекта, где совершено преступление;

- территориальное расположение объекта осмотра (на улице, в помещении, в банке, в магазине, на автостоянке, бензоколонке, станции метро, в ресторане, гостинице, помещении кассы, на складе, вокзале, контрольно-пропускном пункте и т.д.) и его ориентация относительно сторон света;

- ближайшее окружение объекта и подступы к нему - здания, технические сооружения, площади, зоны, участки (производственные, административные, жилые) и расстояние до них; наличие дорог, подъездных путей (в т.ч. и водного транспорта), парковок и автостоянок; наличие линий и пунктов (колодцев, концентраторов, коробов, потерн и т.д.) инженерно-технических коммуникаций (электросвязи, электропередачи, тепло- , водо- и газоснабжения, вентиляции и т.д.);

- технические и конструктивные особенности местности, связанные с установкой и эксплуатацией СВТ (этажность, материал стен и других строительных конструкций, форма строения, наличие дверей, окон, ограждений, фальшполов и подвесных потолков, наличие и фактическое состояние устройств электропитания и др.);

- наличие, внешнее состояние и расположение охраны объекта, специальных защитных и сигнальных устройств от несанкционированного съема и утечки информации - постов охраны, охранно-пожарной сигнализации, контрольно-пропускных пунктов доступа лиц на данную территорию (неавтоматический, полуавтоматический или автоматический), освещения, металлических решеток, штор, жалюзи, рольставен, замков и запорных механизмов, экранов, заземлений, специальных стекол и пленок, генераторов шума, фильтров и т.д.;

- расположение СВТ относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видеонаблюдения, а также других рабочих мест (если таковых несколько в одном помещении);

- расположение в одном помещении вместе с СВТ других электрических устройств и приборов - телефонных и иных аппаратов электросвязи, систем электрочасофикации, оргтехники (ксероксов, аудио-, видеомагнитофонов, автоответчиков, электрических пишущих машинок и т.п.), приборов электроосвещения (настольных, напольных, настенных,

потолочных, подвесных и т.д.), абонентских громкоговорителей, телевизоров и мониторов, радиоприемников и магнитол, электроплиток, печей, чайников, кондиционеров и т. д.;

- наличие в одном помещении со СВТ линий, пунктов, разъемов промежуточных и оконечных устройств систем инженерно-технических коммуникаций (электросвязи, электропередачи, антенны-провода, тепло-, водо- и газоснабжения);

- наличие или отсутствие технических средств сопряжения СВТ с каналами электросвязи и между собой (на это могут указывать кабели и провода, которыми СВТ соединены между собой, а также с аппаратами или линией электросвязи);

- наличие или отсутствие соединений СВТ с оборудованием или вычислительной техникой, находящейся вне территории (помещения) осмотра; на это могут указывать кабели и провода, идущие от осматриваемого СВТ за границу места осмотра (в другие помещения или здания) либо к аппаратам внутренней связи (в этом случае граница осмотра места происшествия значительно расширяется);

- наличие на объекте, путях подхода и отхода следов преступления и преступника, специфическими среди которых являются: следы орудий взлома, повреждения, уничтожения и/или модификации охранных и сигнальных устройств; показания регистрирующей (электронный журнал) или специальной мониторинговой (тестовой) аппаратуры; следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих СВТ и электрооборудование; остатки соединительных проводов и изоляционных материалов, капли припоя, канифоли или флюса; следы проплавления, прокола, надреза изоляции проводов СВТ, наличие участков механического сдавливания и приклеивания сторонних предметов;

- наличие или отсутствие учетно-справочной документации к СВТ - технического паспорта и подобного ему документа; журнала оператора или протокола автоматической фиксации расчетно-кассовых и иных операций; журнала учета машинных носителей информации (МНИ), машинных документов, заказов (заданий или запросов); журнала (карточки) учета выдачи МНИ и машинных документов; журнала (карточки) учета массивов (участков, зон), программ, записанных на МНИ; журнала учета уничтожения брака бумажных МНИ и машинных документов; актов на стирание конфиденциальной информации, уничтожение машинных носителей с конфиденциальной информацией, конфиденциальных машинных документов.

Осмотр средства вычислительной техники

Осмотр СВТ, участвовавшего в преступлении, ***производят для достижения следующих целей*:**

1. Обнаружения следов, образовавшихся в результате происшествия или совершения преступления, и других вещественных доказательств для установления, кем, с какой целью и при каких обстоятельствах было совершено преступление;

2. Выяснения обстановки происшествия для восстановления механизма совершения преступления;

3. Установления технического состояния СВТ.

При реализации первой цели требуется участие специалиста-криминалиста и специалиста в области СВТ и информационных технологий. В решении двух других непосредственное участие специалиста-криминалиста не требуется. В зависимости от специфики осматриваемого СВТ ***в следственном действии должны принимать участие следующие специалисты:***

- по обслуживанию и ремонту СВТ (для осмотра аппаратной части СВТ и соединительной арматуры; для ЭВМ - инженер-системотехник);

- в области сетевых технологий (для осмотра СВТ, используемых в системах дистанционной передачи данных - компьютерных сетях, периферийного оборудования удаленного доступа, удаленных терминалов);

- по средствам связи и телекоммуникациям (для осмотра оборудования электросвязи, используемого для передачи компьютерных данных и команд, а также СВТ, являющихся средствами связи);

- операторы СВТ - ЭВМ, пейджинговой и сотовой связи, контрольно-кассовых аппаратов, бухгалтер по приему и отправке электронных платежей и т. д. (для наружного осмотра СВТ);

- сотрудник Гостехкомиссии России (для осмотра специальных технических средств защиты выделенных помещений, СВТ и информации от несанкционированного доступа, утечки и съема, а также обнаруженной специальной разведывательной аппаратуры негласного получения информации);

- инженер-программист (для осмотра программного обеспечения СВТ, определения принципа его функционирования, установления следов преступной деятельности в среде машинной информации).

Отметим, что во избежание уничтожения (повреждения) СВТ и следов преступления при работе специалиста - криминалиста по осмотру СВТ недопустимо использование магнитосодержащих материалов, инструментов, приборов и оборудования, направленных источников электромагнитного излучения (магнитного порошка, магнитной кисточки, электромагнита, металлодетектора, мощных ламп освещения, мощных УФ и ИК излучателей, и т.д.), а также кислотно-щелочных материалов и нагревательных приборов.

При осмотре места происшествия и при производстве других следственных действий вышеуказанными материалами и оборудованием можно пользоваться с особой осторожностью на расстоянии более 1 метра от СВТ и их соединительных проводов.

***В протоколе осмотра СВТ фиксируются следующие данные*:**

- тип, марка, конфигурация, цвет и заводской номер (или инвентарный, учетный номер) изделия;

- тип (назначение), цвет и индивидуальные признаки соединительных и электропитающих проводов;

- состояние СВТ на момент проведения осмотра (выключено или включено);

- техническое состояние - внешний вид, целостность корпуса, комплектность СВТ - наличие и работоспособность необходимых блоков, узлов, деталей и правильность их соединения между собой, наличие расходных материалов, тип используемого машинного носителя информации и т. д. (проверку проводит соответствующий специалист);

- тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенных к нему электроприборов, число разъемов - розеток и т.д.);

- наличие заземления («зануления») СВТ и его техническое состояние;

- наличие и техническая возможность подключения к СВТ периферийного оборудования и/или самого СВТ к такому оборудованию, либо к каналу электросвязи (определяется специалистом по наличию у СВТ соответствующих портов и разъемов);

- повреждения, непредусмотренные стандартом конструктивные изменения в архитектуре строения СВТ, его деталей (частей, блоков), особенно те, которые могли возникнуть в результате происшествия или преступления, а также спровоцировать создание внештатной технической ситуации (привести к возникновению происшествия);

- следы преступной деятельности (орудий взлома корпуса СВТ, проникновения внутрь корпуса СВТ, пальцев рук, несанкционированного подключения к СВТ сторонних технических устройств, а также канифоли, припоя, флюсов и других химических веществ, обрезки монтажных проводов и изоляционных материалов, кровь, пот, волосы, волокна ткани и т.д.);

- расположение СВТ в пространстве относительно периферийного оборудования и других электротехнических устройств;

- точный порядок соединения СВТ с другими техническими устройствами;

- категорию информации, циркулирующей в СВТ (общедоступная или конфиденциальная);

- наличие или отсутствие индивидуальных средств защиты осматриваемого СВТ и обрабатываемой на нем информации от несанкционированного доступа, съема и утечки (особенно тех из них, которые автоматически уничтожают информацию и МНИ при нарушении процедуры доступа к СВТ, порядка их использования и/или правил работы с информацией) определяется специалистом Гостехкомиссии России;

- расположение рабочих механизмов СВТ и изображение на его экране (мониторе) или визуально-контрольном окне (для принтеров, контрольно-кассовых машин, контрольно - пропускных механизмов, цифровых аппаратов связи и т.д.) в том случае, если на момент осмотра они находится в рабочем состоянии;

- все основные действия, производимые специалистом при осмотре СВТ (порядок нажатия на клавиши и запорные механизмы, корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения или соединения СВТ и ее составляющих, отсоединения коммуникационных и электропитающих проводов и кабелей, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.).

Осмотр машинного носителя информации

Осмотр машинного носителя информации может быть произведен в ходе осмотра места происшествия или как самостоятельное следственное действие.

Осмотр МНИ производится с участием специалиста и начинается с определения типа, вида, назначения, технических параметров и ознакомления с его содержанием.

К машинным носителям информации относятся:

- магнитные диски (гибкие дискеты, жесткие «винчестеры», «банки» и «Zip»);

- оптические и магнитооптические компакт-диски (CD - «лазерные диски»);

- бумажные перфоленты и магнитные ленты (в бобинах и кассетах);

- бумажные перфокарты и магнитные карты (поштучно и в «колодах», комплектах);

- пластиковые карты (карточки);

- интегральные микросхемы (ИМС) в виде оперативной памяти (ОЗУ) и/или постоянного запоминающего устройства (ПЗУ), в т. ч. находящиеся в различных СВТ (персональных компьютерах, пейджерах, сотовых и иных аппаратах электросвязи, электронных записных книжках, электронных переносных справочниках и переводчиках, контрольно-кассовых аппаратах, банкоматах, контрольно-пропускных устройствах, смарт-картах и т.д.).

***В протоколе осмотра должны быть зафиксированы следующие фактические данные*:**

1. Тип, вид, марка, назначение, цвет и заводской номер (или учетный номер носителя).

2. Наличие, индивидуальные признаки и техническое состояние футляра (коробки, упаковки, специального технического устройства) - тип, размеры, цвет, материал, физические повреждения, наклейки, принцип функционирования, емкость и т.д.

3. Техническое состояние - размеры носителя, внешний вид, материал каркаса носителя, его целостность и индивидуальные признаки, материал основного информационно-несущего слоя и его целостность (механические повреждения - царапины, деформации, нарушения несущего слоя и т.д.), наличие и положение (сохранность) приспособлений от несанкционированного уничтожения (перезаписи) информации (ключей, пломб, заглушек, маркеров), наличие и техническое состояние механизмов защиты информационно-несущего материала (отверстий окон для считывания и записи информации).

4. Наличие, размеры, цвет, марка и техническое состояние разъемов для подключения к специальному считывающему устройству.

5. Присутствие внешней спецификации, ее цвет и размеры (заводские или пользовательские наклейки с текстом или специальными пометками).

6. Наличие, индивидуальные признаки защиты носителя от несанкционированного использования (тип - голография, штрихкод, эмбосинг, флуоресцирование, перфорация, ламинирование, вплавление личной подписи пользователя и т. д.; размеры, цвет, вид).

7. Признаки материальной подделки МНИ и их защиты - подчистки, подтирки, травления, термического воздействия, переклеивания (склеивания, наклеивания, заклеивания), дописки, замены, переэмбосирования, перепайки и т.д.

8. Работоспособность и внутренняя спецификация - серийный номер и/или метка тома, либо код; размер разметки (для дисков - по объему записи информации, для лент - по продолжительности записи); размер области носителя, свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров, цилиндров; количество записанных программ, файлов, каталогов (подкаталогов), данных, их структура, название (имя и/или расширение), размер и объем, который занимают их названия, дата и время создания (или последнего изменения), а также специальная метка или флаг (системный, архивный, скрытый, только для чтения или записи и т.д.); наличие скрытых или ранее стертых файлов (программ) и их реквизиты (название, размер, дата и время создания или уничтожения).

9. Результат осмотра содержимого файлов (программ, компьютерной информации), записанных на МНИ или находящихся в оперативной памяти СВТ и имеющих значение для дела.

10. Все манипуляции (нажатия на клавиши и т.д.) со средствами вычислительной техники, совершенные в процессе осмотра.

11. Индивидуальные признаки СВТ, используемых в процессе осмотра, - тип, вид, марка, название, заводской или регистрационный (учетный) номер и т.п.

12. Ссылка на то, что используемые в процессе осмотра СВТ перед началом следственного действия были тестированы специалистом на предмет отсутствия в них вредоносных программных и аппаратных средств.

Осмотр машинного документа

Осмотр документа на машинном носителе и машинограмме, создаваемым СВТ, производится с участием специалиста (или группы специалистов) в зависимости от сферы (области) деятельности, в которой используется осматриваемый документ (кредитно-финансовая, банковская, расчетно-кассовая, услуг, охраны и т.д.).

Цели осмотра - выявление и анализ внешних признаков и реквизитов документа, анализ его содержания, обнаружение возможных признаков его подделки (фальсификации).

При подготовке к проведению данного следственного действия следователю необходимо ознакомиться с требованиями ГОСТ 6.10.4-84 от 01.07.87 г. «УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения». Этим нормативным актом определяются требования к составу и содержанию реквизитов, придающих юридическую силу документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники; порядок внесения изменений в эти документы; транспортирования (передачи, пересылки и т.д.) машинных документов, их записи на МНИ; система приема по каналам электросвязи, воспроизведения машинного документа на машинограмму, создания копий и дубликатов машинных документов.

Документы, используемые в документообороте юридических лиц (учреждений, организаций, предприятий и т.д.) могут создаваться как для внешнего, так и внутреннего пользования. Однако в соответствии с требованиями ГОСТ 6.38-72 «Система организационно - распорядительной документации. Основные положения», рассматриваемые документы должны всегда иметь следующие реквизиты: наименование юридического лица, выдавшего (или создавшего) документ; номер документа и дата его составления; заголовок; адресат; содержание; подпись и печать на документах, требующих особого удостоверения их подлинности (или код лица, утвердившего документ).

В соответствии со статьей 160 Гражданского кодекса Российской Федерации допускается использование для удостоверения подлинности юридических документов факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи (ЭЦП) либо иного аналога собственноручной подписи физического лица.

