

О ПРАВОВЫХ ПРОБЛЕМАХ ИСПОЛЬЗОВАНИЯ ДОКАЗАТЕЛЬСТВ, ПОЛУЧЕННЫХ С ПОМОЩЬЮ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Вопрос о том, при каких условиях фактические данные, полученные с помощью средств компьютерной техники, могут являться доказательствами по делу, в настоящее время встает все чаще. В некоторых научных исследованиях предлагается закрепить в Уголовно-процессуальном кодексе РФ новый вид доказательств – документированную компьютерную информацию [1]. Полагаем, что в этом нет нужды, поскольку в целом система таких доказательств подчиняется общей логике доказывания в пределах действующего УПК РФ.

Для раскрытия темы необходимо сначала определить содержание и форму существования в уголовном процессе доказательств, полученных с использованием средств компьютерной техники. Компьютерная информация, которая может быть использована для установления обстоятельств, подлежащих доказыванию, обладает специфическими признаками:

- она хранится, передается и принимается в виде электромагнитных импульсов, сигналов, полей, которые не могут быть восприняты человеком непосредственно. Для человеческого восприятия она переводится в обычный вид с помощью специальных устройств;
- не исчезает при потреблении, легко обрабатывается (с чрезвычайно высокой скоростью) и легко передается;
- может копироваться и переносится без какого-либо ущерба.

Компьютерная информация может храниться на различных носителях. В связи с отсутствием какого-либо законодательного определения понятия носителя компьютерной информации на практике деятельность по расследованию данных преступлений сильно затруднена (например, встают вопросы о том, можно ли считать контрольно-кассовую машину или пейджер электронно-вычислительными машинами «ЭВМ» и т.п.). В связи с этим Н.П. Царева [2] предлагает при определении понятия «иных» документов перечислять носители компьютерной информации в ч. 2 ст. 84 УПК РФ. Однако данное дополнение указанной статьи мы полагаем излишним из-за постоянного возникновения все новых носителей компьютерной информации и технических средств ее перевода в «человекочитаемую» форму. По мнению автора, для нужд практики необходимо не перечислять всевозможные носители компьютерной информации в рамках Уголовно-процессуального кодекса, а дать законодательное определение данного термина или разъяснить его в Постановлении Пленума Верховного суда РФ.

В отличие от традиционных технологий, где информация жестко привязана к физическому носителю – бумаге, в документах, созданных с помощью средств компьютерной техники, форма и содержание относительно самостоятельны из-за технического характера их изготовления. Одна и та же информация в определенный момент времени может находиться на различных типах носителей и иметь несколько форм представления. Например, документ может быть зафиксирован на магнитном диске (в форме статической записи двоичного машинного кода – машиночитаемая форма предоставления) и одновременно существовать с помощью специальных драйверов на экране дисплея или на распечатке-листинге, полученной с помощью специальной программы для принтера (человекочитаемая форма). Поэтому не исключена возможность изменения содержания документа в одной из его форм существования, оставляя в неприкосновенности другие.

Полагаем, что документы, содержащие сведения, которые зафиксированы в виде магнитных записей, магнитооптических накопителей, в виде документов электронной связи, документов, подписанных электронной цифровой подписью или зафиксированных на других носителях посредством современных научно-технических средств, могут являться доказательством по делу и вводиться в уголовный процесс как вещественные доказательства или как «иные документы» (ч. 4, 6 п. 2 ст. 74 УПК РФ).

Вещественным доказательством может являться программное обеспечение, несущее на себе следы преступного деяния (например, взломанная или скопированная программа). Исходя из смысла ст. 84 УПК РФ письменная форма для «иного документа» не является определяющей. «Иным документом» может быть

* © И.Г. Иванова, Юридический институт Красноярского государственного университета, 2006.

признан любой документ материального мира, содержащий словесную, цифровую и иную информацию. Главное условие, чтобы содержащиеся в документе сведения имели значение для дела. В качестве примера «киного документа», полученного с использованием средств компьютерной техники, можно привести документы, удостоверенные электронной цифровой подписью, распечатку текста на бумаге в виде копии (листинг), журналы учета сбойных ситуаций вычислительной техники, журналы рабочего времени и т.п.

Для признания таких электронных документов в качестве доказательств необходимым условием является их удостоверение (т.е. подтверждение того, что они получены из надлежащего источника).

