УДК 343.985

УДАЛЁННОЕ ИССЛЕДОВАНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ПРОБЛЕМЫ

А.Н. Иванов

Саратовский государственный университет
E-mail: aivanov@sgap.ru

Статья посвящена малоисследованным вопросам извлечения и исследования компьютерной информации при расследовании преступлений. Анализируются процессуальные проблемы осуществления осмотра и обыска компьютерных систем. Обосновывается принципиальная возможность производства данных следственных действий. Отмечается необходимость разработки тактических приемов удаленного исследования компьютерных систем и содержащихся в них данных.

Ключевые слова: компьютерная информация. удаленный осмотр, удаленный обыск компьютерных систем.

Remote Study of Computer Information: Criminal Procedure and Forensic Problems

A.N. Ivanov

This article is devoted to extracting of extraction and the study of computer information when investigating computer crimes. Analysis of procedural issues in the implementation of inspection and search of computer systems. We substantiate the possibility of these investigations. There is a need to develop tactics remote computer systems and studies of their data.

Key word: computer info, remote inspection, remote searches of computer systems.

Распространение компьютерной техники обусловило ее широкое использование как при совершении преступлений, так и хранении в ней информации, имеющей значение для расследования.

В последнее время в преступных целях все более активно используются возможности коммуникации, представляемые глобальной сетью Интернет. Помимо непосредственного общения (текстового, звукового и визуального) пользователи могут пересылать экземпляры контрафактных произведений, не взирая на расстояния и границы.

Это обстоятельство обусловило появление ряда работ, в которых значительное внимание уделено осмотру компьютерных объектов, обыску, сопряженному с изъятием компьютерной информации, выемке электронных документов.

Обычно приемы осуществления данных следственных действий сопряжены с физическим проникновением в помещение, где находятся компьютеры и иные носители компьютерной информации. Между тем развитие информационных технологий и средств телекоммуникаций позволяют осуществлять и удаленное (дистанционное) исследование компьютерных систем и содержащейся в них информации.

К файлам, устройствам и другим ресурсам сети, которые не принадлежат непосредственно рабочей станции – компьютеру, за которым работает пользователь, применяется понятие «удаленный» (англ. *remote*). Ресурсы компьютера, с которого выполняется работа, считаются локальными.

Возможны различные варианты уделенного исследования компьютерной информации. Удаленное (дистанционное) исследование не носит признаки чрезвычайных действий. Этот метод применяется в повседневной работе многих пользователей, например, при доступе сотрудников различных организаций к удаленным базам данных, в работе администратора сети при исследовании информации на подчиненных компьютерах.

Работа с удаленными ресурсами может осуществляться двояко. Возможно дистанционное управление программами и устройствами удаленно расположенной компьютерной системы. Программы для удаленного управления могут предоставлять доступ к данным, хранящимся на компьютере, даже мобильному пользователю. При дистанционном управлении только клавиатурные действия и экранные обновления передаются между двумя компьютерами, в то время как все вычисления (программы) выполняются на удаленном компьютере. Второй вариант – возможность войти в сеть с удаленного места. Вообще говоря, чтобы связаться с конкретной сетью путем удаленного доступа, требуется компьютер, модем и программное обеспечение. Единственное отличие удаленного компьютера, подключенного через модем, от рабочей станции локальной сети заключается в меньшей скорости передачи данных. Разумеется, допустимо подключение через провайдера и Интернет по выделенной линии.

В принципе удаленный (дистанционный) поиск, извлечение и фиксация компьютерной информации могут осуществляться как в рамках оперативно-розыскных мероприятий, так и следственных действий. На данный момент такими следственными действиями являются осмотр и обыск. Попробуем обосновать возможность и правомерность их дистанционного осуществления.

Под следственным осмотром в криминалистике обычно понимается следственное действие, проводимое для непосредственного обнаружения и исследования объектов, имеющих значение дела, их признаков, свойств, состояния и взаиморасположения[1]. В том или ином вариан-

те подобное определение встречается в работах большинства авторов. Несмотря на некоторые (в основном редакционные) различия в определениях, практически все авторы указывают на такой специфический признак осмотра, как непосредственность восприятия следователем объектов, имеющих значение дела, их признаков, свойств, состояния и т.д.[2]