В частности, порядок использование ЭЦП определяется ГОСТ Р 34.10.94 «Электронная цифровая подпись (ЭЦП)». Электронная подпись дает возможность не только гарантировать аутентичность документа в части его авторства путем электронно-цифровой фиксации основного текста и личностных характеристик подписи физического лица, утвердившего документ, но и установить факт неискаженности (целостности) содержащейся в нем информации, а также зафиксировать попытки подобного искажения. Электронная подпись, состав которой непосредственно зависит от заверяемого текста, соответствует только этому тексту при условии, что его никто не изменял. Проверочная сумма (хэш-функция) измененного (фальсифицированного) электронного документа отличается от проверочной функции, которая получается в результате обработанного преобразования электронной подписи. Алгоритм криптографического преобразования данных в ЭВМ, системе ЭВМ или их сети с помощью ЭЦП определяется ГОСТ Р 34.11.94 «Функция криптографического преобразования данных (хэш-функция)». Переданный получателю подписанный документ состоит из текста, электронной подписи и сертификата пользователя, который содержит в себе гарантированно подлинные данные пользователя, в том числе его отличительное имя и открытый ключ расшифрования для проверки подписи получателем либо третьим лицом, осуществившим регистрацию сертификата.

На документы, создаваемые СВТ, распространяется также ГОСТ 13.002-79 «Микрофильм на правах подлинника. Основные положения».

Порядок работы с некоторыми видами документов, создаваемых СВТ, может регулироваться, кроме вышеуказанных, межотраслевыми, внутриотраслевыми и другими нормативными актами (например, приказом по объединению, учреждению, организации, предприятию, возлагающим обязанности по удостоверению документов определенной категории на конкретное должностное лицо или работника).

В протоколе осмотра документа должны быть отражены следующие данные:

1. Наименование (назначение) документа (например, идентификационный код и наименование формы документа по классификатору ОКУД).

2. Тип используемого машинного носителя, его индивидуальные признаки и техническое состояние.

3. Тип, марка, конфигурация и техническое состояние аппаратного и программного оборудования, других технических устройств, применявшихся при осмотре.

4. Наличие сопроводительного письма или документа, его заменяющего (например, договора на использование пластиковой карточки или регистрационного сертификата на использование ЭЦП).

5. Форма записи содержания документа (человекочитаемая, закодированная в машинном формате, смешанная).

6. Реквизиты организации (лица) создателя документа (наименование и юридический адрес).

7. Наличие грифа ограничения доступа к документу на машинном носителе или машинограмме («конфиденциально», «для служебного пользования», «секретно», «совершенно секретно»).

8. Регистрационный номер документа и/или машинного носителя (заводской номер, серийный номер тома, метка тома).

9. Дата изготовления (создания) или выдачи документа (с указанием времени записи документа на МНИ, позволяющим идентифицировать ее с машинным протоколом).

10. Размер документа (линейный или объемный - по количеству символов или общему объему символов в документе в байтах) и/или количество страниц.

11. На чье имя выдан (реквизиты адресата-получателя).

12. Какими реквизитами заверен (ЭЦП; кодом (позывным) лица, ответственного за правильность изготовления, копирования или передачу документа по телекоммуникационным каналам; собственноручной подписью уполномоченного лица; печатью; индивидуальным кодом абонента сети дистанционной передачи данных - «электронной почты»; специальным позывным кодом аппаратуры связи).

13. Индивидуальные признаки документа (название файла - программы); структура расположения символов; машинный формат текста (формат MS DOS, WORD for WINDOWS и т.д.); наличие маркеров страниц, выделений текста; тип и цвет печати (матричный, струйный, электрографический, смешанный) указать конкретно для каждого элемента; наличие защитных знаков и т.д.).

14. Выявленные при осмотре признаки подлога и материальной подделки документа и его носителя.

Изъятие средств вычислительной техники, машинных носителей информации, компьютерной информации как элемент отдельных следственных действий

Изъятие СВТ, машинных носителей информации и компьютерной информации должно происходить при непосредственном участие соответствующих специалистов. При этом следователь должен обеспечить строгое соблюдение требований уголовно-процессуального законодательства, иначе изъятые при производстве следственного действия СВТ, материалы и документы впоследствии не смогут выступать в качестве доказательств по делу.

Для успешного осуществления вышеуказанного требования ***необходимо придерживаться следующих рекомендаций:***

1. По ходу проведения следственного действия необходимо постоянно акцентировать внимание понятых на все производимые специалистами манипуляции и их результаты.

2. Фактическое изъятие СВТ, находящихся на момент их осмотра во включенном состоянии, производится только после того, как будут выполнены и отражены в протоколе следственного действия такие мероприятия:

- определено и корректно приостановлено выполнение вычислительной операции;

- информация, находящаяся в оперативной памяти СВТ, записана на его постоянный МНИ, либо на специально подготовленный и тестированный для этих целей внешний МНИ;

- определены и корректно закрыты все исполняемые программы (в некоторых случаях некорректное отключение СВТ, путем его перезагрузки или выключения электропитания, без предварительного выхода из исполняемой программы приводит к потере информации, нарушению конфигурации вычислительной системы, стиранию всех информационных ресурсов на данном СВТ);

- выключено электропитание СВТ и всех его периферийных устройств;

- все электропитающие и соединительные провода и кабели, имеющие разъемное соединение, отсоединены от СВТ, источника питания и периферийного оборудования с обязательным указанием в протоколе порядка их соединения (принципиальная схема), отсоединения и индивидуальных признаков каждого элемента.

3. Изымаемые СВТ и их составляющие следует опечатывать так, чтобы исключить возможность непроцессуальной работы с ними, разукомплектовки и физического повреждения. Для достижения данной цели необходимо сделать следующее:

- опечатать аппаратуру и технические устройства путем наложения листа бумаги на разъёмы электропитания и подключения периферийного оборудования (порты) с захлестом на боковые панели корпуса изымаемого устройства и закреплением их краев густым клеем;

- в случае отсутствия у СВТ электропитающего и соединительного (портового) разъемов наложить лист бумаги или бумажный конверт (колпак) на штепсельную и/или

соединительную вилку, зафиксировать его клеем или бечевой на корпусе провода у основания вилки;

- лист (полоску) бумаги-пломбы следует также наложить на все разъемные детали корпуса СВТ и его составляющих, скрепив их между собой, и зафиксировать клеем (на прорезь дисковода, щель приемного устройства, лицевой и боковой панелях, тыльной панели и корпусе и т.п.);

- при наличии картонных коробок, ящиков, бумажных канцелярских или почтовых мешков и больших конвертов изымаемые СВТ можно запаковать в них без соблюдения требований, отмеченных в вышеприведенных пунктах, но обязательно опломбировать все соединительные швы и сделать опись вложения;

- на листах пломбирующей бумаги, на пломбах или упаковке должны быть подписи следователя, понятых и специалиста, участвующего в изъятии;

- МНИ, документы, технические устройства, соединительные (или электропитающие) провода и кабели вместе с разъемными устройствами надо упаковать отдельно друг от друга, сделать точное описание каждого в протоколе индивидуальных признаков и опись вложения для каждой единицы тары;

- при отсутствии четких внешних признаков изымаемый предмет следует запечатать в отдельную коробку (ящик, конверт), сделать об этом обязательную отметку в протоколе проведения следственного действия.

4. При изъятии магнитного носителя машинной информации нужно помнить, что он должен перемещаться в пространстве и храниться исключительно в специальном экранированном контейнере или алюминиевом футляре (оболочке), исключающем разрушающее воздействие различных электромагнитных и магнитных полей и направленных излучений. Для этого магнитные носители информации сначала упаковывают в пакет из обычной фольги (бытового или технического назначения), а затем опечатывают обычным способом, вкладывая в коробку или конверт. В качестве контейнера можно использовать цельноалюминиевую коробку с крышкой (например, алюминиевую посуду с крышкой из того же материала). Если в коробку упаковывается несколько носителей информации, то всегда составляется опись вложения с указанием индивидуальных признаков каждого носителя.

5. Недопустимо приклеивать что-либо непосредственно к МНИ и документам, пропускать через них бечеву, пробивать стиплером, делать пометки или маркировки, накалывать твердым предметом знаки, использовать пластилиновые или сургучовые печати и т. д.

6. При изъятии печатающих устройств (принтеров), особенно матричного (игольчатого) типа, их необходимо упаковывать в отдельные коробки (мешки, конверты) вместе с расходными материалами (красящими лентами, картриджами, бумагой), зафиксировав в том положении, в котором они находились на момент производства следственного действия.

7. В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства вычислительной техники (например, если СВТ является элементом компьютерной сети или системы дистанционной обработки информации), необходимо с помощью специалиста отключать его от источников удаленного доступа или, в крайнем случае, создать условия лишь для приема информации, полностью исключив возможность ее передачи (отправки). Идеальным вариантом изъятия СВТ в подобной ситуации является включение в телекоммуникационную сеть дублирующего СВТ с программно - аппаратными характеристиками, аналогичными изымаемому, после чего требуемое устройство отключается от сети и изымается. Такую технически сложную операцию может выполнить только квалифицированный специалист или группа специалистов, задействованных в следственном действии.

8. Если же возникла необходимость изъятия информации из оперативной памяти СВТ (непосредственно из оперативного запоминающего устройства - ОЗУ или из виртуального диска СВТ), то сделать это можно только путем копирования соответствующей информации на МНИ с использованием стандартных, специально подготовленных и тестированных программных и аппаратных СВТ, тактико-технические характеристики и индивидуальные признаки которых обязательно должны быть отражены в протоколе проведения следственного действия. Процесс изъятия должен быть зафиксирован с использованием видеозаписи.

9. Как показывает практика, при изъятии СВТ у следователя могут возникать конфликты с пользователем. При их разрешении необходимо руководствоваться следующими рекомендациями:

- Недопустимо производить изъятие в несколько приемов. В том случае, если следователь не располагает необходимым транспортом, следует сделать несколько рейсов от объекта до места хранения изъятых материалов с выставлением охраны на объекте изъятия (охране подлежат неизъятые СВТ и помещение, в котором они находятся).

- Изъятые предметы и материалы не могут быть оставлены на ответственное хранение на самом объекте или в другом месте, где к ним могут иметь доступ посторонние лица.

- Недопустимо оставлять на объекте части СВТ по причине их «абсолютной необходимости» в деятельности данного пользователя: как правило, желание сохранить от изъятия определенные СВТ указывает на наличие в них важной для следствия информации.

- Следует изымать все СВТ, находящиеся в помещении объекта и несущие следы преступной деятельности.

- В протоколе следственного действия должны обязательно фиксироваться конкретные признаки изымаемых СВТ (марка, быстродействие, марка процессора, объем памяти и т. д.).[28]

Стоит обратить особое внимание на то, что перед началом производства любых следственных действий, непосредственно связанных со СВТ, средствами и системами их защиты, необходимо в обязательном порядке получать и анализировать с участием специалистов информацию о технологических особенностях функционирования вышеприведенных технических устройств, уровня их соподчиненности и используемых средств связи и телекоммуникации во избежание их разрушения, нарушения заданного технологического ритма и режима функционирования причинения крупного материального ущерба пользователям и собственникам, уничтожения доказательств.

Осмотр места происшествия, средства вычислительной техники, машинного носителя информации и документа необходимо проводить в строгой последовательности, уделяя особое внимание тем частям предметов, на которых имеются повреждения и следы, и с обязательным использованием фото- и/или видеосъемки. Важно сфотографировать или произвести видеозапись не только места происшествия, отдельных объектов, СВТ и их соединений, но и все действия специалистов, участвующих в осмотре.

К протоколу осмотра прилагаются план или схема места происшествия, принципиальная схема соединения СВТ между собой и с каналами электросвязи (со спецификацией и расшифровкой условных обозначений), фото- видеопленка или магнитный носитель информации (лента, дискета или жесткий диск), распечатка информации.

Обыск и выемка

Обыск заключается в принудительном обследовании личности, помещений, сооружений, находящихся в ведении обыскиваемого лица и членов его семьи или организации, для отыскания и изъятия объектов - компьютеров, комплектующих, документов, имеющих значение для дела. Согласно ст. 182 УПК РФ следователь, имея достаточные основания полагать, что в каком-либо помещении или ином месте, или у

---

[28] *Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. № 2. С. 24.*

какого-либо лица находятся предметы или документы, могущие иметь значение для дела, для их отыскания и изъятия производит обыск по мотивированному постановлению (обыск в жилом помещении - только с санкции суда).

Обыск компьютерных устройств может быть необходим не только при расследовании компьютерных преступлений, но и по другим делам, поскольку это весьма удобные места для сокрытия мелких предметов.

Выемка (ст. 183 УПК РФ) представляет собой добровольную выдачу по требованию следователя или принудительное изъятие им компьютерных устройств и их частей, документов. Выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, производится следователем с санкции суда. Выемка документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, производится на основании судебного решения. При проведении выемки действия следователя сводятся обычно к тому, что он предлагает лицу или руководителю учреждения выдать определенный предмет (документ), а в случае отказа производит принудительное изъятие. При отказе выдать требуемые вещи или если была выдана только часть требуемых предметов (документов) и известно, что они спрятаны, искать их в других местах нельзя, поскольку это уже будет не выемка, а обыск. Поэтому следователь выносит постановление и производит неотложный обыск для обнаружения скрываемых предметов.

Обыск по делам о преступлениях, совершаемых с использованием СВТ, в большинстве случаев является неотложным следственным действием и требует тщательной подготовки.

На подготовительном этапе обыска следователю необходимо осуществить следующие мероприятия:

- выяснить, какие СВТ находятся в помещении, намеченном для проведения обыска (по возможности установить их тактико-технические характеристики);

- установить, какие средства защиты информации и СВТ от несанкционированного доступа находятся по месту обыска (по возможности - выяснить ключи доступа и тактико-технические характеристики средств защиты);

- определить режим и технические системы охраны объекта, СВТ и категорию обрабатываемой информации (общедоступная или конфиденциальная);

- выяснить, какие средства связи и телекоммуникаций используются для работы СВТ и информационного обмена - установить их тип, тактико-технические характеристики, категорию (общедоступные или конфиденциальные), абонентские номера, позывные, ключи (коды) доступа и т.п.;

- установить тип источников электропитания вышеперечисленных технических средств (электросеть, автономные, бесперебойные - комбинированные) и расположение пунктов обесточивания помещения и аппаратуры, подлежащих обыску;

- пригласить соответствующих специалистов для подготовки и участия в следственном действии;

- подготовить соответствующие СВТ, специальную аппаратуру и материалы для поиска, просмотра, распаковки, расшифровки, изъятия и последующего хранения машинной информации, СВТ и специальных технических устройств;

- определить дату, время и границы проведения обыска, время поиска и меры, обеспечивающие его конфиденциальность (важно, чтобы пользователь, владелец или оператор СВТ не подозревал о предстоящем следственном действии и не работал в момент проведения обыска на СВТ);

- проинструктировать оперативных сотрудников и видеооператора о специфике проводимого следственного действия;

- по возможности изучить личность обыскиваемого, пользователя (владельца) СВТ, вид его деятельности, профессиональные навыки по владению СВТ;

- пригласить понятых, обладающих специальными познаниями в области автоматизированной обработки информации.

