**УДК** 343.983
**DOI:** 10.19073/2658-7602-2020-17-4-523-533

# ПРОБЛЕМЫ НАЗНАЧЕНИЯ И ПРОИЗВОДСТВА СУДЕБНОЙ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

**СЫСЕНКО Альфия Радиковна***
✉ sysenko_75@mail.ru
*Пр. Комарова, 7, Омск, 644092, Россия*
**СМИРНОВА Ирина Степановна▲**
✉ z1604.smirnova@yandex.ru
*Ул. Короленко, 12, Омск, 644010, Россия*
**ТИМОШЕНКО Светлана Евгеньевна▼**
✉ svet73-13@mail.ru
*Ул. Короленко, 12, Омск, 644010, Россия*

***Аннотация.*** *В силу специфики преступлений, совершаемых в сети Интернет, и необходимости привлечения к участию в уголовном судопроизводстве сведущих лиц, обладающих специальными знаниями в области информационно-вычислительных технологий и информационно-вычислительной техники, назначение компьютерно-технических экспертиз актуально при расследовании большинства сетевых преступлений. Электронная (цифровая) информация, являющаяся предметом преступного посягательства или средством совершения общественно опасного деяния в сети Интернет, может быть правильно собрана, осмотрена и исследована только специалистами либо при их содействии.*

*В научных исследованиях, посвященных компьютерно-технической экспертизе, определение ее понятия не сформулировано, отличительные особенности данного вида экспертиз проанализированы исключительно через описание специфических объектов таких экспертиз. В статье обосновывается, что наименование «компьютерно-техническая экспертиза» выступает самым оптимальным термином, семантически объединяющим исследование как самого устройства, т. е. аппаратного обеспечения, так и его составляющих, а также системного программного обеспечения, информационных данных, включающих различные виды текстовых и графических документов.*

*В основе проблем осуществления судебных компьютерно-технических экспертиз лежат причины объективного и субъективного характера. Не зависящие от профессиональной компетентности эксперта проблемы (объективные) проявляются еще до начала производства рассматриваемого вида экспертиз. Например, несоблюдение требований уголовно-процессуальной формы при собирании в ходе следственных действий электронных документов или компьютерной техники препятствует возможности подготовки экспертом достоверного и допустимого заключения. Важно также учитывать постоянное совершенствование применяемых в преступной деятельности программно-аппаратных средств, что неизбежно вызывает необходимость модификации и оптимизации методик проведения экспертиз.*

*В статье определяются понятие, принципы судебной компьютерно-технической экспертизы, ее виды, объекты исследования и возможности при расследовании и раскрытии преступлений. Практически любое обращение с компьютерной информацией нуждается в использовании специальных знаний. Поэтому авторы подчеркивают возможности судебной компьютерно-технической экспертизы при решении ею диагностических и идентификационных задач, анализируют проблемы назначения и производства компьютерно-технической экспертизы.*

***Ключевые слова:*** *компьютерные преступления, судебная экспертиза, компьютерно-техническая экспертиза, эксперт, специальные знания, сеть Интернет.*

* Доцент кафедры криминалистики Омской академии МВД России, кандидат юридических наук, доцент.

▲ Доцент кафедры уголовного процесса и криминалистики Сибирского юридического университета, кандидат юридических наук, доцент.

▼ Доцент кафедры уголовного процесса и криминалистики Сибирского юридического университета, кандидат юридических наук, доцент.

# Problems of Appointment and Production of Forensic Computer-Technical Expertise

**Sysenko Al'fiya R.****
✉ sysenko_75@mail.ru
*7 Komarova pr., Omsk, 644092, Russia*
**Smirnova Irina S.▲▲**
✉ z1604.smirnova@yandex.ru
*12 Korolenko st., Omsk, 644010, Russia*
**Timoshenko Svetlana E.▼▼**
✉ svet73-13@mail.ru
*12 Korolenko st., Omsk, 644010, Russia*

