УДК 343.985.2

В.Ф. Васюков

НЕКОТОРЫЕ АСПЕКТЫ НАЗНАЧЕНИЯ СУДЕБНОЙ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Раскрываются роль и значение судебной компьютерной экспертизы при расследовании преступлений корыстной направленности в сфере информационных и коммуникационных технологий. Основной акцент делается на понятии, задачах, проблемах назначения данного рода экспертиз. Подчеркивается, что судебная компьютерная экспертиза выполнима не только в лабораторных условиях, но и на месте происшествия, когда экспертному исследованию подлежит энергозависимый носитель информации. Внимание акцентируется на задачах, которые стоят перед экспертом, выполняющим такого рода экспертизы. А также значимости компьютерно-сетевой экспертизы при расследовании хищений в ситуациях, где объектом исследования является не отдельный носитель информации, а целый комплекс компьютерных устройств, программных средств в условиях функционирования криптографической защиты информации. Рассматриваются отдельные случаи из следственной практики, когда экспертное заключение по результатам проведения судебной компьютерно-сетевой экспертизы имело важное доказательственное значение. Перечисляются основные требования к формулированию вопросов следователем, отражаемых в постановлении о назначении судебной компьютерной экспертизы. Также приводятся наиболее типичные вопросы, которые могут быть поставлены перед экспертом в области компьютерных технологий при расследовании отдельных видов хищений в сфере информационных и коммуникационных технологий.

Ключевые слова: судебная компьютерная экспертиза, исследование компьютерного устройства, специалист, эксперт, назначение судебной экспертизы, сети, следователь, уголовное дело, расследование.

В современном обществе в условиях интенсивно развивающихся коммуникационных технологий пользователи цифровых сетей хранят целые массивы информации о личной жизни, трудовой деятельности, совершают различного рода операции с денежными средствами.

Между тем представителями преступного мира формируются целые сообщества для получения незаконного доступа к различного рода компьютерной информации, разрабатывается вредоносное программное обеспечение, которое впоследствии становится орудием совершения хищений денежных средств, хранящихся на счетах в банках, сервисах онлайн-платежей.

При этом повсеместное внедрение «облачных» технологий и технологий аутсорсинга в кредитных организациях позволило злоумышленникам уже не напрямую взламывать системы банка для получения доступа к сведениям по конкретному клиенту или сделке, а с помощью незаконного внедрения в сеть одного из многочисленных партнеров и контрагентов, имеющих необходимый доступ (адвокатов, финансовых аудиторов, консультантов и пр.).

В этих условиях использование экспертных знаний в сфере информационных и коммуникационных технологий становится необходимостью при расследовании преступлений против собственности, которые совершались посредством электронных ресурсов и аппаратных средств. В данном случае успех расследования напрямую зависит от своевременно назначенной и качественно проведенной судебной компьютерной экспертизы.

Судебная компьютерная экспертиза – это проводимое экспертом (специалистом) в установленном уголовно-процессуальным законодательством порядке самостоятельное исследование информации, зафиксированной в электронной форме, а также технических средств и программного обеспечения компьютерной системы, в целях дачи заключения по фактам, имеющим значение для уголовного дела [1. С. 131].

Судебная компьютерная экспертиза является самостоятельным родом экспертизы и относится к классу инженерно-технических. Одним из важнейших характеристик экспертизы является предмет, представляющий собой сложную теоретическую и практическую конструкцию, связанную с процессом познания экспертом определенных закономерностей, которые в основном характеризуются тремя интегрируемыми элементами - объектом, задачами (целями) и методами исследования.