По прибытии к месту проведения обыска необходимо вести себя следующим образом:

- быстро и внезапно войти в обыскиваемый объект (или одновременно в несколько помещений);

- при оказании сопротивления со стороны лиц, находящихся на объекте обыска, - обыскиваемого, его родственников, охранников (сторожей), сотрудников организации и т.п. - принять срочные меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение;

- организовать охрану места обыска и наблюдение за ним; охране подлежат периметр обыскиваемых площадей, СВТ, хранилища МНИ, все пункты (пульты) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади), специальные средства защиты от несанкционированного доступа, хранилища ключей аварийного и регламентного доступа к СВТ, помещениям и другим объектам (пульты, пункты, стенды, сейфы и т.п.).

Следователю необходимо знать, что к изменению или уничтожению машинной информации, ее носителей и СВТ, которые впоследствии могут выступать в качестве доказательств по делу, приводят не только манипуляции с самими СВТ, но и включение или

выключение их электропитания. Поэтому все электротехническое оборудование и средства электротехнических систем, имеющиеся на месте обыска, должны находиться до момента их осмотра специалистом в том пространственном положении и техническом состоянии, в котором они были в момент начала обыска. *Для этого необходимо соблюдать следующие условия*:

- не разрешать кому бы то ни было из находящихся на объекте обыска лиц (за исключением приглашенных специалистов), прикасаться к СВТ и источникам питания электрооборудования с любой целью, даже в случае согласия обыскиваемого добровольно выдать искомый предмет, документ или информацию;

- не разрешать кому бы то ни было без разрешения специалиста выключать-включать электроснабжение объекта;

- в случае если на момент начала обыска электроснабжение объекта выключено, то до его восстановления следует отключить от электросети все СВТ, предварительно зафиксировав в протоколе схему их подключения к источникам электропитания, расположение, тактико-технические характеристики и порядок отсоединения от них СВТ;

- не производить самостоятельно никаких манипуляций с электрооборудованием и СВТ, если результат их заранее неизвестен;

- при настойчивых попытках обыскиваемого или других лиц, находящихся на месте обыска, получить доступ к СВТ, пунктам связи, управления и энергоснабжения, к другим техническим средствам и оборудованию следует принять меры для удаления этих лиц в другое помещение (не подлежащее обыску) с одновременной фиксацией в протоколе данного события.

***На обзорной стадии обыска необходимо*:**

1. Определить и отключить специальные средства защиты информации и СВТ от несанкционированного доступа, особенно те, которые автоматически уничтожают информацию и МНИ при нарушении процедуры доступа к СВТ и машинной информации, порядка их использования и/или установленных правил работы с ними; принять меры к установлению пароля, ключа санкционированного доступа и шифрования-дешифрования информации.

2. Установить наличие телекоммуникационной связи между СВТ, СВТ и каналами электросвязи по схемам «компьютер - компьютер», «компьютер - управляющий компьютер», «компьютер - периферийное устройство», «компьютер - средство электросвязи», «компьютер - канал электросвязи», «периферийное устройство - периферийное устройство», «периферийное устройство - канал (средство) электросвязи» и наоборот.

При наличии компьютерной сети любого уровня технической организации в первую очередь должен быть осмотрен и подвергнут обыску центральный управляющий компьютер (сервер сети, компьютер процессингового центра, узла связи, охранной системы и т.п.). Данное СВТ хранит в своей оперативной и постоянной памяти наибольшую часть машинной информации, управляет другими СВТ, имеет с ними прямую и обратную связь и, как правило, имеет программу автоматической фиксации доступа СВТ друг к другу (своеобразный «электронный журнал» учета работы всех СВТ сети - их индивидуальные номера (позывные, абонентские и т.п.), точные даты и время каждого соединения при обмене информацией, длительность и вид сеанса связи, характеристику передаваемой и получаемой информации, аварийные ситуации, сбои в работе отдельных СВТ (рабочих станций, периферийного оборудования), идентификационные коды и пароли операторов, попытки несанкционированного или нештатного доступа и т.д.).

Следователь должен знать, что при наличии соединения СВТ с другим оборудованием и электронно-вычислительной техникой, находящимися вне периметра обыскиваемой зоны (в другом помещении, здании, населенном пункте и т.д.), существует реальная возможность непосредственного доступа к машинной информации и совершения любых действий с ней и СВТ (стирание, уничтожение, модификация, копирование, блокирование, нарушение работы). *Для предотвращения этого необходимо*, в зависимости от ситуации и рекомендаций специалиста, временно или на длительный срок, частично или полностью отключить СВТ или локальную вычислительную сеть целиком от технических устройств, находящихся за периметром обыскиваемой зоны. Отключение может быть произведено как на программном, так и аппаратном уровне. Если СВТ работает в режиме «электронной почты», то предпочтительнее оставить его до конца обыска в работающем состоянии в режиме «приема почты», исключив возможность какой-либо обработки и передачи информации. Эту работу может сделать только квалифицированный специалист. Все выполняемые им действия должны быть зафиксированы с помощью видеозаписи и отражены в протоколе обыска.

3. Определить СВТ, находящиеся во включенном состоянии, и характер выполняемых ими операций и/или программ. Особое внимание необходимо уделить терминальным печатающим и видеоотображающим устройствам (принтерам и мониторам). Распечатки информации (листинги) при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора изучено и детально описано в протоколе (можно также зафиксировать его на видеопленку, либо сделать распечатку на бумаге с использованием специальных сканирующих программ).

Если специалисту удастся установить, что на момент обыска на каком-либо СВТ происходит уничтожение информации, либо уничтожается машинный носитель информации, необходимо всеми возможными способами приостановить этот процесс и начать обследование с данного места или СВТ.

4. При обследовании персонального компьютера необходимо:

- установить последнюю исполненную программу и/или операцию, а при возможности все, начиная с момента включения компьютера;

- произвести экспресс-анализ машинной информации, содержащейся на жестком диске и в оперативной памяти компьютера с целью получения информации, имеющей значение для следствия (интерес могут представлять файлы с текстовой и графической информацией).

Детальный этап обыска является очень трудоемким и требует высокой квалификации как специалиста в области СВТ, так и всей следственно-оперативной группы.

Необходимо четко организовать поисковые мероприятия, направленные на поиск тайников, в которых могут находиться предметы, устройства и документы. Ими может служить и само СВТ - аппаратные и программные оболочки модулей его составляющих.

***Следователю стоит придерживаться следующих рекомендаций*:**

- При невозможности вскрытия корпуса СВТ (если это может привести к утрате информации, физическому повреждению ее носителя либо приведению к неисправному состоянию) необходимо изъять СВТ целиком для лабораторного исследования.

- Все обнаруженные машинные носители информации (дискеты, пластиковые карточки, ленты, в т.ч. аудио-, видеокассеты и оптические компакт-диски) следует изъять для последующего анализа содержащихся на них данных на *аттестованном* исследовательском *оборудовании*, при отсутствии которого осмотр информации недопустим.

- Нельзя использовать специальную поисковую и досмотровую технику, один из элементов которой - источник электромагнитных или магнитных излучений (металлодетекторы, магниты, электронные стетоскопы, рентгеновские установки и т.п.).

- При необходимости изъятия жесткого диска персонального компьютера целесообразно изъять весь процессорный (системный) блок.

- В случае изъятия печатающего устройства (принтера) необходимо помнить, что в настоящее время возможна идентификация печатной продукции, изготовленной лишь на матричном (игольчатом) принтере. Для лазерного (электрографического) и струйного типов принтеров данный анализ практически невозможен.

На заключительном этапе обыска составляются: протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы

расположения СВТ относительно друг друга, строительных проемов, инженерно - технических коммуникаций, оконечных устройств электронесущей арматуры, а также принципиальная схема соединения СВТ между собой и с другими техническими устройствами; проводятся дополнительная фотосъемка и видеозапись.

Предметом выемки в абсолютном большинстве случаев *служат* средства вычислительной техники, машинные носители информации, машинная информация, всевозможные документы, средства защиты информации, специальная разведывательная и контрразведывательная аппаратура, а также свободные образцы почерка, машинописных текстов и готовой продукции для сравнительного исследования.

Помимо вышеуказанного могут быть изъяты материалы, предметы, приспособления, устройства и инструменты, которые могли быть использованы преступником при изготовлении орудий преступления, поддельных документов, машинных носителей информации и самой информации; черновики, на которых отрабатывалась поддельная подпись или другие реквизиты документа; копии и бланки регистрационно-учетных документов и расчетно-кассовых операций; техническая и справочная литература, косвенно связанная с технологией обращения и изготовления электронных документов и машинных носителей информации, орудий преступления; фотографии, аудио-, видеокассеты соответствующего содержания, в том числе с зарубежными художественными видеофильмами, содержащими эпизоды преступной деятельности, способы подготовки, совершения и сокрытия преступлений, изготовления спецтехники; оргтехника - копировальные и печатные аппараты (ксероксы, печатные машинки, телефонные аппараты с расширенными функциями, факсы, пейджеры, сотовые и радиотелефонные аппараты и т.д.); штампы, печати и маркираторы; ламинаторы; средства эмбосирования машинных носителей, нанесения защитных знаков и т.д.

Назначение экспертиз

По делам рассматриваемой категории существует постоянная необходимость использования в процессе расследования специальных познаний в области новых информационных технологий. Данные познания необходимы как для получения доказательств, так и для процессуального оформления документов, подготовленных средствами компьютерной техники, которые впоследствии могут играть роль доказательств.

С начала 90-ых годов в России появился новый вид криминалистических экспертиз, получивших название ***компьютерно - технических***.

В настоящее время с их помощью можно решать следующие задачи:

- воспроизводить и распечатывать всю или часть компьютерной информации (по определенным темам, ключевым словам и т.п.), содержащейся на машинных носителях, в

том числе находящейся в нетекстовой форме (в сложных форматах - в форме языков программирования, электронных таблиц, баз данных и т.д.);

- восстанавливать компьютерную информацию, ранее содержавшуюся на машинных носителях, но впоследствии стертую или измененную (модифицированную) по различным причинам;

- устанавливать дату и время создания, изменения (модификации), стирания, уничтожения, либо копирования той или иной информации (документов, файлов, программ и т.д.);

- расшифровывать закодированную информацию, подбирать пароли и раскрывать систему защиты СВТ;

- исследовать СВТ на предмет наличия в них программно-аппаратных модулей и модификаций, приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети (вредоносных средств - компьютерных вирусов, «закладок», «жуков» и т.п.);

- определять авторство, место (средство) подготовки и способ изготовления документов (файлов, программ), находящихся на машинном носителе информации;

- выяснять возможные каналы утечки конфиденциальной информации из компьютерной сети, конкретных СВТ и помещений; устанавливать возможные несанкционированные способы доступа к охраняемой законом компьютерной информации и ее носителям;

- выяснять техническое состояние, исправность СВТ, оценивать их износ, а также индивидуальные признаки адаптации СВТ к конкретному пользователю;

- устанавливать уровень профессиональной подготовки отдельных лиц, проходящих по делу, в области программирования и в качестве пользователя;

- определять конкретных лиц, нарушивших правила эксплуатации ЭВМ, системы ЭВМ или их сети;

- выяснять причины и условия, способствующие совершению правонарушения, связанному с использованием СВТ.[29]

Исходя из этих задач, ***следователь может поставить на разрешение эксперта следующие основные вопросы***:

---

[29] *Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. № 2. С. 24.*

1. Является ли представленное на исследование техническое устройство средством электронно-вычислительной техники? Если да, то укажите тип, вид, назначение, техническое состояние и тактико-технические характеристики.

2. Каковы тип, вид, марка, изготовитель, техническое состояние, тактико-технические характеристики (исправность, процент износа, и т.п.) средств вычислительной техники, представленных на исследование?

3. Какая информация содержится на машинных носителях, представленных на исследование?

4. Возможна ли раскодировка информации, записанной в сложных форматах? Если да, то каково ее содержание в человекочитаемой форме?

5. Какие документы находятся на представленных на исследование машинных носителях информации? По возможности представьте их в человекочитаемой форме путем распечатки на бумажном носителе.

6. Какая компьютерная информация и в какой форме (файл, программа, документ) была стерта, скопирована, изменена (модифицирована), уничтожена?

7. Каковы индивидуальные признаки компьютерной информации, представленной на исследование, - название, размер, дата и время создания, изменения (модификации)?

8. Когда и в какое время был создан файл (документ), представленный на исследование?

9. Как изменялось содержание обнаруженных документов (конкретных файлов, программ) на представленных на исследование машинных носителях информации - по названию, размеру, дате, времени создания (стирания, изменения)?

10. Возможно ли получение скрытой информации, касающейся проходящих по делу лиц (предметов, документов, событий)? Если да, то распечатайте ее в человекочитаемой форме.

11. Изготовлены ли представленные документы с использованием печатающих средств компьютерной техники?

12. Какого типа (вида, класса) печатающее устройство (принтер) использовалось при изготовлении представленных на исследование документов?

13. Изготовлены ли представленные документы на одном или на разных печатающих устройствах (принтерах)?

14. Не производилась ли допечатка в представленном на исследование документе с использованием печатающего устройства (принтера)?

15. Подготовлены ли предъявленные на исследование документы на представленных на исследование печатающих устройствах (принтерах)?

16. Какого рода программное обеспечение могло использоваться при подготовке и распечатке представленных на исследование документов?

17. С помощью каких программно-аппаратных средств вычислительной техники был подготовлен документ (машинный носитель), представленный на исследование?

18. Содержатся ли на представленных на исследование средствах вычислительной техники программно-аппаратные модули и модификации, способные уничтожать, блокировать, модифицировать либо копировать информацию, нарушать работу ЭВМ, системы ЭВМ или их сети без предварительного предупреждения пользователя о характере действия или не запрашивающие разрешение пользователя на реализацию программой своего назначения? Если да, то какие? Каков характер их воздействия на ЭВМ и ее программное обеспечение?

19. Содержатся ли на представленных на исследование средствах вычислительной техники программно-аппаратные модификации, влияющие на конечные результаты работы конкретного технического устройства либо программного продукта? Если да, то какие? Каков характер и последствия их воздействия на конкретное устройство и его программное обеспечение?

20. Нарушение каких правил эксплуатации ЭВМ, системы ЭВМ, их сети, а также систем их безопасности привело к образованию ущерба (наступлению иных тяжких последствий)? Определите конкретные должностные лица, ответственные за нарушение указанных правил.

21. Какой материальный ущерб причинен потерпевшему?

22. Каким паролем (кодом) осуществляется доступ к ЭВМ (системе ЭВМ, компьютерной сети, программе, файлу, периферийному устройству и т.п.), представленной на исследование?

23. Каковы тип, вид, марка, изготовитель, техническое состояние и основные тактико-технические характеристики средства защиты ЭВМ (компьютерной информации), представленной на исследование?

24. Каков уровень профессиональной подготовки конкретного лица, проходящего по делу, в области программирования (в качестве пользователя ЭВМ, системы ЭВМ, компьютерной сети, программиста, оператора, администратора баз данных и т.п.) либо защиты компьютерной информации?

25. Каковы каналы утечки компьютерной информации из ЭВМ, системы ЭВМ, компьютерной сети, иного средства электронно-вычислительной техники, помещения, проходящих по делу?

26. С помощью каких технических устройств было осуществлено копирование (стирание, уничтожение, модификация) охраняемой законом компьютерной информации? По возможности укажите тип, вид и основные тактико-технические характеристики устройства.