Серьезной юридической и технической проблемой является удостоверение «иных» электронных документов. Так, довольно часто в процессе расследования требуется получение документированной информации в виде log-файлов в соответствии с ч. 4 ст. 32 ФЗ «О связи». Однако при изъятии компьютерной информации в процессе обыска или выемки невозможно обеспечить ее сохранность в том виде, в каком она обнаружена, можно провести лишь ее копирование. В результате подобных действий неминуемо произойдут изменения в файле, связанные с датой и временем самого копирования, что влечет утрату информации о фактической дате и времени создания копируемого файла. Нерешенность данного вопроса в нормах УПК РФ является существенным препятствием признания судом копируемой информации доказательством по уголовному делу. В связи с этим в следственной практике зачастую проводится не копирование информации, а изъятие самих средств компьютерной техники для экспертных исследований, заключение которых и признается доказательством. Тем самым в уголовном судопроизводстве искусственно сужается круг доказательств.

Для того чтобы доказательства могли быть исследованы и оценены следователем и судом, они должны быть представлены в форме, воспринимаемой человеком, поскольку информация в электронно-цифровой форме не воспринимается непосредственно и однозначно человеческими органами чувств. Получение «человекочитаемого» документа на основе расшифровки компьютерной информации ставит перед следователем много вопросов (какие из этих документов считать первоначальными, а какие производными; какой из документов может быть подвергнут экспертизе и т.д.). Полагаем, что бумажная распечатка компьютерной информации (листинг) является производным доказательством (информация приняла новую физическую форму, сохранив свое содержание). Специфика в том, что здесь производное доказательство имеет гораздо большее практическое значение при оценке доказательств, так как его содержательная сторона доступна пониманию всех участников процесса.

В зависимости от тех или иных условий изготовления, хранения или передачи документов правовые нормы должны устанавливать требования к реквизитам документа, соблюдение которых обеспечивает признание юридической силы за его конкретной формой, поскольку визуально сличить содержание жесткого или гибкого диска и бумажной распечатки невозможно.

По нашему мнению, существует несколько вариантов решения указанной проблемы: 1) назначение компьютерно-технической экспертизы в целях установления соответствия сведений на бумажной распечатке («человекочитаемой» форме) и информации, содержащейся на магнитном носителе; 2) проведение самостоятельного следственного действия по снятию распечатки с информации, зафиксированной на магнитном носителе; 3) создание независимой организации, которая могла бы по запросу соответствующих органов фиксировать содержание информации, находящейся на магнитном носителе; 4) перенос интересующей следствие информации на специальный аппаратно-программный комплекс, способный подписывать считываемую информацию электронно-цифровой подписью третьего лица (например, нотариуса) [3]; 5) использование только оригиналов на не перезаписываемых, энергозависимых и однозначно идентифицируемых носителях, все изменения состояния которых на протяжении жизненного цикла восстанавливаемы для рассмотрения.

Все эти пути имеют свои недостатки. В первом методе прослеживается явное загромождение расследования несколькими сложными техническими экспертизами, что неоправданно его затян timer. Недостаток второго, третьего и четвертого способов решения в том, что данные действия требуют внесения изменений в Уголовно-процессуальный кодекс РФ и также усложняют расследование (во втором случае из-за производства дополнительного следственного действия, в третьем и четвертом из-за неоправданного привлечения дополнительных лиц к участию в деле). В пятом варианте накладываются существенные ограничения на структуру и функциональные характеристики таких документов и, как следствие, практическую возможность использования электронных документов в качестве доказательств.

Полагаем, что наиболее оптимальным способом введения в уголовный процесс электронных документов будет изъятие их с помощью специально паспортизованных программ, которые прошли соответствующий контроль на защиту от возможности внесения изменений в распечатываемую (или копируемую) информацию. Данные программы должны проходить обязательную государственную сертификацию и обеспечиваться системой государственной стандартизации. Вопрос о сертификации указанных программ необходимо решать по аналогии с существующей в настоящее время системой по лицензированию и сертификации в области защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М.: Юрлитинформ, 2002. – С. 209-210; Карась И.З. Юридические факты и доказательства в информационных правоотношениях / И.З. Карась // Советское государство и право. – 1988. – № 11. – С. 92.
2. Царева Н.П. Иные документы, допускаемые в качестве доказательств по УПК РФ: дис. ... канд. юрид. наук / Н.П. Царева. – Саратов, 2003. – С. 50.
3. Козлачкова Ю.И. Информация на электронных носителях как источник доказательств в уголовном процессе / Ю.И. Козлачкова // Следователь. – 2003. – № 6. – С. 27.