***Abstract.*** *Due to the specifics of crimes committed on the Internet and the need to involve competent persons with special knowledge in the field of information and computing technologies and information and computer technology in criminal proceedings, the appointment of computer and technical expertise is relevant in the investigation of most online crimes. Electronic (digital) information that is the subject of criminal encroachment or a means of committing a socially dangerous act on the Internet can be correctly collected, examined and examined only by specialists or with their assistance.*

*In scientific research on computer-technical expertise, the definition of its concept is not formulated, the distinctive features of this type of expertise are analyzed exclusively through the description of specific objects of such expertise. The article proves that the name "computer-technical expertise" is the most optimal term that semantically combines the study of both the device itself, that is, hardware, and its components, as well as system software, information data that includes various types of text and graphic documents.*

*The problems of performing forensic computer-technical examinations are based on objective and subjective reasons. Problems that do not depend on the expert's professional competence (objective) appear even before the start of production of the type of expertise under consideration. For example, failure to comply with the requirements of the criminal procedure form when collecting electronic documents or computer equipment during investigative actions prevents the expert from preparing a reliable, respectively, and acceptable conclusion. It is also important to take into account the continuous improvement of software and hardware used in criminal activities, which inevitably causes the need to modify and optimize the methods of conducting examinations.*

*The article defines the concept, principles of forensic computer-technical expertise, its types, objects of research and opportunities in the investigation and detection of crimes. Almost any handling of computer information requires the use of special knowledge. Therefore, the authors emphasize the possibilities of forensic computer-technical expertise in solving diagnostic and identification problems, analyze the problems of assigning and producing computer-technical expertise.*

***Keywords:*** *computer crimes, forensic expertise, computer-technical expertise, expert, special knowledge, Internet.*

Многообразие способов совершения преступлений в сети Интернет, а также постоянно расширяющийся диапазон составов таких преступлений способствуют тому, что разработанные криминалистической наукой традиционные механизмы и алгоритмы расследования нередко оказываются устаревшими для использования при установлении фактических данных, необходимых для раскрытия сетевых преступлений и изобличения лиц, виновных в их совершении.

Данная ситуация обусловлена прежде всего тем, что электронная (цифровая) информация,

** Docent of the Department of Criminalistics at the Omsk Academy of the Ministry of the Interior of Russia, Candidate of Legal Sciences, Docent

▲▲ Docent of the Department of Criminal Procedure and Criminalistics at the Siberian Law University, Candidate of Legal Sciences, Docent.

▼▼ Docent of the Department of Criminal Procedure and Criminalistics at the Siberian Law University, Candidate of Legal Sciences, Docent.

являющаяся средством совершения преступлений или предметом преступных посягательств в сети Интернет, хотя и может быть предназначена для обычных людей, но правильно получена, осмотрена и исследована может быть только специалистами или с их помощью. Практически при любом обращении с компьютерной информацией необходимы специальные знания, благодаря применению которых (как при собирании аппаратного обеспечения, так и при последующем его экспертном исследовании) изъятые объекты (аппаратные средства, программное обеспечение и данные) приобретают все свойства и значение доказательств.

В ходе компьютерно-технической экспертизы (далее – КТЭ) исследуются закономерности разработки и эксплуатации компьютерных средств, обеспечивающих реализацию информационных процессов, зафиксированных в материалах уголовного (или гражданского) дела. Объективная составляющая установленных фактов и обстоятельств часто связана с уяснением компонентов компьютерных средств, т. е. функциональных возможностей их применения в различных сферах жизнедеятельности человека [6, с. 31; 13, с. 795–800].

Как правило, в научных исследованиях, посвященных КТЭ, дефиниция данного понятия не формулируется авторами, отличительные особенности рассматриваемого вида экспертиз анализируются через описание их специфических объектов.

По мнению Е. Р. Россинской, «вид экспертизы, в ходе каких изучается техника и ее компоненты, называется компьютерно-технической экспертизой, потому что своим началом вычислительная (или же компьютерная) техника напрямую обязана как раз инженерно-техническим наукам. Известный термин “компьютерная техника”, который исторически включает в себя все виды обеспечения автоматизированных систем управления (математическое, лингвистическое, техническое, программное, информационное и другие), по сути, является прародителем сегодняшнего названия СКТЭ» [8, с. 233].