27. Какие причины и условия, способствовали совершению правонарушения в сфере компьютерной информации? Представьте их подробное описание.

28. Возможно ли сопряжение (соединение) представленной на исследование ЭВМ (средства электронно-вычислительной техники) с каналами электросвязи? Укажите конкретно, с какими (вид, тип, модификация канала электросвязи) и с помощью каких устройств?

29. Возможно ли сопряжение (соединение) представленного на исследование технического устройства с ЭВМ, системой ЭВМ или компьютерной сетью? Укажите тактико-технические характеристики аппаратуры.

Этот список вопросов не является исчерпывающим и может быть расширен, исходя из обстоятельств конкретного уголовного дела. В затруднительных случаях при постановке вопросов следует консультироваться у самого эксперта.

Постановление о назначении компьютерно-технической экспертизы должно содержать максимально полную описательную часть, в которой следует отразить:

- обстоятельства уголовного дела;

- сведения о лицах, причастных к совершению преступления;

- документы, сведения о которых могут содержаться на машинных носителях, представляемых на исследование;

- сведения, которые могут быть использованы в качестве «ключевых» слов при восстановлении и/или поиске экспертом информации (например, названия фирм, учреждений и организаций, фамилии клиентов, предполагаемые номера счетов и т.д.).

В резолютивной части объем задания эксперту должен быть определен конкретно. Современные СВТ имеют большие объемы постоянной памяти в виде жестких дисков (до нескольких гигабайт), поэтому следователь физически не сможет изучить и оценить содержание всего машинного носителя в течение приемлемого для этого времени. Для оптимизации данного процесса темы интересующей следователя информации должны быть точно обозначены при постановке вопросов, а сами они - сформулированы кратко и информативно.

При назначении компьютерно-технической экспертизы следователь должен четко представлять ее возможности и ограничения, не ставить перед экспертами вопросы и задания, выходящие за рамки их компетенции.

Нередко в процессе расследования компьютерного преступления возникает необходимость в установлении этапов обработки бухгалтерских данных с использованием СВТ, на которых вносились те или иные изменения, а также признаков интеллектуального подлога в первичных и сводных бухгалтерских документах, составленных на ЭВМ; в определении фактов уменьшения облагаемой налогом прибыли, выявлении счетных работников, причастных к совершению компьютерного преступления, путем исследования носителей оперативной информации, а также лиц, вводивших соответствующие данные в ЭВМ, и т.д. Для этих целей необходимо использовать *возможности судебно - бухгалтерской экспертизы*, позволяющей при проведении исследований установить, насколько соблюдены те или иные требования положений о документах и документообороте в бухгалтерском учете при оформлении различных хозяйственных и иных операций первичными документами и отображении их в регистрах бухгалтерского учета и отчетности, в том числе выраженных в форме, зафиксированной на машинном носителе и машинограмме, созданных средствами компьютерной техники.

В случаях выявления нарушения этих нормативных документов, эксперт-бухгалтер может установить их причины (не сделаны ли они с целью совершения преступления - злоупотребления, сокрытия недостачи материальных ценностей, уменьшения их размера и т.д.) и сделать вывод о том, насколько эти нарушения положений повлияли на состояние бухгалтерского учета и выполнение функций лицами, ответственными за это в управлении хозяйственной или иной деятельностью. При этом возможно установление лиц, ответственных за созданные или допущенные нарушения правил составления первичных документов и учетных регистров.

Наиболее оптимальным вариантом в некоторых случаях является назначение *комплексной компьютерно-технической и судебно-бухгалтерской экспертизы*. Как правило, необходимость такой экспертизы возникает в процессе расследования многоэпизодных уголовных дел о преступлениях в сфере экономики, совершенных с использованием компьютерной информации.

По делам рассматриваемой категории назначаются также: *технологические, электроакустические, фоноскопические, видеофоноскопические, радиотехнические, электротехнические и иные технические экспертизы*; в зависимости от отрасли хозяйства или характера нарушений - *товароведческие, финансово-экономические, криминалистические*, в частности, *технико-криминалистические экспертизы документов, созданных с использованием СВТ и новых репрографических технологий*, *и т.д.*

Например, ***при назначении радиотехнической экспертизы перед экспертом можно поставить следующие вопросы***:

1. Является ли представленное на исследование устройство (само или в комплекте) радиопередающей (радиоприемной) аппаратурой (установкой)?

2. В каком диапазоне радиочастот работает данное устройство и какова его мощность в антенне? Укажите дальность и другие тактико-технические характеристики радиоприема (или передачи).

3. В работе какого канала электросвязи используется данное устройство?

4. Является ли данное устройство самодельным, заводского изготовления или частью промышленной аппаратуры (ее отдельными блоками)?

5. Возможно ли использование данного устройства для проведения специальных технических мероприятий (разведывательных или контрразведывательных)?

6. Создает ли данное устройство помехи в каналах электросвязи, в частности, для радио- и телеприема (телефонной, телеграфной, факсимильной, связи ЭВМ и др. видов электросвязи)? Если да, то насколько превышены допустимые нормы и к каким вредным последствиям может привести эксплуатация данного устройства?

Таким образом, наряду со штатными экспертами соответствующих учреждений правоохранительных органов к подготовке и участию в следственных действиях необходимо шире привлекать специалистов профильных предприятий и учреждений, научно-исследовательских и учебных заведений, а также отдельных специалистов, имеющих опыт практической работы в определенной области знаний.

Следователь, правильно оценив и тщательно изучив заключения экспертов и прилагаемые к ним материалы, может широко использовать полученные данные как при назначении и производстве других экспертиз и следственных действий, так и в качестве самостоятельных доказательств по делу.

Изучение специальной литературы на предмет проведенных компьютерно-технических экспертиз и анализ имеющихся результатов позволяет сделать определенные выводы по кругу задач, которые могут быть успешно решены с их помощью.

В отношении носителей информации:

- прочтение и распечатка данных с машинных носителей информации;

- восстановление данных на машинном носителе, подвергшихся удалению или модификации;

- расшифровывание закодированных данных.

В отношении компьютерных систем:

- установление обстоятельств (даты, времени) помещения данных на машинный носитель и возможных действий с ними (модификации, удаления, копирования);

- вскрытие систем защиты (пароли, электронные ключи)

- выявление программно-аппаратных средств для несанкционированного доступа к машинным данным (модификации, копирования, блокирования и уничтожения данных);

- установление места совершения преступления;

- установление каналов доступа к защищаемой информации и путей ее возможной утечки;

- установление технических параметров оборудования, его состояния, возможностей аппаратно-программной модификации;

В отношении лиц, эксплуатирующих компьютерную систему:

- установление авторства данных, средств и способов их подготовки на машинных носителях (файлов документов, вредоносных программ);

- установление уровня квалификации проходящих по делу лиц в области технических средств и программного обеспечения (информационных технологий).

Приведенный список задач не претендует на полный охват, однако отражает очевидные особенности рассматриваемых экспертиз: комплексный характер и потребность в привлечении специальных познаний. Эти особенности служат, по нашему мнению, достаточным основанием для выделения уже в настоящее время самостоятельного класса судебных экспертиз, которые можно назвать судебной экспертизой компьютерных (информационных) систем. Выделение особого класса судебных экспертиз, который охватывал бы практически все основные задачи по делам, связанным с использованием информационных технологий, должно способствовать построению целостной доказательной базы и эффективному решению поставленных экспертных задач.

Подготовка материалов для проведения экспертных исследований должна предусматривать мероприятия, обеспечивающие исключение доступа (удаленного и местного, физического или технического) к электронному оборудованию. В общем виде процесс подготовки материалов для аппаратной экспертизы включает в себя три последовательных стадии, обеспечивающие получение процессуально-корректных доказательств.

1. Процессуально-корректное выключение аппаратуры, разборка конфигурации и подготовка к упаковке.

В эту стадию включаются этап завершения работы электронного средства с соблюдением методических и процессуальных норм, сбор торговой и технической документации об аппаратном средстве. Приведем пример. При подготовке аппаратных средств к изъятию для проведения экспертизы необходимо: путем опроса персонала или в ходе допросов выяснить сетевые имена пользователей и их пароли; изъять все оборудование, находящееся на компьютерных столах. При работе ПК произвести его «парковку».

Необходимо изымать все оборудование независимо от того, работает оно или нет. Опечатать столы. Внимание следует уделять и упаковочной таре, на которой может быть информация, помогающая идентифицировать электронное устройство. При подготовке к изъятию и перед упаковкой компьютерных и радиоэлектронных средств должны быть установлены и зафиксированы: конфигурация компьютера; номера моделей и серийные номера каждого из устройств; инвентарные номера, присваиваемые бухгалтерией при постановке оборудования на баланс предприятия; прочая информация, имеющаяся на фабричных ярлыках и коробках. Изымается сопутствующая техническая, торговая и упаковочная документация и тара, относящиеся к данному аппарату. Например, уникальный IMEI-номер (международный идентификатор мобильного оборудования), позволяющий идентифицировать мобильный терминал, наносится как на упаковке под штрих-кодом, так и в аккумуляторном отсеке аппарата. Все изъятые системные блоки должны быть опечатаны таким образом, чтобы исключить возможность их включения в сеть или разборки.

К изъятым носителям информации необходимо приложить информацию о владельце и месте изъятия. При изъятии НЖМД необходимо произвести описание содержимого жесткого диска и побитовое (лучше двойное) копирование НЖМД на «зеркальную» копию или компакт-диск (640 Мб). Эти действия должны найти свое отражение и быть зафиксированы в протоколе следственного действия. При этом следует иметь в виду, что «технически» подобную операцию можно осуществить только для компьютеров с файловой системой FAT16 или FAT32, не являющихся выделенными серверами в сети. Эти файловые системы используются в следующих операционных системах (ОС): MS-DOS и его клоны (FAT16); Windows и Windows for Workgroups (FAT16); Windows 95,98 (FAT16, FAT32); Windows 2000, NT, Windows NT Server.

Для опечатывания носителей информации (данных) необходимо:

1) упаковать их в жесткую коробку, опечатать ее;

2) на листе бумаги сделать описание упакованных носителей (тип каждого из них, их количество);

3) коробку с носителями и лист с описанием положить в полиэтиленовый пакет, который заклеить.

При опечатывании носителей информации недопустимо производить какие-либо действия с ними.

2. Упаковка и консервация аппаратного средства для его транспортировки в экспертное учреждение.

В эту стадию следует включить мероприятия по упаковке, перевозке и сдаче образцов в экспертное учреждение. В частности, опыт ФБР (группа компьютерного анализа

и исследований), в области работы с доказательствами показывает, что вопросам транспортировки изъятого оборудования уделяется очень серьезное внимание, так как некачественное выполнение этого мероприятия ведет к утрате вещественной доказательственной базы[30]. Перед транспортировкой образцов ВТ и РЭУ их следует упаковать, упаковку опечатать. Для этого следует использовать промышленную тару, коробки (пенопласт в качестве уплотнителя), мешки или ткань. НЖМД желательно упаковывать в устройства для безопасной перевозки носителей памяти типа «Mobile-Rack» и «Fleksi-Drive». Дискеты, компакт-диски, кассеты следует перевозить в плексигласовой упаковке. Аппаратуру необходимо плотно размещать в упаковочной таре, которую необходимо жестко закрепить в транспортном средстве. При транспортировке следует категорически избегать воздействия вибраций, взаимодействий с химически активными веществами; магнитных воздействий на аппаратуру и на магнитные носители информации, а также оградить изъятое от воздействия магнитосодержащих средств и криминалистической техники (например, магнитных подъемников, магнитных кисточек для выявления следов рук и проч.)[31]. Перевозку и хранение радиоустройств необходимо осуществлять в экранирующей таре. Например, перевозка сотовых телефонов на экспертизу должна проводиться в экранированной таре, т.е. металлических коробках с крышкой (если выяснены коды блокировок аппарата). После транспортировки в зимних условиях необходимо обеспечить прогрев объектов исследования в течение двух часов при комнатной температуре.

Если изъятые аппаратные средства оставлены на временное хранение на месте происшествия, следует организовать охрану выделенного для этих нужд помещения.

3. Хранение аппаратных образцов до производства экспертизы.

В эту стадию включаются обеспечивающие мероприятия по инструментальному хранению изъятых аппаратных образцов в соответствии со ст. 82 УПК РФ. Инструментальное хранение доставленных аппаратных средств необходимо обеспечить в соответствии с паспортными требованиями изготовителя. Аппаратные объекты представляются на экспертизу в неизмененном виде, соответствующем их фиксации и упаковке в ходе проведенного следственного действия. Получение аппаратных образцов и их

---

[30] *Бычков В.В. Соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования // Российский следователь. 2013. № 24. С. 12.*

[31] *Усов А.И., Зубаха В.С. Направление разработки методического обеспечения производства компьютерных экспертиз и исследований. Сб.: Экспертная практика. №47.- М., 1999.*

выдача оформляются в соответствии с приложениями № 66, 67 к УПК РФ постановление и протокол о получении образцов для сравнительного исследования.

В общем виде экспертное исследование аппаратных средств также как и любое другое исследование в судебной экспертизе, имеет следующие основные стадии: подготовительную; проведения собственно экспертного исследования, в том числе экспертного эксперимента; анализа результатов и составление экспертного заключения САКЭ.

Подготовительный этап аппаратной экспертизы включает в себя осмотр экспертом объектов экспертизы еще на месте происшествия и далее в стационарных условиях. При этом эксперт уясняет взаимосвязь исследуемого аппарата с другими КЭС и на основании классификации использования преступниками аппаратных средств производит выдвижение экспертных гипотез (версий) о возможных путях решения вопросов и применяемых методах исследования. Продумывается составление плана экспертного исследования КЭС, планируются организационно-технические меры, необходимые для проведения исследования.

Осмотр объектов САКЭ начинается с ознакомления с основаниями проведения экспертизы, предоставленными материалами следствия и аппаратными объектами и материалами, с которыми предстоит работать. Следующим действием эксперта является непосредственный осмотр представленных на экспертизу аппаратных объектов. При этом ему необходимо обратить внимание на целостность упаковки и печатей. При необходимости осуществляется предварительный просмотр данных, хранящейся на носителях. Экспертом должна учитываться, в соответствии с УПК РФ, возможность проведения повторного (ст.207 УПК РФ) комплексного (ст.201 УПК РФ) или комиссионного (ст.200 УПК РФ) экспертного исследования. После этого экспертом осуществляется планирование и логическое моделирование предстоящего экспертного исследования, включающего описание используемого аппаратно-программного (лицензированного) инструментального обеспечения, его подключение, планируемые промежуточные и конечные результаты. При этом следует зафиксировать следующие моменты:

- полный состав аппаратного обеспечения эксперта и режимы подключения всех плат (положения джемперов, используемые аппаратные настройки и т.п.);

- режимы подключения внешних носителей информации (на каком разъеме они установлены, как установлены джемперы и т.п.);

- полный состав общего (операционные системы, драйверы внешних устройств), общесистемного (системы управления базами данных, электронные таблицы, командные оболочки и т.п.) и специального программного обеспечения, установленного на компьютере

эксперта, основные параметры установки, последовательность запуска при начальной загрузке операционной системы, а также степени соответствия, используемой при экспертизе конфигурации;

Значение такого подробного описания весьма велико, так как в ряде случаев из-за некорректного или нестандартного подключения исследуемых магнитных носителей данных (информации) могут быть получены неверные результаты или вообще поставлено под сомнение сама возможность проведения исследований. Опыт проведения КТЭ в ОВД показал необходимость выполнения ряда обязательных первоочередных исследований (практически независимо от особенностей поставленных перед экспертом вопросов), а именно:

- проведение проверки на наличие программных вирусов и других вредоносных программ с использованием последней версии рекомендуемых антивирусных программ;

- определение системного времени, установленного на системной плате, а также соответствующих атрибутов файлов и директорий;

- определение используемого режима форматирования магнитного носителя, размера кластеров, количество дорожек и цилиндров. Выявление наличия поврежденных областей на НЖМД. Данная информации в исследовательской части заключения эксперта даст возможность решить впоследствии и при необходимости вопрос о проведении экспертизы последующих уровней.