В настоящее время выделяют следующие виды судебных компьютерных экспертиз:

1) судебная аппаратно-компьютерная экспертиза, предметом которой являются обстоятельства, устанавливаемые на основе исследования закономерностей эксплуатации аппаратных средств;

2) судебная компьютерно-программная экспертиза, предназначенная для разрешения вопросов закономерности разработки и применения программного обеспечения, в том числе прикладного характера (программы-приложения для мобильных версий операционных систем Android, iOS, Windows, Simbian и др.);

3) судебная информационно-компьютерная экспертиза, в рамках которой исследуются закономерности, связанные с процессом ввода, поиска, передачи и использования информации с помощью компьютерных средств.

Вышеназванные виды судебных компьютерных экспертиз образуют классическую классификацию, данную в работе А.И. Усова, обозначение которых осуществлялось в условиях развития информационно-коммуникационных технологий в начале XXI в. [2. С. 86].

Между тем существенное преобразование коммуникационных технологий, повсеместное распространение корпоративных, социальных сетей, увеличение сегмента услуг «облачных» сервисов по хранению пользовательских данных привело к тому, что на исследование экспертам стали поступать специфичные объекты, требующие комплексного изучения.

Так, например, 21 февраля 2011 г. приговором Промышленного районного суда г. Оренбурга гр. Н. был признан виновным в совершении восьми эпизодов незаконного доступа и копирования охраняемой законом компьютерной информации в системе ЭВМ и их сети, использование вредоносных программ для ЭВМ с целью уклонения от оплаты услуг по доступу к сети Интернет.

Следствием установлено, что Н., находясь в своём жилище, с помощью своего ноутбука «ASUS K50AB», имеющего доступ к сети Интернет под собственным логином и паролем, предоставленным провайдером Оренбургского филиала ОАО «Уфанет», используя вредоносную программу «Radmin Viewer», осуществил сканирование IP-адреса, а также доступ к восьми удаленным компьютерам. После этого Н., используя вредоносную программу, скопировал сетевые реквизиты, в частности логины и пароли, принадлежащие абонентам Оренбургского филиала ОАО «Уфанет», осуществлял неправомерный доступ в сеть Интернет[1].

В ситуациях подобного рода возникает необходимость получения экспертного заключения по результатам проведения судебной компьютерно-сетевой экспертизы, которая основывается на исследовании компьютерных средств, использующих какую-либо сетевую информационную технологию.

Выделение данного вида экспертизы впервые в 2001 г. было обосновано Е.Р. Россинской и А.И. Усовым как экспертизы, предметом которой является установление закономерностей, связанных с функционированием и использованием сетей связи [3. С. 127].

При проведении судебной компьютерно-сетевой экспертизы перед экспертом стоят следующие задачи:

1) определить характеристики программного обеспечения, посредством которого обеспечивается доступ устройства к сетевым ресурсам;

2) определить роль и предназначение исследуемого объекта в сети. (Чаще всего определяется в соотношении конкретного устройства к другому, например, функциональное соотношение аппаратного средства к серверу, активному сетевому оборудованию и т. д.);

3) определить условия модификации свойств и характеристики вычислительной техники;

4) установить свойства и характеристики, архитектуру, конфигурацию сети, соответствие этих характеристик для обозначения класса средств сетевой технологии, принадлежность к серверной или клиентской части приложений;

5) установить наличие определенных физических дефектов, исправность сетевого средства, состояние системного журнала, компонент управлением доступа;

6) определить исходное состояние вычислительной сети в целом и каждого сетевого средства в отдельности;

7) установить обстоятельств инцидента в сети по его результатам и т.д.

Особую значимость компьютерно-сетевая экспертиза приобретает при расследовании преступлений в сфере экономической деятельности, когда объектом исследования является целый комплекс компьютерных устройств, включающих персональные компьютеры работников, серверы организации, а также иные накопители электронной информации, образующих внутрикорпоративную виртуальную сеть. Причем исследование может осложниться наличием криптографической защиты информации, передаваемой по каналам связи такой сети.

[1] Приговор Промышленного районного суда г. Оренбурга по делу 1-55/2011 от 21 февраля 2011 года // ГАС «Правосудие».