Предлагаемое название – компьютерно-техническая экспертиза – самый оптимальный термин, поскольку семантически объединяет как само устройство, т. е. аппаратные объекты (персональные компьютеры, периферийные устройства в виде принтеров и модемов, серверы и рабочие станции как сетевое оборудование, мобильные телефоны, иммобилайзеры, карты памяти и др.), так и его составляющие, системное программное обеспечение, информационные данные, включающие различные виды текстовых, графических, электронных документов, лог-файлы, базы данных, а также составные части компьютерной сети (проводные и беспроводные сети, компоненты и каналы их взаимодействия). Часто эксперту при производстве экспертизы приходится сталкиваться с разного рода мультимедиа данными, к таковым можно отнести видеозаписи, аудиозаписи и т. д. [14, с. 286].

Е. Р. Россинская и Е. И. Галяшина подчеркивают, что «судебные компьютерно-технические экспертизы производятся в целях определения статуса объекта как компьютерного средства, выявления и изучения его роли в расследуемом преступлении, а также получения доступа к информации на носителях данных с последующим всесторонним ее исследованием» [9, с. 275]. Согласимся с тем, что данное определение в целом верно детерминирует назначение и сущность таких экспертиз. Тем не менее названные авторы неоправданно узко трактуют КТЭ как техническое исследование компьютера, поскольку главнейшей задачей раскрытия и расследования сетевых преступлений является установление цифровых (виртуальных) следов криминальной деятельности в сети Интернет и факта осуществления такой деятельности конкретным лицом. Следовательно, компьютер, под которым мы понимаем любое электронно-вычислительное устройство, его части (детали) и носители цифровой информации действительно являются объектом КТЭ, но не во всех случаях выступают предметом такого исследования. Техническая диагностика компьютера сама по себе не всегда отвечает целям расследования сетевого преступления, важно установить факт использования компьютера для его совершения.

В процессе КТЭ эксперт, воспроизводя картину следообразования с учетом характера отображения изучаемых цифровых (виртуальных) следов, исследует механизм взаимодействия следов и возможность его осуществления в конкретных ситуациях.

В научной литературе нет единства мнений относительно типизации судебных компьютерно-технических экспертиз. В разработанных учеными классификациях указывается от двух-трех до пяти видов таких экспертиз. Так, Б. Н. Андреев, П. Н. Пак и В. П. Хорст выделяют два вида

КТЭ: программно-техническую (экспертиза данных и программного обеспечения) и техническую экспертизу компьютеров и их конфигураций [1, с. 64].

В. А. Мещеряков среди компьютерно-технических экспертиз предлагает вычленить: аппаратно-техническую, программно-технологическую, информационную, интегральную компьютерно-техническую [4, с. 325].

При этом сущность аппаратно-технической (аппаратно-компьютерной) КТЭ состоит в диагностическом исследовании технических средств (устройств) электронно-вычислительной техники с определением функциональных и технических возможностей и работоспособности, исходного и текущего их состояния, причин неработоспособности, технологии изготовления, места действия, режима эксплуатации и проч.

Аппаратные средства, составляющие материальную часть компьютерной системы, представлены электрическими, электронными и механическими схемами, блоками, приборами и устройствами. Аппаратное обеспечение включает центральные (процессор, запоминающие устройства, системная шина и проч.), периферийные (устройства ввода-вывода информации, телекоммуникационные устройства и иные устройства, функционирующие с компьютером под его управлением) и вспомогательные устройства (устройства электропитания; сетевые, экранные фильтры и иная аппаратура, работающая автономно от центрального процессора).

В ходе программно-технологической (или программно-технической, программно-компьютерной) экспертизы исследуются основные функциональные свойства установленного на устройстве программного обеспечения. Данный вид экспертизы применим по уголовным делам о нарушении авторских и смежных прав (ст. 146 Уголовного кодекса Российской Федерации (далее – УК РФ)), мошенничестве в сфере компьютерной информации (ст. 159[6] УК РФ), неправомерном доступе к компьютерной информации (ст. 272 УК РФ), создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ).