По характеру выполняемых действий осмотр электронных объектов на месте происшествия или в экспертном учреждении, можно разделить на общий осмотр, осмотр вложений и внешний осмотр компьютерных средств (в частности, носителей данных).

При общем осмотре производятся следующие действия: изучение содержимого протоколов осмотра, обыска и др. (при их наличии) с целью учета в дальнейших исследованиях особенностей выполнявшихся ранее следственных действий; изучение оборудования и уяснение его связи с другими КЭС. В случае проведения экспертизы в экспертном учреждении - осмотр упаковки на целостность (коробок, пакетов, мешков и пр.), наличие и состояния печатей, подписей следователя и понятых, установление полного соответствия представленных материалов перечню приложения, сопроводительного письма и постановления о назначении экспертизы. Осмотр производится путем вскрытия упаковки и сверки содержимого вложений внутренней описи, составления описи объектов исследования по факту и фиксирования целостности упаковки, вложений и признаков механических повреждений.

Внешний осмотр КЭС и носителей информации производится: путем установления форм-факторов (фиксируются размеры корпуса, его особенности, наличие устройств для

работы с носителями информации, наличие и состав разъемов, плат расширения, заглушек, наклеек, маркировок); конструктивных особенностей и параметров принтеров, сканеров клавиатур, мониторов, устройств-манипуляторов типа «мышь», шнуров питания и т.д.; определения типа носителей данных (информации) (НЖМД, ГМД, компакт-диск, стриммерная кассета, FLASH-карта, электронная записная книжка, магнитооптический диск, ZIP-диск и др.). Фиксирование признаков механических повреждений компьютерной техники и носителей информации, затрудняющих работу с ними в обычном (штатном) режиме, позволит впоследствии эксперту выяснить необходимость исследования нештатного состояния аппаратного средства, а также серийных и инвентарных номеров осматриваемых объектов.

Осмотр экспертом компьютерных или радиоэлектронных объектов должен заканчиваться подробным описанием признаков исследуемых объектов.

Для аппаратных объектов этими признаками являются: тип (вид, модель); форм-фактор и геометрические размеры; цвет; наличие или отсутствие серийного номера, кода и т.п.; отличительные признаки и особенности с полным их описанием и составом (кнопки, переключатели, наклейки, характерные надписи, повреждения) и т.д. Проведение осмотра объектов экспертом рекомендуется сопровождать фиксированием на цифровую видео- и фотокамеру. Полученные изображения оформляются в виде фототаблицы, распечатываются и прикладываются к заключению эксперта в части, касающейся описания объектов.

Выдвижение экспертных гипотез. Экспертом выдвигается рабочая гипотеза (экспертная версия), в которой им формируется предположения о том, какими, по мнению эксперта, могут быть результат исследования и выводы, а также предполагаемые аппаратные методы, которые будут использованы для достижения предполагаемого результата. На основе этого предположения эксперт составляет план экспертного исследования, который представляет из себя логически проработанную последовательность действий, предпринимаемых экспертом с целью оптимального решения поставленной задачи. Логическая проработанность и обоснованность, с криминалистической точки зрения и придают впоследствии заключению статус доказательства.

Проведение организационно–технических мер. Эти экспертные действия необходимы для обеспечения технологической стороны исследований. Они включают в себя определение требуемого экспертного инструментария, который представляет собой аппаратное и программное обеспечение компьютеризированного рабочего места эксперта (КРМЭ) и организационно-методическое, в которое входят сертифицированные экспертные методики, рекомендации, справочное и каталоговое обеспечение, инструкции, техническая документация на аппараты и т.д. Эксперту необходимо также определить способ

взаимодействия с другими экспертами в случае необходимости проведения комплексной комиссионной и дополнительной экспертизы.

Анализ результатов исследования и формулирование выводов.

Необходимо отметить, что ст.25 Закона «О государственной судебно-экспертной деятельности»[32], ст. 204 УПК РФ указывают основания и принципы изложения экспертного заключения в самых общих чертах. Исходя из специфичности судебного аппаратно-компьютерного исследования, на основании вышеуказанных источников можно в целях систематизации и методических требований к изложению полученного экспертного материала предложить трехуровневую «условную» структуру заключения: вводный, исследовательский и заключительный разделы.

Во вводном разделе в соответствии со ст. 204 УПК РФ указываются формальные данные эксперта и его квалификация и экспертного учреждения, основания проведения экспертизы, вопросы, поставленные перед экспертом, предоставленные эксперту аппаратные объекты и материалы, отмечаются лица, присутствующие при экспертизе (см. ст. 204 УПК РФ).

В исследовательском разделе также отмечаются лица, присутствующие при экспертизе, дается обоснование применяемым методикам исследования, их характеристикам. Производятся само исследование аппаратного объекта, содержание и результаты исследования.

В заключительном разделе даются выводы по поставленным перед экспертом вопросам и их обоснование с подборкой иллюстративного материала.

При экспертном исследовании аппаратного средства, в ходе которого решается задача его идентификации, подводится итоговая оценка совпадающих и различающихся признаков сравниваемых объектов, констатируется, что совпадающие признаки являются или не являются устойчивыми, существенными и образуют или не образуют индивидуальную, неповторимую их совокупность. Например, номер материнской платы совпадает с паспортными данными, указанными в техпаспорте на ПК; номер IMEI для мобильного терминала сотовой связи совпадает с номером на представленной коробке; выявленный номер кредитной ЧИП-карты соответствует PIN - коду названному лицом, держателем карты, и т.д.).

При исследовании КЭС, в ходе которого решается задача по его диагностике, выполняется итоговая оценка выявленных диагностических признаков, например, аппаратная конфигурация компьютерной системы и установленное на нем ПО позволяют

---

[32] *Волеводз А.Г. Противодействие компьютерным преступлениям. М., 2002. С. 159.*

выполнить распечатку представленного денежного знака; с исследуемой кредитной карты был прокатан данный слип; и т.д. Констатируются устойчивость, существенность и неповторимость установленной функциональной совокупности применительно к исследуемому аппаратному объекту (системе).

Рассмотрим далее основные положения по обнаружению (поиску), фиксации и изъятию компьютерной информации. Известно, что любое следственное действие состоит из трех этапов: подготовки к проведению, рабочего этапа и протоколирования результатов. Производство осмотра или обыска в помещениях, где находится много компьютерных устройств, работает множество людей, сопряжено со значительными трудностями. Для проведения таких объемных и крупномасштабных следственных действий зачастую необходимо привлечение большого количества работников правоохранительных органов, включая сотрудников силовых подразделений, поскольку лица, в отношении которых расследуются уголовные дела, часто оказывают серьезное сопротивление. Число участников такого объемного следственного действия достигает нескольких десятков, а подчас и сотен, поэтому важнейшим элементом его проведения является четкая организация, инструктаж каждого участника о целях и задачах следственного действия.

Владение такой информацией позволит следователю получить всю криминалистически значимую информацию, хранящуюся в компьютерных устройствах; максимально повысить ее доказательственное значение.

При подготовке к осмотру или обыску полезно допросить (опросить) администратора системы (системного администратора) и выяснить следующие вопросы[33]:

- какие операционные системы установлены на каждом из компьютеров;
- какое используется программное обеспечение;
- какие применены системы защиты и шифрования;
- где хранятся общие файлы данных и резервные копии;
- каковы пароли супервизора и администраторов системы; какие зарегистрированы имена и пароли пользователей.

Другой причиной выбора того или иного компьютерного средства является подозрительное поведение обыскиваемого, его неубедительные объяснения по поводу данного устройства, файла, программы, несоответствие обнаруженных компьютерных средств или программ личности обыскиваемого. Важную роль при этом играет умение следователя подмечать мелкие детали, факты, явления, т.е. его способность к длительным целенаправленным наблюдениям,

---

[33] *Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М.: ООО Издательство «Юрлитинформ», 2005. С. 145.*

Включать и выключать компьютеры, производить с ними какие-то манипуляции может только специалист, участвующий в производстве данного следственного действия. Если на объекте было отключено электроснабжение, например, в связи с пожаром или взрывом, до его включения следует проверить, находятся ли все компьютеры и периферийные устройства в отключенном состоянии.

Если компьютер на момент начала осмотра (обыска) оказался включен, необходимо оценить информацию, изображенную на дисплее и определить, какая программа исполняется на данный момент. В случае работы стандартного программного обеспечения нельзя приступать к каким-либо манипуляциям на входе без предварительного визуального осмотра технических средств. Экран монитора необходимо сфотографировать. Отключить все телефонные линии, подключенные к компьютеру (если таковые соединения имеются).

В протоколе необходимо описать все соединения на задней стенке системного блока. Если это признано целесообразным, вскрывается кожух системного блока и визуально определяют конфигурацию ЭВМ, описывают месторасположение электронных плат. Следование данной рекомендации позволит обезопасить поиск информации от различного рода устройств повреждения или уничтожения как аппаратных средств, так и информационной базы. Такими устройствами могут быть электронные ключи, радиозакладки, шумоподавители. В случае, если при осмотре аппаратных средств выявлены неизвестные участникам следственного действия устройства (платы расширения, нестандартные соединения), компьютер необходимо сразу выключить. При этом следует не отключать тумблер блока питания, а вынимать вилку из розетки.

Если для поиска информации задействуется программное обеспечение, не находящееся в компьютере, это необходимо отметить в протоколе. Такие программы должны быть стандартны и лицензированы, а контроль за их работой - нагляден, т.е. все ключевые этапы работы программы должны изображаться на экране монитора, и специалист должен комментировать происходящее. Максимально активное участие понятых при поиске информации важно еще и потому, что результатом выполнения искомой программы может явиться не текстовый или графический документ, а аудио- или видеоролик. Такой итог работы программы будет уникальным (неповторимым) и зафиксировать эту информацию можно только запротоколировав ее, а также использовав фотосъемку или видеозапись. В случае обнаружения искомой информации, текущее изображение экрана монитора также необходимо сфотографировать, после чего стандартными средствами переписать информацию на постоянный носитель.

Особого внимания требуют места хранения носителей информации. Если при внешнем осмотре компьютеров в их составе обнаружены устройства типа стримера,

магнитооптического накопителя и им подобные, то необходимо найти места хранения носителей информации к соответствующим накопителям. Кроме того, в учреждениях с развитой локальной сетью, как правило, производится регулярное архивирование информации на какой-либо носитель. Поэтому очень важно выявить это место хранения данных копий.

Только после выполнения указанных выше мероприятий специалист, участвующий в следственном действии, может произвести изъятие носителей информации. В отдельных случаях специалистом может быть выполнено копирование компьютерной информации на заранее приготовленные носители. Это могут быть 3.5» дискеты, однако при большом объеме изымаемой информации рекомендуется использовать такие носители данных, как дополнительный жесткий диск, магнитооптические диски. Носители, на которые была переписана информация, должны быть упакованы в пластиковые коробки. Если изымается жесткий диск (винчестер), то его необходимо упаковать в антистатический (т.е. исключающий воздействие статического заряда) пакет, предотвратить его свободное перемещение в упаковке при транспортировке) и опечатать.

В случае принятия решения изъять компьютерные средства требуется учесть как все компьютеры, так и носители данных. При осмотре документов следует обратить особое внимание на рабочие записи сотрудников, где могут содержаться пароли, коды доступа и прочие вспомогательные данные. Необходимо также составить список внештатных и временно работающих специалистов организации, среди которых следует выявить всех специалистов по компьютерным технологиям.

В протоколе следственного действия следователь описывает основные физические характеристики изымаемых устройств, их видимые индивидуальные признаки, конфигурацию компьютерных средств (их комплектацию); номера моделей и серийные номера каждого из устройств; инвентарные номера, присваиваемые бухгалтерией при постановке средства на баланс организации; иную информацию, имеющуюся на фабричных ярлыках фирмы-изготовителя.

Наложение ареста

Современное российское законодательство не предусматривает такого следственного действия, как наложение ареста на локальную вычислительную сеть, но предусматривает наложение ареста на имущество обвиняемого, подозреваемого или лиц, несущих по закону материальную ответственность за их действия, или иных лиц, у которых находится имущество, приобретенное преступным путем в целях обеспечения гражданского иска или возможной конфискации имущества. Причем наложение ареста на имущество может быть произведено одновременно с выемкой или обыском либо самостоятельно (ст.

115 УПК РФ). Наложение ареста на имущество или денежные средства, принадлежащие ответчику как мера по обеспечению иска допускается и ст. 140 ГПК РФ161 и ст. 91 АПК РФ162. По смыслу статей наложение ареста на имущество препятствует собственнику имущества им распоряжаться[34].

Аналогично сущность наложения ареста на вычислительную сеть, состоит в запрете доступа к сети ее собственников и пользователей. Таким образом, достигается обеспечение минимального изменения состояния информационных ресурсов, хранящихся в локальной вычислительной сети, а также предупреждается несанкционированная модификация компьютерной информации. Отметим, что подобная практика наложения ареста на локальные вычислительные сети существует уже во многих странах (Голландии, Бельгии, США). Наложение арестов на вычислительную сеть, допускаемые в этих странах, позволяют сохранить криминалистически значимую информацию, которая легко может быть удалена как умышленно, так и случайно при неквалифицированном обращении с вычислительной сетью и носителями информации.

4. ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ.

Внедрение информационных технологий в уголовное судопроизводство вызвало необходимость совершенствования как теории уголовно-процессуальной науки, так и криминалистики. Не избежала этого влияния и теория косвенных доказательств, которая справедливо занимает центральное место в науке уголовного процесса.

В качестве первого шага для реализации поставленной цели создана компьютерная программа «Форвер» (формирование версий), которая рассчитывает корреляционные связи и условные вероятности между признаками криминалистической характеристики преступлений[35].