Практике известны случаи, когда изъятие в ходе проведения первоначальных следственных действий (осмотра места происшествия, обыска, выемки) всего компьютерного оборудования, посредством которого осуществлялись преступные действия, не приносит должного результата при проведении исследования в лабораторных условиях, так как пользователи компьютерных систем корпоративного типа могут использовать специализированные «облачные» шлюзы для хранения информации. Отключение компьютерного устройства от сети при изъятии может повлечь утрату аутентификационной информации, восстановление которой потребует больших временных и ресурсных затрат [4]. Поэтому при производстве такого рода следственных действий нужно задействовать специалистов того экспертного учреждения, которому впоследствии будут переданы объекты для исследования при назначении компьютерной (компьютерно-технической) экспертизы, либо предоставить возможность проведения экспертизы в месте, где установлено сетевое оборудование. К тому же участие специалиста, например, при осмотре места происшествия может способствовать получению необходимых данных для проведения дальнейшего исследования.

В ситуациях, когда в сети действует организованная преступная группа в целях хищения денежных средств, специалисты могут привлекаться для сопровождения всех первоначальных действий, так как идентификационная абонентская информация о подозреваемых, как правило, хорошо конспирируется с помощью программных средств.

Например, в апреле 2012 г. правоохранительными органами США была пресечена деятельность интернет-организации по продаже наркотиков, действовавшей во всех 50 штатах и округе Колумбия. Преступникам удавалось маскировать свои операции, используя зашифрованную компьютерную сеть TOR. Злоумышленниками в течение двух лет было получено более пяти тысяч заказов на покупку запрещенных наркотических и психотропных веществ на сумму, превышающую 1 млн долл.[2]

При назначении компьютерной экспертизы, объектом которой могут стать коммуникационные технологии, следователь должен учитывать, что подозреваемый может находиться за тысячи километров от места совершения преступления, используя для реализации преступных замыслов общественные точки доступа Wi-Fi к сети Интернет, а также мобильные электронные устройства, содержащие информацию, которая в экстренных ситуациях может быть уничтожена, в том числе с помощью специализированных аппаратных средств.

2 июня 2015 г. органами предварительного расследования МВД России было предъявлено обвинение участникам организованной группы, совершившим более 250 хищений денежных средств клиентов крупных российских банков на общую сумму около 12 млн руб.[3] При задержании подозреваемых было установлено, что по месту их проживания находился электромагнитный излучатель для уничтожения информации с компьютеров, были заготовлены специальные кодовые смс-сообщения, по которым любой из участников группы мог инициировать процесс уничтожения данных[4].

Традиционно постановление о назначении судебной компьютерно-сетевой экспертизы структурно разделяется на три составляющие: вводную, описательно-мотивировочную и резолютивную.

Во вводной части постановления о назначении компьютерно-сетевой экспертизы указывается, где, когда, кто вынес постановление, по какому делу либо материалу. В описательной части излагаются обстоятельства уголовного дела (материала), в связи с которым назначена экспертиза, а также обстоятельства обнаружения компьютерной информации, изъятия электронных носителей, на которых она находится. В резолютивной части указывается род экспертизы, какому конкретно учреждению или лицу поручается ее проведение; вопросы эксперту.

Основываясь на типовой экспертной методике, приведем требования к вопросам, выносимым на компьютерно-сетевую экспертизу [5. С. 193].

1. Формулируя вопросы в постановлении, следователь не должен использовать жаргонные термины («винчестер», «гаджет», «хакнуть» и т. п.), а только устоявшийся понятийный аппарат. При отсутствии таких терминов в законодательных и нормативных актах следует использовать термины, указанные разработчиками в документации, инструкциях, которые прилагаются к техническим средствам и (или) программным продуктам. Так, инструкции по использованию самых распространенных смартфонов размещены на официальных сайтах производителей, в специальной литературе [6. С. 77].