Несомненно, что участие лица, проводящего осмотр, необходимо на всех его этапах. Вместе с тем в последние годы в криминалистике активно используются термины «виртуальные» следы[3], «электронно-цифровой след»[4], «цифровые доказательства»[5]. Такие следы существуют объективно в памяти технических устройств, в электромагнитном поле, на машинном носителе компьютерной информации, но не доступны непосредственному восприятию. Опосредованное восприятие в данном случае обусловливается тем, что для извлечения и исследования указанных следов необходимо обязательное использование программно-технических средств. Поэтому при определении сущности осмотра указание на непосредственность восприятия является, на наш взгляд, излишним. С другой стороны, «отличительную особенность среди преступлений, совершаемых с использованием информационных технологий, имеют следы преступлений в компьютерных сетях, связанную с тем, что в крупных сетях физическое местонахождение следовой информации и ее носителей (например, конкретного физического сервера) может быть вообще не установлено или он может быть физически недоступен, а возможен только виртуальный доступ по компьютерным сетям. Причем очень часто для следствия физическое местонахождение искомой компьютерной информации не имеет какого-либо значения»[6]. Таким образом, уровень развития телекоммуникационных средств не требует непосредственного присутствия следователя в том месте, где находится компьютерная информация (ее физический носитель). Такая информация может быть извлечена и изъята дистанционно в рамках осмотра или обыска.

Полагаем, что удаленный (дистанционный) осмотр может быть осуществлен при необходимости исследования общедоступных данных, размещенных в открытых источниках, независимо от их географического местонахождения в целях обнаружения следов преступления, например, размещенной на сайте информации (порнографических материалов, призывов к экстремистской деятельности и т.п.), и выяснения иных обстоятельств, имеющих значение для дела. В этом случае следователь с помощью специалиста, в присутствии понятых посещает сайт, осматривает его, устанавливает факт присутствия определенных документов непосредственно на конкретном сайте, сохраняет (копирует) имеющую значение для дела информацию в виде файлов и распечатывает ее, после чего сравнивает распечатку с тем, что имеется на осматриваемом сайте. Результаты, полученные в процессе проведения данного следственного действия, должны оформляться протоколом осмотра документов, к которому приобщаются распечатки содержимого страниц сайта и носители, содержащие скопированную с него информацию. Учитывая простоту создания сайтов в глобальных сетях, а равно возможность быстрого изменения или уничтожения размещенной на них информации, такой осмотр должен стать неотложным и незаменимым следственным действием.

В свое время нами был поставлен вопрос о необходимости выделения нового вида обыска – обыска средств компьютерной техники[7]. На наш взгляд, такой обыск может осуществляться в двух формах: 1) обыск компьютерной техники членами поисковой группы, находящимися в месте, где она расположена; 2) удаленный (дистанционный) обыск компьютерной системы или её частей.

В США возможен обыск без физического проникновения в помещение при условии, что к конкретному компьютеру возможен доступ других лиц с удаленных терминалов по телефонным линиям[8]. Ситуация, в которой обыск осуществляется с использованием удаленного доступа, с компьютера, расположенного, например, в кабинете следователя, порождает ряд проблем процессуального характера, связанных с необходимостью обеспечения прав лица, у которого производится данное следственное действие. Так, до начала обыска следователь должен: обеспечить участие лица, у которого производится данное следственное действие, либо совершеннолетних членов его семьи; предъявить кому-либо из указанных лиц постановление о его производстве, а в случаях, предусмотренных ч. 3 ст. 182 УПК РФ, – судебное решение, разрешающее производство обыска; предложить указанным выше лицам добровольно выдать подлежащие изъятию документы, которые могут иметь значение для уголовного дела. По мнению ряда авторов, «произвести эти мероприятия перед началом обыска в компьютерных сетях не представится возможным»[9]. На наш взгляд, в ситуации, когда проводить обыск в обычном порядке нецелесообразно (например, незамедлительно проникнуть в помещение, где расположены носители компьютерной информации невозможно, а члены семьи обвиняемого (подозреваемого), охрана проинструктированы о порядке и методике действий по уничтожению информации в случае появления членов следственно-оперативной группы), можно пригласить владельца имеющей значение для дела информации к следователю. Затем участвующим лицам (лицу, у которого производится обыск, понятым и др.) разъясняются их права, ответственность, а также порядок производства обыска, их предупреждают о применении технических средств, обыскиваемому предъявляется постановление о производстве обыска и предлагается выдать интересующие следствие документы, хранящиеся в электронном виде

на его компьютере. Естественно, за компьютер обыскиваемое лицо не пускают, ему лишь можно предложить назвать IP-адрес своего компьютера, пароль доступа к информации и т.п. Как видим, выполнить процессуальные требования, установленные в ст. 182 УПК РФ, вполне возможно.