Криминалистическая характеристика в данной программе выступает в качестве электронной базы данных ранее раскрытых уголовных дел. Несмотря на то, что представление о корреляционных связях в криминалистике сформировалось более 30 лет назад, прогресса в их установлении без использования теории вероятностей не было. Ранее не были предложены методы расчета таких связей. К вышеприведенным положениям,

---

[34] *Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М.: ООО Издательство «Юрлитинформ», 2005. С. 145.*

[35] *Толстолуцкий В. Ю., Рыбочкин А. В. Программа формирования следственных версий (ФОРВЕР Следователь). Свидетельство о государственной регистрации программы для ЭВМ № 2013660539.*

раскрывающим уголовно-процессуальное и криминалистическое содержание условной вероятности, можно добавить следующее: найденное решение проблемы заключается в том, что корреляционная связь между криминалистически значимыми признаками рассматривается как состоящая из двух связей - прямой и обратной. Такой подход позволяет не только использовать понятие условной вероятности, но обеспечивает конкретизацию внутри корреляционной связи, влияние одного признака на другой. Как правильно было указано А. А. Эйсманом, главный факт может выступать причиной, следствием, условием появления частных фактов[36].

Для расчета указанных вероятностей используется база данных раскрытых уголовных дел. В основе методики ISSN 1997-292X N 11 (49) 2014, часть 2 155 расчета лежит понятие частотной вероятности[37]. В число методов использования программы включен расчет условных вероятностей на основе теоремы Байеса. От следователя требуется формализовано описать место происшествия и следы преступления, что достигается заполнением предлагаемых программой полей ввода данных.

Под электронной криминалистической характеристикой понимается система криминалистически значимых признаков и их значений, предназначенная для выдвижения следственных версий, и представляющая собой совокупность элементов:

1) классификатора базы данных, содержащего криминалистически значимые признаки;

2) электронной базы данных раскрытых уголовных дел;

3) алгоритмы обработки криминалистической информации, позволяющих составить перечень версий и рассчитать их условные вероятности подтверждения в конкретной следственной ситуации.

Таким образом, под электронной криминалистической характеристикой понимается система криминалистически значимых признаков и их значений, предназначенная для выдвижения следственных версий. Данная система представляет собой совокупность следующих элементов: классификатора базы данных; электронной базы данных раскрытых уголовных дел; алгоритмы обработки криминалистической информации.

Программная реализация электронной криминалистической характеристики преступлений выражается в применении виртуальной среды для обучения студентов, а так

---

[36] Селиванов Н.А., Танасевич В.Г., Эйсман А.А., Якубович Н.А.; Юрид.лит., М./1978./С.123-127

[37] Компьютерная программа формирования следственных версий и учебно-методический комплекс, обеспечивающий ее изучение и использование в раскрытии убийств [Электронный ресурс].
URL: http://www.unn.ru/ law/index.php?option=com_content&view=article&id=336&Itemid=278

же используются графическая реконструкция фактических обстоятельств и превращение создаваемой модели в доказательство.

Обучение по использованию электронной криминалистической характеристике преступлений должно осуществляться на криминалистическом полигоне, где обучающийся проходит все этапы криминалистической методики расследования преступлений, а на занятиях по тактике осмотра места преступления изучается несколько видов криминалистической деятельности, сочетая эксперимент с использованием программы «ФОРВЕР».

Выдвижение и проверка версий является неотъемлемой частью производства отдельного следственного действия и обеспечивает целенаправленность всего хода расследования.

В силу высокой практической значимости рассматриваемого вопроса он не раз рассматривался на научно-практических конференциях следователей. Например, следственное управление Прокуратуры Тамбовской области в 2017 году издало «Информационно-методическое письмо о значимости осмотров мест происшествий по делам об умышленных убийствах и протоколах данного следственного действия». В этом письме приводятся рекомендации по осмотру места происшествия и отмечается, что на статической стадии осмотра необходимо «выдвижение версий о круге лиц, среди которого может (или могут) находиться убийца (убийцы) на основе взаимосвязей характеристик места убийства, пола и возраста жертвы, рода ее занятий и сферы деятельности, характеристик нанесенных жертве ранений и иных повреждений, действий убийцы в отношении тела и одежды трупа, мотива убийства с характеристиками лиц из круга, обычно совершающих убийства, соответствующие обнаруженному случаю.

Отмеченное положение дел обусловило принятие дополнительных мер для решения поставленной задачи. В качестве одного из способов внедрения все тех же криминалистических рекомендаций в деятельность каждого следователя было решено разработать справочную систему в виде компьютерной программы. Одновременно проводилась работа по накоплению статистической базы данных на текущем материале.

К началу 2019 года в отделе криминалистики прокуратуры была собрана статистика, отражающая результаты раскрытия и расследования убийств, совершенных в области за последние 3 года. Были заполнены 480 специальных справок, в каждой из которых отмечено более 300 признаков. Проведенная работа позволила перейти к разработке компьютерной программы формирования версий («ФОРВЕР»). В число разработчиков проекта «ФОРВЕР» вошли работники областной прокуратуры и сотрудники двух факультетов ННГУ им Н.И.

Лобачевского – юридического факультета и факультета вычислительной математики и кибернетики.

Компьютерная программа должна была решить задачу информационной поддержки раскрытия убийств, совершенных без очевидцев. В качестве методологической базы был избран метод расследования неочевидных убийств Л.Г. Видонова, который вошел в научно-исследовательский коллектив в качестве одного из разработчиков компьютерной программы.

Первоначальный вариант компьютерной системы полностью воспроизводил методическое руководство Л.Г. Видонова, изданное им в 2002 году. После запуска программы у следователя запрашивались данные о характеристике места преступления, пол и возраст жертвы, предполагаемый мотив преступления. Ввод указанных сведений в первом варианте программы осуществлялся путем выбора из меню щелчком левой кнопки мышки. После ввода необходимых сведений программа автоматически определяла номер следственной ситуации и выводила на экран (с возможностью распечатки на принтере) два различных документа. Первым из документов был перечень типовых характеристик убийц, позволяющий выдвинуть наиболее вероятную версию в данной следственной ситуации. Вторым документом была типовая программа сбора первичной информации среди населения, проживающего неподалеку от места совершения убийства, необходимая для выдвижения конкретных версий, уникальных для данного убийства.

Попытка внедрения в следственную практику первого варианта компьютерной программы закончилась полным провалом. Анализ причин, обусловивших отрицательный результат, позволил выделить две основные группы.

К первой группе причин можно отнести вполне ожидаемые до разработки компьютерной программы факторы, такие как обусловленное здоровой субъективной консервативностью сопротивление сложившейся на практике системы расследования любым нововведениям. К этой же группе мы отнесли ряд известных проблем, носящих типовой характер для процесса компьютеризации любого вида деятельности. К ним может быть отнесена, например, проблема обеспечения следователей компьютерной техникой, а также обучения следователей применению программного продукта. Кроме того, следует указать противоположное консервативности, творческое восприятие продвинутыми следователями программы, выразившееся в появившемся у следователей желании добавить в нее элементы экспертной системы, то есть расшить ее возможности в направлении качества информационного сервиса. Несмотря на положительный характер подобного отношения к программному продукту, в целом, такой подход следователей оказал негативное влияние на процесс внедрения ее в практику. Вместо решения сугубо прикладной задачи – использования содержащихся в программе сведений для выдвижения версий и реализации

программ сбора первичной информации в ходе производства осмотра места происшествия, следователи требовали от разработчиков улучшения программного продукта, при этом сами абсолютно не изменяли своих методов расследования. В результате происходило разделение программы и практической деятельности, приводящее к тому, что совершенствование программы становилось оторванным от практики упражнениями программистов.

Вторая группа причин отсутствия реального применения в расследовании первоначального варианта программы «ФОРВЕР» рассматривалась как наиболее существенная, по отношению к первой группе. Входящие во вторую группу причины носили уже не организационный, а специфический криминалистический характер. Среди этих проблем, прежде всего, следует указать тот факт, что не все следователи приняли положенную в основу программного продукта научную методологию. По этой причине, возникла необходимость разделить обучение следователей использованию компьютерной программы от обучения основам частной криминалистической методики расследования неочевидных убийств. Таким образом, были сформулированы две весьма существенные причины, первая из которых относилась к теории и методологии криминалистики, вторая к системе обучения следователей новым криминалистическим подходам, существующим в методике расследования неочевидных убийств.

Следует рассмотреть проблемы обучения. Параллельно совершенствованию программы «ФОРВЕР» за период с сентября по декабрь 2019 года ежемесячно отделом криминалистики организовывалось и проводилось, в том числе с выездом на одну неделю в п. Мулино, обучение следователей основам частной криминалистической методики расследования и прежде всего проблемы раскрытия неочевидных убийств. На лекционных и семинарских занятиях рассматривались взятые из конкретных уголовных дел ситуационные задачи, решение которых обеспечивается алгоритмами, положенными в основу программы «ФОРВЕР». Следует отметить, что кроме заранее подготовленных учебных задач, на семинарских занятиях анализировались реальные уголовные дела, подбор которых производился самими обучаемыми, из их личного опыта. В качестве подготовки к семинару следователи готовили справки по одному из раскрытых ими уголовных дел. В результате такого подхода к обучению, следователями усваивали научную методологию, положенную в основу компьютерной программы «ФОРВЕР», у многих возникла заинтересованность в получении программного продукта и желание использовать его в своей практической деятельности. Таким образом, был найден путь, в котором одновременно решались две задачи: во-первых, у следователей создавались профессиональный интерес к данной методике и необходимая мотивация по использованию программного продукта, во-вторых, профессиональная подготовка и обучение новым методам органично увязывались с

механизмом выдвижения версий, построенным на новых криминалистических приемах, представляющих собой информационные технологии расследования.

Опыт разработки компьютерной системы, обеспечивающей информационную поддержку раскрытия убийств, совершенных без очевидцев, показывает, что следует на первом этапе ее внедрения целесообразно разделять криминалистическую подготовку следователей от обучения использованию компьютерной программы.

Целесообразность отмеченного разделения объясняется в первую очередь тем, что задачей организации криминалистической подготовки следователей должно стать усвоение ими новой криминалистической методологии, реализованной в компьютерной программе «ФОРВЕР».

Только после того, как успешно усвоена новая криминалистическая методология и частная криминалистическая метода раскрытия убийств, совершенных без очевидцев, применение программы «ФОРВЕР» становится проблемой, сводящейся уже к техническим навыкам работы с программным продуктом, логику работы которого пользователь полностью понимает.

В связи с чем, следует рассмотреть содержание новой криминалистической методологии, усвоение которой составляет первый этап криминалистической подготовки следователей по применению компьютерной программы «ФОРВЕР». В ней выделены две группы вопросов: 1) основные теоретические положения криминалистики, обеспечивающие применение в расследовании информационных технологий, и 2) последовательность действий следователя, реализующего частную криминалистическую методику. Решение комплекса вопросов первой группы обеспечивает решение второй группы вопросов. Разработка теории криминалистики в части разработки средств решения информационных задач переходит в практическую реализацию и выражается в создании для следователя однозначно понимаемых программ действий в типовых следственных ситуациях. До появления компьютеров и компьютерных программ в криминалистике исследовались вопросы программирования расследования.

Рассмотрены теоретические основы использования информационных технологий в деятельности по выявлению и раскрытию преступлений. Большинство современных учебников по криминалистике содержат раздел, посвященный применению компьютеров. Возросшее за последнее десятилетие значение излагаемых в этом разделе закономерностей нашло свое выражение в том, что они стали рассматриваться в качестве самостоятельной частной криминалистической теории. Так А.Г. Филиппов выделяет в качестве частной

криминалистической теории «Основы применения ЭВМ в раскрытии и расследовании преступлений»[38].

С.И. Цветков указал ряд закономерностей, составляющих рассматриваемую частную криминалистическую теорию: методическое обеспечение расследования преступлений, использование средств вычислительной техники непосредственно следователем, решение аналитических задач, информационное обеспечения работы следователей на базе АИПС и некоторые другие аспекты. В первой из отмеченных закономерностей С.И. Цветков выделил следующие направления использования средств вычислительной техники, связанные с методическим обеспечением расследования преступлений:

- контроль за исполнением указаний, данных по уголовным делам в порядке ч.2 ст. 38 УПК РФ;

- учет сведущих лиц, которые могут быть привлечены к расследованию различных категорий преступлений;

- получение информации с помощью компьютерных справочных систем;

- компьютерные системы поддержки процесса принятия тактических решений по расследованию различных категорий преступлений;

- компьютерный расчет данных криминалистической характеристики отдельных видов преступлений для отдельных регионов;

- компьютерный анализ интенсивности криминальных связей между различными городами и районами того или иного субъекта Российской Федерации;

- компьютерные сборники типовых планов расследования, методических рекомендаций, информационных писем[39].

В число вопросов, относящихся к использованию средств вычислительной техники непосредственно следователем автор отнес:

- составление процессуальных документов на основе библиотек «компьютерных бланков».

- планирование расследования по уголовному делу и календарное планирование;

- использование компьютера как средства связи;

---

[38] Филиппов А.Г. Указанная частная криминалистическая теория отнесена им в самостоятельный раздел криминалистической науки: «Организация раскрытия и расследования преступлений». Общие положения организации раскрытия и расследования преступлений (криминалистические аспекты) / Криминалистика. Учебник. Под ред. А.Г. Филиппова. М. Юриспруденция. 2020. С. 207.

[39] Цветков С.И. Использование средств вычислительной техники при расследовании преступлений / Криминалистика: учебник / под ред. А.Г. Филиппова. – 3-е изд. М. Спарк. 2017. С.434.

- автоматизация информационно-аналитической работы при расследовании уголовного дела.

Под решением аналитических задач автором понимает составление сложных аналитических процессуальных документов: обвинительных заключений, постановлений о продлении сроков следствия и содержания обвиняемого под стражей и других. В качестве примера приводит работу программы «Бинар-3», которая позволила резко сократить время, затрачиваемое на составление обвинительных заключений по наиболее сложным и большим по объему делам[40].

Вышеуказанные сведения из литературы приведены для того, чтобы подтвердить правильность мнения Р.С. Белкина, отметившего, что ни один из созданных в результате перечисленных разработок программных продуктов не решает центральную для криминалистической методики проблему – использования компьютерных программ для выдвижения версий, их проверки и планирования расследования, использования сведений, приведенных в криминалистической характеристике преступлений. Отсутствие удовлетворительного решения этой проблемы стало одним из оснований для заявления Р.С. Белкина о том, что криминалистическая характеристика, не оправдав возлагавшихся на нее надежд и ученых, и практиков, изжила себя[41].

Указанная Р.С. Белкиным проблема носит комплексный характер и требует решения на уровне криминалистической теории. На первый взгляд проблема криминалистической характеристик преступлений не имеет отношения к проблемам «компьютеризации» криминалистической методики. Однако, это не так. Криминалистическая характеристика представляет собой сведения, которые с помощью использования ЭВМ создают условия информационного обеспечения методики расследования. Поэтому на этапе постановки задачи при создании компьютерного программного обеспечения перед разработчиками программы фактически ставится задача автоматизации имеющихся криминалистических рекомендаций по методике расследования отдельных категорий дел.

Примером, подтверждающим указанное положение, может служить и опыт других разработчиков программных продуктов, например, перечень задач, изложенных Е.П. Ищенко и АА. Топорковым, которые целесообразно решать с помощью компьютерной техники:

1) автоматизация деятельности следователя на стадии возбуждения и расследования уголовных дел (АРМ следователя);

---

[40] Цветков С.И. Использование средств вычислительной техники при расследовании преступлений / Криминалистика: учебник / под ред. А.Г. Филиппова. – 3-е изд. М. Спарк. 2018. С.435.