---

[2] Министерство юстиции США разместило доклад о группе киберпреступников. URL: http://inspitech.ru/2013/04/ 22/tor-set-mesto-mirovogo-zagovora-sborishha-pedofilov-prodazha-oruzhiya-narkotikov-lozhnyx-dokumentov-i-kradennyx-kreditok/ (дата обращения: 20.02.2016).

[3] Официальный сайт МВД России. URL: https://mvd.ru/news/item/3531571/

[4] Интернет-портал портал Банки.ru. URL: http://www.banki.ru/ news/lenta/?id=8036884/

2. При постановке вопроса следователь не должен касаться этапов исследования, которые являются обязательными. Например, некорректным является вопрос о характеристиках электронных устройств и особенностей размещения информации на них, так как в ходе исследования эти данные априори выясняются экспертом.

3. Вопрос должен ставиться перед экспертом четко и однозначно, то есть формулироваться без использования абстрактных фраз, которые могут привести к альтернативному пониманию.

4. Вопрос не должен носить правовой, справочный характер и выходить за пределы компетенции эксперта (одна из самых распространенных ошибочных формулировок: «Установлено ли контрафактное программное обеспечение в операционной системе?»). Возможность постановки в постановлении о назначении компьютерной экспертизы такого рода вопросов достаточно велика в ситуациях, когда вопросы ставятся следователем без консультации со специалистом. Между тем, отвечая на вопрос, который выходит за пределы компетенции, эксперт ставит под угрозу доказательственное значение как данного ответа, так и всего заключения.

5. Вопрос должен быть направлен на установление конкретных обстоятельств расследуемого события, соответствовать уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, которому назначается экспертиза, а также представляемым на исследование объектам.

Вопросы в постановлении о назначении компьютерно-сетевой экспертизы могут быть сформулированы следующим образом:

1) имеются ли на предоставленном электронном носителе программы (фрагменты программ), для несанкционированного (в отсутствии волеизъявления пользователя) уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации? Если да, то какие именно, каково их функциональное назначение и сетевые возможности;

2) имеется ли на представленном на исследование носителе информации программное обеспечение, позволяющее без ведома пользователя осуществлять копирование или модификацию компьютерной информации, в частности, программы, способные выполнять без ведома пользователя сбор учетных данных, предоставлять удаленный доступ или самостоятельно, без вмешательства пользователя, взаимодействовать с системами дистанционного банковского обслуживания? Если указанные программы имеются, то каковы их функциональные возможности, расположение и даты появления на данном носителе;

3) содержат ли представленные на исследование электронные носители компьютерную программу или иную компьютерную информацию, предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, если да, то для каких именно вышеуказанных функций данная программа предназначена;

4) имеется ли на представленном электронном носителе программное обеспечение «…», а также программное обеспечение, способное его создавать? Если имеется, является ли оно вредоносным? Каковы его классификация и предназначение;

5) содержатся ли на электронном носителе, представленном для проведения экспертизы, сведения об обращении к доменам «…», а также сведения об использовании их пользователем сервисов мгновенного обмена сообщениями? Если содержатся, то имеются ли данные об аккаунтах пользователя;

6) имеются ли на электронных носителях, представленных для проведения экспертизы, сведения о контактах пользователя, а также история переписки пользователя? Если имеется, то какова история переписки;

7) имеется ли на электронных носителях, представленных для проведения экспертизы, программное обеспечение, предназначенное для удаленного управления? Если имеется, то какое именно;

8) присутствуют ли среди программ, содержащихся на представленном на экспертизу электронном носителе, программы, позволяющие без ведома пользователя отправлять SMS-сообщения или USSD-запросы, а также скрывать от пользователя входящие SMS-сообщения? Если да, то каковы их функциональные возможности;

9) способны ли данные программы предоставлять удаленный доступ к устройству, на котором они запущены, через сеть Интернет без ведома пользователя? Если имеются, то какова дата и время установки на устройство, информация о предполагаемых интернет-ресурсах, с которых данные приложения были скопированы на устройство;