Несколько иначе решается вопрос удаленного обыска в Конвенции о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). В указанной конвенции отмечается, что в случае, когда компетентные органы производят обыск или получают аналогичный доступ к определенной компьютерной системе или ее части и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части и когда такие данные на законном основании могут быть получены из первой системы или с ее помощью, такие органы имеют возможность оперативно распространить производимый обыск или иной аналогичный доступ на другую систему. К сожалению, Российская Федерация в настоящей Конвенции не участвует.

УПК РФ оставляет открытым вопрос: возможен ли обыск в компьютерных системах, соединенных сетью, если такие системы (или устройства в составе соответствующих сетей) расположены вне обыскиваемых помещений (физически расположенных на определенном расстоянии от места производства обыска)? Естественно, что «процессуальное изучение содержимого … сетевой вычислительной системы в реальности отличается по характеру производимых действий от, например, обыска помещения. Для просмотра файлов, содержащихся в системе, как правило, требуются специальные знания, набор специализированных программ и, возможно, особых аппаратных средств. В некоторых случаях такой просмотр удобнее осуществлять удаленно, т.е. осматривать содержимое одного компьютера, находясь при этом за другим»[10].

В литературе справедливо отмечается, что если допустить невозможность осуществления такого обыска, то возникает риск уничтожения данных в период, пока будет получено разрешение на обыск места, где информация физически размещена. В больших сетях зачастую практически невозможно установить точное физическое расположение данных[11]. Очевидно, поэтому среди типовых мест проведения обыска В.А. Мещеряков называет «обыск в автоматизированной информационной системе: сосредоточенной (один или несколько не взаимосвязанных компьютеров в пределах одного помещения), рассредоточенный (локальная вычислительная сеть в пределах одного или нескольких рядом расположенных помещений или зданий), открытой (отдельные компьютеры или их локальные сети объединены через общедоступные коммуникационные каналы связи)[12].

Полагаем, что следователь, проводящий обыск помещения, в котором расположена компьютерная система, вправе обследовать все носители информации, к которыми имеется удаленный доступ с данной системы[13], в том числе и те, которые физически расположены в ином месте (но в пределах территории Российской Федерации) и принадлежат другим лицам. Фактическим основанием для подобных действий, на наш взгляд, является наличие следующих условий: а) в помещении, в котором расположена компьютерная система, на законных основаниях проводится обыск; б) в распоряжении следователя имеются достаточные сведения, позволяющие полагать, что в удаленной компьютерной системе или ее части находятся данные (документы в электронной форме), имеющие значение для дела; в) доступ к интересующим следствие документам возможен с компьютера, расположенного в помещении, в котором уже производится обыск.

В уголовно-процессуальном кодексе следовало бы решить вопросы: должен ли следователь в данном случае вынести постановление о производстве обыска в отношении подсоединенной системы и содержащихся в ней данных, будут ли действия по обследованию другой компьютерной системы считаться самостоятельным обыском, следует ли фиксировать ход и результаты такого обыска в отдельном протоколе? Полагаем, что если лицо, у которого проводится обыск, на законных основаниях хранит компьютерные данные (например, почтовые сообщения) в вычислительной системе провайдера, то постановление о производстве обыска этой системы выносить не требуется. Действия следователя в указанной ситуации, на наш взгляд, можно рассматривать как дополнительный обыск. Соответственно, в случае удаленного обыска, проводимого в определенной компьютерной системе или ее части с компьютера, расположенного в обыскиваемом помещении, его результаты должны фиксироваться в одном протоколе.

Известно, что обыск направлен на обнаружение и изъятие предметов и документов, имеющих значение для дела. По мнению А.П. Рыжакова, «изъятие» в узком смысле этого слова – это действие, в результате которого изменяется место нахождения и хранения обнаруженного в ходе следственного действия объекта[14]. В криминалистике «изъятие понимается как извлечение носителей, источников информации из обстановки, в которой они обнаружены»[15]. В случае удаленного исследования компьютерной системы компьютерная информация не изымается в натуре, а копируется (переносится в материалы уголовного дела), оставаясь в обследуемой системе. Этот факт, как и ряд указанных выше обстоятельств, затрудняет использование в доказывании по уголовному делу информации, полученной в результате удаленного обыска.