[41] Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. НОРМА. 2017. С. 223.

2) автоматизация учета и контроля за расследованием уголовных дел в следственном подразделении (АРМ руководителя);

3) создание автоматизированных информационно-рекомендующих систем, содержащих типовые методики расследования отдельных видов преступлений;

4) фиксация обстановки места происшествия для его компьютерной визуальной реконструкции с построением схем этого места;

5) автоматизация криминалистических учетов, в особенности дактилоскопических и т.д.[42]

Обращает на себя внимание то, что все задачи, изложенные Е.П. Ищенко и А.А. Топорковым, представляют собой не что иное, как автоматизацию некоторых действий или операций. В характере перечисленных задач проявляется ведущее влияние специалистов по программированию. Недостатком такого подхода, используемого в создании компьютерных программ, можно отнести то, что в какой-то части работы делается попытка решить с помощью написания программы проблемы, представляющие собой теоретические задачи криминалистики. Однако нельзя решить «программистскими» средствами нерешенные в содержательном плане криминалистические проблемы.

Во всех перечисленных Е.П. Ищенко и АА. Топорковым задачах основной целью оказывается автоматизация уже выполняемых практиками действий. Процесс автоматизации расследования, ведущийся на базе уже имеющихся методов следственной работы, не повышает эффективность расследования, а наоборот ее снижает. Создавая автоматизированное рабочее место (АРМ) следователя с целью автоматизации некоторых этапов его работы, разработчики компьютерной программы фиксируют сложившуюся систему деятельности. Компьютерная программа должна стать явлением в криминалистике не только новым по форме, но, прежде всего, по содержанию. То есть основываться на новой методологической базе, ряд положения которой уже разработаны в криминалистической теории.

Толстолуцким В.Ю. были рассмотрены основные принципы построения АРМ следователя, изложенные Е.П. Ищенко и АА. Топорковым, и обращено внимание на то, что собственно криминалистическим вопросам уделяется несоизмеримо мало внимания. В основе АРМ следователя оказываются проблемы составления процессуальных документов, то есть те, которые относятся в первую очередь к науке уголовного процесса. По нашему мнению, в учебнике по криминалистике, в силу его ограниченного объема, им стоит уделять

---

[42] *Ищенко Е.П., Топорков А.А. Криминалистика. Под ред. Е.П. Ищенко. М. ИНФРА-М. М. 2015. С. 73.*

внимание лишь настолько, насколько это необходимо, чтобы не нанести ущерб изложению собственно криминалистических проблем.

Авторы пишут, что АРМ следователя позволяет решать следующие задачи:

1) фиксировать в его локальной базе данных тексты допросов, очных ставок, фабул расследуемых преступлений, предъявленных обвинений и на этой основе получать все необходимые по ходу следствия процессуальные документы (протоколы, постановления, запросы и др.)

2) автоматически формировать обвинительные заключения и ходатайства о продлении сроков расследования и (или) содержания обвиняемых под стражей по многоэпизодным групповым делам;

3) фиксировать в базе данных основные моменты движения каждого уголовного дела и проходящих по ним лиц;

4) находить по произвольным поисковым признакам интересующее следователя дело и (или) конкретное лицо.

Резюмируя задачи, которые решаются с помощью АРМ следователя, авторы указывают: «Таким образом, каждое автоматизированное рабочее место следователя снабжено локальной базой данных для хранения конфиденциальной информации по расследуемым делам и обеспечения процессуальной самостоятельности следователя»[43]. В итоге, речь идет в большей степени о документационном обеспечении расследования, чем о задачах, которые являются основными в криминалистической методике расследования.

Высказываемые критические замечания в отношении АРМ следователя не являются утверждением, что работу в это направлении проводить не следует. Целью критических замечаний является попытка показать необходимость движения одновременно и в другом направлении, более важном с точки зрения «компьютеризации» криминалистической методики. Таким направлением является создание, проводимое с учетом современных достижений в области информатики, новой теоретической концепции в области общей теории криминалистики и криминалистической методики. Следует предположить, что перед разработчиками компьютерных программ в области частной криминалистической методики, должен ставиться вопрос о первоначальном создании новой по своей методологической основе криминалистической методики, с последующим решением вопроса ее компьютерной автоматизации.

При такой постановке вопроса на первый план выходит проблема соотношения действий следователя и работы компьютера. Каждый разработчик компьютерных программ,

---

[43] *Ищенко Е.П., Топорков А.А. Криминалистика. Под ред. Е.П. Ищенко. М. ИНФРА-М. М. 2017. С. 74.*

обеспечивающих следственную работу, явно или неявно формулирует свое отношение к проблеме, которую образно представил известный криминалист XX века А.М. Ларин. Эпиграф, подобранный А. М. Лариным к одной из глав своей работы «Криминалистика и паракриминалистика», представляет собой, по выражению автора, студенческий фольклор: «Нам электричество любой заменит труд! Нажал на кнопку – чик-чирик! И тут как тут!»[44]. Рассматривая причины роста нераскрытых убийств, автор пишет: «Не раз уже возникала идея: если интеллектуальные возможности наличных кадров для решения задачи недостаточны, то нельзя ли переложить задачу на умные кибернетические машины?»[45]. На поставленный им вопрос, заключающийся в использовании ЭВМ непосредственно в целях раскрытия преступления, А.М. Ларин дает категорически отрицательный ответ: «Нет двух одинаковых убийств. Построение и проверка версий, обеспечивающие проникновение в тайну убийства, - штучная работа»[46].

Под критику А.М. Ларина попали работы И.Л. Петрухина, осмелившегося указать в 1973 году: «В принципе возможно представить себе процедуру введения в память ЭВМ картотеки из «доказательственных прецедентов», например по вопросу достаточности доказательств…, постепенной накопление этих «прецедентов», а затем «идентификация (сначала родовая, групповая, а затем «индивидуальная») доказательственной ситуации по данному и уже разрешенным делам…»[47].

Комментарий А.М. Ларина к высказанному положению таков: «Осуществление этого проекта, казалось, сделает раскрытие преступлений посильным и для самого неопытного следователя. Почему бы и нет? Введи наличную информацию, нажми кнопку и получи распечатку с готовым решением»[48]. Несмотря на то, что Л.Г. Видонов не предлагал использовать ЭВМ в своей методике, А.М. Ларин с критики «кибернетизации» и «компьютеризации» расследования перескакивает на критику использования статистических методов при формировании криминалистической характеристики убийств. В результате чего работы И.Л. Петрухина и Л.Г. Видонова объединяются и попадают в разряд ненаучных, а сами авторы в число «паракриминалистов». Если учесть, что для криминалистического сообщества того времени, сформированного в период политического руководства страной Коммунистической партии Советского Союза, еще было свежо воспоминание об объявлении

---

[44] Ларин А. М. Криминалистика и паракриминалистика. М.: БЕК, 1996. С. 116.

[45] Ларин А. М. Криминалистика и паракриминалистика. М.: БЕК, 1996. С. 117.

[46] Ларин А. М. Криминалистика и паракриминалистика. М.: БЕК, 1996. С. 117.

[47] Петрухин И.Л. Понятие и содержание оценки доказательств // Теория доказательств в советском уголовном процессе. М., 1973. С. 433-434.

[48] Ларин А. М. Криминалистика и паракриминалистика. М.: БЕК, 1996. С. 118.

кибернетики «продажной девкой империализма», то такая оценка выходила за рамки научной дискуссии, приобретая политическое звучание с вытекающими последствиями.

Сегодня про кибернетику забыли, а взгляды на процесс «компьютеризации» криминалистической методики изменились «с точностью до наоборот». В каждом учебнике криминалистики существует раздел, в котором освещается практика применения компьютеров в следственной работе. Тем не менее, на уровне криминалистической теории еще не найдено научно обоснованного решения поставленного А.М. Лариным вопроса. Существующий в криминалистике теоретический пробел во многом является следствием неконструктивной критики А.М. Ларина, огульно объявившим не научным два отмеченных выше направления криминалистических исследований. Уже и КПСС нет, а созданное А.М. Лариным табу в области криминалистической теории обеспечивает инерцию мышления. Если уж криминалистическая наука до сих пор остается на методологических позициях конца 60-х прошлого века, то не следует требовать большего от рядовых следователей, выросших на соответствующих учебниках криминалистики.

Таким образом, с точки зрения теории, вопрос соотношения криминалистической методики и компьютерных технологий оказывается сложнейшим. К счастью, не одна наука криминалистика столкнулась с этой проблемой. Среди множества предложенных в иных науках решений, кажется наиболее обоснованной позиция П.Я. Гальперина. Являясь представителем психологической науки, П.Я. Гальперин исследовал различие между интеллектуальной деятельность человека и работой компьютера.

П.Я. Гальперин создал теорию поэтапного формирования умственных действий и показал, с одной стороны, некоторое сходство, а с другой - принципиальное отличие между алгоритмом, по которому действует машина и подобной алгоритму последовательностью выполнения действия человеком, названную автором схемой «ориентировочной основы действия».

Автор пишет: «Вот это обстоятельство, немного парадоксальное на первый взгляд, но совершенно понятное, состоящее в том, что человек, не умеющий выполнить данное действие, пользуясь схемой ориентировочной основы действия, с первого раза и каждый раз далее, т. е. не случайно, выполняет это действие правильно. Это показатель того, что вы правильно составили действие. А если человек, следуя вашей схеме (если он отвлекается, то это не нужно брать во внимание), выполняет одно указание за другим и не приходит к намеченному результату, значит, схема не составлена, вы что-то пропустили. Ищите сами! Это всегда было очень важно для нас, вот почему мы затратили свыше 20 лет на все эти истории, ибо далеко не всегда просто составить эту схему.

Значит, такова схема ориентировочной основы действия, представленная в последовательном виде. Ее часто называют алгоритмом, но это не алгоритм в собственном смысле слова, не математический алгоритм, это алгоритмоподобное предписание, причем оно отличается от предписания, которое математика предъявляет к алгоритму, т. е. такое предписание, которое машина выполняет без понимания. А здесь наоборот. Вы всегда составляете каждое предписание с расчетом на понимание человеком. Пусть это совсем маленькое предписание, как у того умственно отсталого ребенка, о котором я вам рассказывал, маленькое понимание, но обязательно понимание. Потому что хотя бы на коротком этапе он сам должен ориентировать свое действие. Он! Действие само же не идет, его направляют. Значит, здесь, вопреки тому, что требуется для вычислительной машины, мы с самого начала рассчитываем на понимание испытуемым того участка действия, на котором он его производит»[49].

В процитированном тексте сформулирована позиция, которая позволяет увидеть, в чем А.М. Ларин был не прав, когда критиковал саму возможность применения ЭВМ в расследовании. Вся критика А.М. Ларина и особенно эпиграф указывают на то, что будто бы можно использовать ЭВМ или компьютерную программу без понимания криминалистических закономерностей процесса расследования: «Введи наличную информацию, нажми кнопку и получи распечатку с готовым решением»[50].

Проведенный анализ критических замечаний противников «компьютеризации» расследования позволил решить весьма важную проблему: нельзя подменять криминалистические рекомендации, ориентированным на машину алгоритмом, выполнение которого не требует понимания криминалистических вопросов и содержания хода расследования. Этот вопрос важен и при разработке проблемы, называемой «алгоритмизацией расследования».

Разработка теории криминалистики в части разработки средств решения информационных задач переходит в практическую реализацию и выражается в создании для следователя однозначно понимаемых программ действий в типовых следственных ситуациях. До появления компьютеров и компьютерных программ в криминалистике исследовались вопросы программирования расследования.

Следует привести мнение Р.С. Белкина о программировании расследования преступлений[51]. Р. С. Белкин связывает формирование раздела криминалистической науки – криминалистической методики – с решением проблемы методической обоснованности

---

[49] Гальперин П.Я. Психология. Четыре лекции. М. Юрайт. 2018. С. 43.

[50] Ларин А. М. Криминалистика и паракриминалистика. М.: БЕК, 1996. С. 118.

[51] Белкин Р.С. Курс криминалистики. 2017. С. 722- 724.

систематизации действий следователя. Термин «методика» был введен, как отмечает Р.С. Белкин, в научный и практический обиход В.И. Громовым в 1929 г. По мере разработки научных основ криминалистической методики, содержание частных методик усложнялось, объем содержащейся в них информации увеличивался. В результате чего, по мнению Р.С. Белкина, использование их непосредственно при работе по конкретному уголовному делу становилось все затруднительнее, адаптация частной методики к обстоятельствам реального случая требовала все более трудоемких процедур. Некоторое время проблему пытались разрешить с помощью издания различных справочников — от справочников типа «Первоначальные следственные действия» до справочников по отдельным действиям: по осмотру места происшествия, по допросу и т.п. Однако эти справочники при всей их положительной роли не могли способствовать оперативному решению возникающих задач в условиях дефицита времени. Руководства по методике расследования тех или иных видов преступлений, методические и практические пособия по частным криминалистическим методикам все более вытеснялись в сферу криминалистического образования и переставали быть практическими инструментами следственной работы.

Возникшая ситуация, по мнению Р.С. Белкина требовала упрощения процесса оценки исходной информации, определения направлений расследования и выдвижения версий[52]. Ряд авторов, в числе Л.Г. Видонов, Н. А. Селиванов, Л.А. Соя-Серко, предложили решение этой поставленной практикой задачи. Предметом исследования указанных авторов, по мнению Р.С. Белкина, стало установление корреляционных зависимостей между элементами криминалистической характеристики по делам об убийствах. Результаты этих исследований демонстрировались в виде схем или кодовых таблиц типовых версий. Эти исследования положили начало новому направлению в криминалистике: «Постепенно умами ученых, работающих в области криминалистических методик, все больше овладевала идея разработки лаконичных программ действий следователя в зависимости от вида расследуемого преступления, исходной информации и складывающихся следственных ситуаций»[53].

Р.С. Белкин верно описывает исторически обусловленную проблему и перечисляет основоположников, которые первыми предложили способы ее решения. Наши исследования продолжили это направление. В ходе работы над программными продуктами для ЭВМ было выдвинуто положение о том, что требуется одновременная разработка технологической карты, которая обеспечивает заданную последовательность действий следователя в ходе осмотра трупа на месте его обнаружения. Сформулированный принцип базируется на том,

---

[52] *Белкин Р.С. Курс криминалистики. 2017. С. 723.*
[53] *Белкин Р.С. Курс криминалистики. 2017. С. 723.*

что никакая программа для ЭВМ не может заменить следователя, поскольку является лишь криминалистическим средством или орудием в системе его деятельности. Способ применения нового криминалистического средства должен быть разработан одновременно с разработкой самого средства орудийной деятельности следователя. Отмеченная закономерность хотя и не выделяется, насколько известно, в криминалистической технике как имеющая самостоятельное теоретическое значение, однако фактически играет роль «неписаного правила».