10) имеются ли на представленных на исследование электронных носителях информации программы для операционной системы «…», способные скрытно от пользователя отправлять SMS-сообщения на абонентские номера, содержащиеся в адресной книге, по команде управляющего сервера;

11) имеются ли на представленных на исследование электронных носителях информации сведения об использовании программ, предоставляющих доступ к заданным пользователем серверам по протоколам FTP и SSH? Если да, то к каким серверам осуществлялся доступ, а также с использованием каких учетных данных (логин и пароль);

12) имеются ли на представленных электронных носителях информации сведения о посещении следующих сайтов: «…», «…», «…».

В качестве заключения можно отметить, что в связи с возрастающими потребностями в специальных знаниях в области информационно-коммуникационных технологий при расследовании хищений, совершаемых в сфере информационно-коммуникационных технологий, роль и место судебной компьютерно-сетевой экспертизы будет иметь все большую значение.

СПИСОК ЛИТЕРАТУРЫ

1. Пропастин С.В. Состояние и тенденции развития технологий как основа формирования теории расследования интернет-преступлений // Современное право. 2015. № 11. С. 130-135.
2. Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы: дис. ... докт. юрид. наук. М., 2002. 402 с.
3. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. М.: Право и закон, 2001. 416 с.
4. Васюков В.Ф. Изъятие электронных носителей информации: нерешенные проблемы практики // Уголовный процесс. 2016. № 2 (134). С. 54-57.
5. Саенко Г.В., Тушканова О.В. Компьютерная экспертиза. Типовые экспертные методики исследования вещественных доказательств. Ч. I / под ред. Ю.М. Дильдина; общ. ред. В.В. Мартынова. М.: ЭКЦ МВД России, 2010.
6. Васюков В.Ф. Некоторые вопросы истребования информации о пользователях сотовой связи при расследовании грабежей и разбоев, совершаемых на открытой местности // Закон и право. 2009. № 3. С. 77-78.

Поступила в редакцию 11.05.16

V.F. Vasyukov

SOME ASPECTS OF THE APPOINTMENT OF FORENSIC COMPUTER EXAMINATION WHEN INVESTIGATING EMBEZZLEMENT IN THE SPHERE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

The article reveals the role and importance of forensic computer examination in the investigation of crimes with a mercenary motive in the field of information and communication technologies. The main focus is on the concept, objectives, and problems of appointing this kind of examinations. It is emphasized that forensic computer examination is feasible not only in the laboratory but also on the scene of the crime, when the expert assessment is needed for a volatile storage medium. Focus is on the challenges faced by an expert performing this kind of examination. The author points to the importance of computing and networking expertise in the investigation of theft in situations where the object of study is not a separate type of media but a range of computer devices, software in the conditions of functioning of cryptographic protection of information. Individual cases of the investigative practice, when an expert opinion on the results of the forensic computing and networking expertise was of invaluable probative value, are considered. The author lists the basic requirements for the formulation of questions by the investigator, reflected in the resolution on appointment of forensic computer examination. The article contains the most typical questions that can be posed to the expert in the field of computer technology during the investigation of certain types of embezzlement in the sphere of information and communication technologies.

Keywords: forensic computer examination, expertise of a computer device, specialist, expert, appointment of forensic examination, network investigation, investigator, criminal case investigation.

Васюков Виталий Федорович,
кандидат юридических наук, старший преподаватель
Орловский юридический институт МВД России
им. В.В. Лукьянова
302027, Россия, г. Орел, ул. Игнатова, 2
E-mail: vvf0109@yandex.ru

Vasyukov V.F.,
Candidate of Law, Senior lecturer
Oryol Law Institute of the MIA of Russia
Ignatova st., 2, Orel, Russia, 302027
E-mail: vvf0109@yandex.ru