К сожалению, отсутствие в УПК РФ норм, регламентирующих основания, порядок и особенности удаленного (дистанционного) исследования

компьютерной информации при расследовании преступлений является существенным пробелом, ограничивающим деятельность следователя по собиранию доказательств. Между тем данная проблема существует, и позицию в отношении подобных процедур необходимо выработать.

На наш взгляд, необходимо внести коррективы в УПК РФ, учитывающие современные достижения в области обработки и передачи компьютерной информации, а также преступить к разработке тактических приемов удаленного исследования компьютерных систем и содержащихся в них данных, которые обеспечивали бы признание полученных данных допустимыми доказательствами по уголовному делу.

Примечания

1 См.: *Белкин Р.С.* Криминалистическая энциклопедия. М., 1997. С. 152.

2 См.: *Колмаков В.П.* Следственный осмотр. М., 1969. С. 18; Криминалистика / Под ред. Б.А. Викторова и Р.С. Белкина. М., 1976. С. 244; Следственные действия. Криминалистические рекомендации. Типовые образцы документов / Под ред. В.А. Образцова. М., 1999. С. 176; *Ищенко Е.П.* Криминалистика: Краткий курс. М., 2003. С. 127; *Баев О.Я.* Тактика уголовного преследования и профессиональной защиты от него. Следственная тактика. М., 2003. С. 75.

3 *Мещеряков В.А.* Преступления в сфере компьютерной информации. Основы теории и практики расследования. Воронеж, 2002. С. 104.

4 *Вехов В.Б.* О понятии, механизме образования и классификации электронно-цифровых, оптических и магнитных следов // Криминалистика в системе правоприменения: Материалы конф. М., 2008. С. 103.

5 *Иванов Н.А.* Цифровые доказательства: понятие и классификация // Криминалистика в системе... С. 130, 133.

6 *Кукарникова Т.Э.* Компьютерная информация как следообразующая система // Там же. С. 148.

7 См.: *Иванов А.Н.* О новом виде обыска // Актуальные проблемы криминалистики на современном этапе. Сб. науч. ст. / Под ред. З.Д. Еникеева. Уфа, 2003. Ч. 1. С. 105–109.

8 См.: *Айков Д., Сейгер К., Фонсторх У.* Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М., 1999. С. 284.

9 *Сумин В.И., Мещеряков В.А., Бородин А.В., Сумин А.В.* Особенности производства обыска при расследовании преступлений в сфере компьютерной информации // Информационная безопасность и компьютерные технологии в деятельности правоохранительных органов. Саратов, 2003. Вып. 2. С. 149.

10 *Осипенко А.Л.* Борьба с преступностью в глобальных компьютерных сетях: Международный опыт. М., 2004. С. 274–275.

11 См.: *Волеводз А.Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002. С. 343.

12 См.: *Мещеряков В.А.* Основы методики расследования преступлений в сфере компьютерной информации: Автореф. дис. … канд. юрид. наук. Воронеж, 2001. С. 28.

13 Вторая система должна быть на законных основаниях доступна для изначально обыскиваемой.

14 См.: *Рыжаков А.П.* Осмотр: основание и порядок производства. Ростов н/Д, 2007. С. 130.

15 *Драпкин Л.Я., Карагодин В.Н.* Криминалистика: Учебник. М., 2007. С. 6.

УДК 341(032)

СИСТЕМА ДОГОВОРОВ ПЕРЕВОЗКИ АВТОМОБИЛЬНЫМ ТРАНСПОРТОМ

О.Ф. Фаст

Саратовский государственный университет
E-mail: fastolga@mail.ru

В статье рассматриваются проблемы воздействия рыночных отношений на формирование системы договоров перевозки грузов автомобильным транспортом. Делается вывод, что большинство договоров, связанных с перевозкой грузов, взаимно дополняют друг друга и образуют взаимосвязанную систему договоров.

Ключевые слова: автомобильный транспорт, система, договоры, реализация.

Motor-Traction Contracts System

O.F. Fast

In the article problems of the market relations influence on the forming of the motor-traction contracts system are analyzed. In the work it is concluded, that the majority of contracts, connected with freight, supplement each other and make interconnected system of contracts.

Key words: transport, road transport, system, contracts, implementation.

Автомобильный транспорт, сохраняя приоритетное положение в хозяйствующих системах России, в условиях перехода к рынку постепенно освобождается от прямого государственного регулирования своей деятельности. Рынок автотранспортных услуг все активнее заполняется коммерческими, частнопредпринимательскими