Перенос отмеченного положения из криминалистической техники в тактику свидетельствует о неразрывной связи и содержательном единстве двух разделов криминалистической науки. Технологическая карта представляет собой самостоятельный вид тактико-криминалистических средств. Отмеченная группа средств должна развиваться параллельно совершенствованию программных продуктов, обеспечивая согласованность действий следователя и используемой им компьютерной программы. В результате, информационные технологии расследования воплощаются в виде взаимосвязанного комплекса: информационно-технологической карты и программы для ЭВМ.

До настоящего времени в криминалистических публикациях не приводятся механизмы формирования версий, а тем более программы, обеспечивающие автоматизацию этого механизма.

Следует отметить, что Р.С. Белкин указал, что программы Л.Г. Видонова не единственный вариант программирования действий следователя, и напомнил, что в 70-х годах ВНИИ МВД СССР были разработаны программы действий оперативной группы, выезжающей на место происшествия. Программы содержали перечень неотложных следственных действий с краткими комментариями, различающимися в зависимости от вида преступлений, и хранились в дежурной части органа внутренних дел. Оперативная группа получала нужную программу-карточку при выезде на место происшествия. Думается, что эти карточки программированных действий были прообразом позднее созданных следственных программ.

Особо интересно, что в связи с проблемой программирования расследования, Р.С. Белкин рассматривает вопрос об алгоритмизации расследования и применения вычислительных машин

Р.С. Белкин ссылается на позицию АА. Эйсмана, который полагал, что в программе, рассчитанной на реализацию самим следователем (в отличие от машинной) должны содержаться как минимум следующие элементы:

1) формулировка задачи либо системы конечных и промежуточных задач применительно к исходным данным;

2) выбор средств и методов решения задачи;

3) оптимальная последовательность действий по решению задачи;

4) вспомогательная информация, способствующая решению задач (по некоторым категориям дел)».

Р.С. Белкин считал, что решение проблемы программирования расследования выдвигает два вопроса: в каком соотношении должны находиться программы действий следователя с соответствующими частными криминалистическими методиками и какая область следственной деятельности должна быть объектом программирования.

Решение первого вопроса обусловлено содержанием частных криминалистических методик. Еще А.А. Эйсман подметил, что поиск новых форм подачи методических данных привел к формализации компонентов частных методик: отсекалась вся мотивировочная или обосновывающая часть рекомендаций, следственные действия излагались в логической последовательности. В результате содержание методики сближалось с типичной программой действий.

Отмеченная закономерность должна учитываться в ходе криминалистической подготовки следователей. Следует поддержать позицию Р.С. Белкина, указавшего, что при этом не должно происходить смешение двух видов методической документации: программы и частной методики. Частные методики излагаются, пояснял Р.С. Белкин, как правило, в руководствах, практических и учебных пособиях, в справочниках и т.п. Они обычно предназначаются для обучения, для формирования у обучающихся определенного комплекса знаний о процессе расследования тех или иных видов преступлений. «По большому счету, - указал Р.С. Белкин, - эти методики не являются рабочим инструментом следователя в силу избыточности содержащейся в них информации и весьма общей связи с конкретными следственными ситуациями. Это именно средство обучения, средство повышения квалификации. Проблема формирования частных методик — предмет дальнейшего рассмотрения; здесь же заметим лишь, что существующая форма изложения методических рекомендаций в виде таким образом формализованных их систем имеет обоснованную функциональную направленность и не требует радикальной перестройки. Нужно только отчетливо представлять, что это не программы действий оперативного характера, а общее руководство к действию»[54].

Рассматривая программы действий Р.С. Белкин отмечал, что «Программы действий следователя не должны подменять собой частные криминалистические методики, но и не должны включаться в их содержание. Это методические разработки прямого действия,

---

[54] *Белкин Р.С. Курс криминалистики. 2017. С. 724.*

рассчитанные на оперативное использование и максимально приспособленные к такому оперативному использованию. Их адаптация к условиям конкретного случая должна быть максимально проста - путем перебора зафиксированных в программе вариантов действий в зависимости от наличной информации»[55].

Следует согласиться с точкой зрения Р.С Белкина, который выделил основной объект создания таких программ: объектом должен служить первоначальный этап расследования, точнее даже — его неотложная часть. «Именно на этом этапе, - пишет автор, - деятельность следователя поддается формализации, число ее вариантов относительно невелико, вариантов исходной информации также немного. Программа действий на начальном этапе расследования действительно способна повысить его оперативность и результативность, риск шаблонизации здесь сравнительно невелик при достаточно квалифицированном анализе исходной информации»[56].

Таким образом, следует отметить, что опыт разработки компьютерной программы «ФОРВЕР» выдвижения версий при расследовании неочевидных убийств позволяет очертить достаточно широкий круг проблем, которые должны решаться одновременно с разработкой программного продукта. В число таких проблем входят: разработка теории криминалистики в части криминалистической методики и познания закономерностей формирования информационных технологий расследования, обучение следователя новым криминалистическим идеям, создание технологических карт, которые представляют собой одновременно и программу действий следователя и средство организации его деятельности, включающей в качестве тактико-криминалистического средства компьютерную программу. Перечисленные проблемы возникли в результате осмысления практики создания и внедрения нескольких вариантов компьютерной программы «ФОРВЕР».

---

[55] *Белкин Р.С. Курс криминалистики. 2017. С. 724.*

[56] *Белкин Р.С. Курс криминалистики. 2017. С. 724.*

ЗАКЛЮЧЕНИЕ

Развитие компьютерной техники и различных гаджетов, их широкое внедрение в различные сферы человеческой деятельности в сочетании с интернетом привело к тому, что практически каждое действие человека оставляет цифровой след. В связи с этим в 2012 году российский законодатель внес соответствующие изменения в Уголовно-процессуальный кодекс Российской Федерации о правилах проведения следственных действий, сопровождающихся изъятием электронных носителей информации (и информации на них), имеющих доказательственное значение для расследования преступлений. Личные и корпоративные электронные носители информации могут быть изъяты следствием как по обоснованным подозрениям, так и в рамках проработки версии преступления, которая в будущем не подтвердится. Поскольку разнообразие противоправных действий, объектом и орудием совершения которых являются цифровые носители информации, постоянно расширяется, следствие прибегает к их изъятию всё чаще. В подобном контексте чёткое понимание порядка изъятия электронных устройств, а также прав их владельцев при осуществлении следственных действий поможет обезопасить себя от злоупотреблений, избежать простоя в работе, а также случайной или временной утери данных, необходимых человеку или предприятию в своей личной, профессиональной и экономической деятельности.

Согласно подп. 3.1.9 ГОСТа 2.051-2013, под «электронным носителем» понимается материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. На практике это могут быть различные носители: компьютеры, мобильные телефоны, блоки, устройства, составляющие материальную часть компьютерной системы, серверы, кассовое оборудование и иные гаджеты.

Изъятие электронных носителей информации может производиться в организациях и жилищах граждан для целей расследования разных преступлений: кража, убийство, террористические акты, превышение полномочий, преступления в сфере экономической деятельности (например, уклонение от уплаты налогов организацией, отмывание денег), кибер-преступлений, а также при расследовании по факту распространения запрещённой на территории РФ информации (например, призывы к нарушению территориальной целостности, призывы к экстремизму, и даже клевета).

Развитие цифровых технологий привело к процветанию киберпреступности и появлению новых форм противоправного поведения в сети, средствами которого являются электронные носители информации. Количество выемок и обысков растет, поиск и изъятие

цифровых доказательств получает все большее значение в расследованиях преступлений, однако не всегда изъятие электронных носителей в итоге оказывается обоснованным. Поэтому важно знать свои права и процедуру при внезапных визитах правоохранителей, а также необходимо заранее позаботиться о внутренней защите данных, например, сохранить резервную копию данных, использовать облачные хранилища данных, чтобы не лишиться значимой информации, необходимой вам для работы и иных нужд.

Компьютерная преступность представляет собой естественный и необходимый результат эволюции постиндустриального общества, основанного на информационных технологиях, дополнительную конформную форму жизнедеятельности, принципиально не поддающуюся ликвидации либо преодолению и требующей адекватных способов и методов регулирования и управления в целях минимизации причиняемого вреда интересам личности, общества и государства, оцениваемая с точки зрения последнего как негативное явление действительности, обладающее признаками профессиональной преступности и в правовой сфере представляющее собой массовое виновное нарушение уголовно-правовых запретов, совокупность всех фактически совершенных вменяемыми лицами, достигшими шестнадцатилетнего возраста, преступлений в сфере информационных технологий.

Однако следует различать компьютерную преступность как правовую категорию и компьютерную преступность как социальное явление. Последнее включает в себя не только совокупность всех преступлений этого вида, но и различные формы тесно связанных с ними «поддерживающей» и организационной деятельности.

К наиболее существенным особенностям компьютерной преступности относятся ее чрезвычайно высокая латентность; организованный и транснациональный характер, базирование на стремительном развитии и использовании телекоммуникационных средств сообщений; постоянное наращивание и совершенствование способов совершения преступлений.

Подводя итог, отметим, что в России назрела острая необходимость в разработке концепции информационной безопасности с обязательным планированием и программированием мер противодействия компьютерной преступности, которые должны охватывать общефедеральный и региональный уровни. Важной составляющей противодействия рассматриваемому типу преступности выступает виктимологический аспект. Интересен в этой связи опыт некоторых зарубежных государств (ФРГ, Франция, США и др.) по созданию общегосударственной системы уведомлений о готовящихся атаках хакеров. Перспективной является идея о предоставлении налоговых льгот пользователям, осуществившим обновление системы защиты информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные акты

1. Конституция Российской Федерации (принята на всенародном голосовании) 12.12.1993 г. // https://www.consultant.ru/document/cons_doc_LAW_28399/
2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_5142/
3. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_9027/
4. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_64629/
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_10699/
6. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_34481/
7. Федеральный закон от 07.07.2003 № 126-ФЗ О связи (ред. от 06.12.2011) // Российская газета, № 135, 10.07.2003.
8. Закон РФ от 07.02.1992 № 2300-1 О защите прав потребителей // Российская газета, № 8, 16.01.1996.

Научная, учебная, справочная литература

9. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М.: ООО Издательство «Юрлитинформ», 2005. С. 145.
10. Багмет А.М., Скобелин С.Ю. Извлечение данных из электронных устройств как самостоятельное следственное действие // Право и кибербезопасность. 2013. № 2. С. 24.
11. Белкин Р.С. Курс криминалистики. М. Юнити-дана. Закон и право. 2017. - 837с.
12. Бычков В.В. Соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений при проверке сообщений о преступлениях и в ходе их расследования // Российский следователь. 2013. № 24. С. 12.
13. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М., 2006. С. 111.
14. Виговский Е.В. Защита прав интеллектуальной собственности. Проблемы и пути решения // Административное право. 2009. № 2. С. 31-40.
15. Волеводз А.Г. Противодействие компьютерным преступлениям. М., 2002. С. 159.
16. Гальперин П.Я. Психология. Четыре лекции. М. Юрайт. 2018. С. 43.
17. ГОСТ Р 57429–2017 Судебная компьютерно-техническая экспертиза. Термины и определения. – М.: Стандартинформ, 2017. – 12 с.
18. ГОСТ Р ИСО/МЭК 27037–2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. – М.: Стандартинформ, 2014. – 48 с.
19. ГОСТ Р ИСО/МЭК 30121–2017 Информационные технологии (ИТ). Концепция управления рисками, связанными с проведением судебной экспертизы свидетельств, представленных в цифровой форме. – М.: Стандартинформ, 2017. – 12 с.
20. Грибунов О.П., Старичков М.В. Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие. – М.: ДГСК МВД России, 2017. – 160 с.
21. Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями: Сб. документов. М., 2001. С. 249.
22. Иногамова-Хегай.Л.В. Уголовное право РФ. Особенная часть. – М. 2010.
23. Ищенко Е.П., Топорков А.А. Криминалистика. М.: МГАЮ, 2015. С. 8

24. Компьютерные преступления и информационная безопасность. М.: Новый юрист, 2009.

25. Компьютерная программа формирования следственных версий и учебно-методический комплекс, обеспечивающий ее изучение и использование в раскрытии убийств [Электронный ресурс]. URL: http://www.unn.ru/ law/iNdex.php?optioN=com_content&view=article&id=336&Itemid=278 (дата обращения: 02.06.21).

26. Ларин А.М. Криминалистика и паракриминалистика. М.: БЕК, 1996. С. 117.

27. Масалков А.С. Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.

28. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. М., 2009. С. 184.

29. Петрухин И.Л. Понятие и содержание оценки доказательств // Теория доказательств в советском уголовном процессе. М., 2018. С. 433-434.

30. Преступления в сфере компьютерной информации: квалификация и доказывание / Под ред. Ю.В. Гаврилина. М., 2009. С. 380.

31. Рассолов И.М. Киберпреступность: понятие, основные черты, формы проявления // Юридический мир. 2008. № 2.

32. Селиванов Н.А., Танасевич В.Г., Эйсман А.А., Якубович Н.А.; Юрид.лит., М./1978./С.123-127

33. Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия. Курган, 2009.

34. Слыщенков В.А., Левин А.Е. Охрана программ для ЭВМ: в поисках эффективных правовых решений // Юрист. 2010. № 8. С. 8-15.

35. Толстолуцкий В. Ю., Рыбочкин А. В. Программа формирования следственных версий (ФОРВЕР Следователь). Свидетельство о государственной регистрации программы для ЭВМ № 2013660539.

36. Торичко Р. С., Клишина Н. Е. Некоторые вопросы совершенствования действующего законодательства, регламентирующего расследование киберпреступлений // Вестник экономической безопасности. — 2018. — № 3. — С. 179—184.

37. Усов А.И., Зубаха В.С. Направление разработки методического обеспечения производства компьютерных экспертиз и исследований. Сб.: Экспертная практика. №47.- М., 1999.

38. Филиппов А.Г. Указанная частная криминалистическая теория отнесена им в самостоятельный раздел криминалистической науки: «Организация раскрытия и расследования преступлений». Общие положения организации раскрытия и расследования преступлений (криминалистические аспекты) / Криминалистика. Учебник. Под ред. А.Г. Филиппова. М. Юриспруденция. 2020. С. 207.

39. Цветков С.И. Использование средств вычислительной техники при расследовании преступлений / Криминалистика: учебник / под ред. А.Г. Филиппова. – 3-е изд. М. Спарк. 2019. С.434.

40. Чекунов И. Г., Рядовский И. А, Иванов М. А. [и др.]. Методические рекомендации по расследованию преступлений в сфере компьютерной информации : учебное пособие / под ред. И. Г. Чекунова. — М. : Московский университет МВД России имени В. Я. Кикотя, 2018. — 106 с.

41. Юрлов И.А. Проблемы правового регулирования оборота компьютерных программ // Правовые вопросы связи. 2010. № 2. С. 12 - 14.

Судебная практика

42. Постановление Пленума Верховного Суда РФ № 5, Пленума Высшего Арбитражного Суда № 29 от 26 марта 2009 г. «О некоторых вопросах, возникших в связи с введением в действие части четвертой Гражданского кодекса Российской Федерации» // БВС РФ. 2009. № 6.