Объектами программно-компьютерной экспертизы могут выступать системное программное обеспечение, сервисы веб-серверов, системная безопасность, базы и банки данных, в зависимости от чего данный вид экспертизы подразделяется на подвиды, что обусловлено потребностью привлечения знаний из различных областей теории программирования. При этом исследуется алгоритм функционирования, функциональное предназначение, характеристики, реализуемые требования, структурные особенности, текущее состояние программного средства компьютерной системы, причинная связь между действиями пользователя и наступившими последствиями и т. д.

Информационно-компьютерная экспертиза способствует получению доказательственных сведений путем разрешения диагностических и идентификационных вопросов посредством поиска, обнаружения, восстановления, анализа и оценки данных, созданных конкретным человеком (группой лиц) или программой для организации информационных процессов в компьютерной системе [3, с. 11].

Е. Р. Россинская разделяет КТЭ на аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную (данных) и компьютерно-сетевую экспертизы, в основе чего лежит аппаратное, техническое, программное или информационное обеспечение компьютерного средства [8, с. 347].

В уголовном судопроизводстве по делам о преступлениях, совершенных в сети Интернет, особая роль принадлежит компьютерно-сетевой экспертизе (экспертизе особенностей взаимодействия компьютерных систем с использованием каналов связи), объектами которой являются подключенные к сети Интернет (либо предназначенные для подключения) устройства различной конфигурации, различные ресурсы интернет-провайдеров (поставщиков сетевых услуг), предоставляемые последними информационные услуги (например, служба электронных объявлений, телеконференции, электронная почта, www-сервисы и т. п.).

Такая экспертиза обязательно должна быть назначена и проведена в целях определения фактов использования посторонних объектов в сети государственных, негосударственных и других организаций (возможно ли подключение к работе офиса и оказание влияния на связанные с отчетами и конфиденциальной информацией организации сведения, имеются ли установление фактов попыток несанкционированного подключения к компьютеру).

А. А. Бессонов выделяет и такой вид криминалистической экспертизы, как «судебная информационно-аналитическая экспертиза, исследующая

информацию о соединениях абонентов и (или) абонентских устройств как по отношению к конкретным лицам, так и по массиву телефонных соединений в месте преступления в интересующий следствие период» [2, с. 3]. Данный вид исследования позволяет эксперту на основе изучения и анализа цифровых следов пользователей информационно-телекоммуникационной сети составить схему таких пользователей друг с другом, установить номера, IP-адреса и иные идентификационные признаки, позволяющие соотнести действия, совершаемые с помощью того или иного электронного устройства, с конкретным лицом и (или) с некоторой степенью точности установить место нахождения такого лица.

В результате анализа видов и возможностей КТЭ для расследования преступлений А. И. Усов, Л. Г. Эджубов, Е. С. Карпухина и Н. А. Хатунцев приходят к выводу, что многообразие обстоятельств предмета доказывания, подлежащих установлению при расследовании преступлений в сети Интернет, предрешают сложность и комплексность характера самой КТЭ [6, с. 31]. Благодаря появлению в качестве объектов исследования цифровых следов в различных видах судебных экспертиз, дальнейший их анализ становится невозможным без одновременного совместного участия экспертов различных областей знаний в самом исследовании, формулировании общего вывода и написании заключения.

Именно в этом проявляется особенность объектов КТЭ – поставленные вопросы получают разрешение либо в рамках комплексной экспертизы, либо в виде комплекса экспертиз. Так, по мнению указанной группы авторов, в подавляющем большинстве случаев для расследования преступлений в сети Интернет одной лишь КТЭ недостаточно, необходимо, чтобы она проводилась комплексно вместе с другими видами экспертиз или комиссионно – с участием лиц, обладающих специальными знаниями в различных отраслях науки и техники [10, с. 5].

Анализ материалов уголовных дел показывает, что заключения КТЭ как вид доказательств активно используется в расследовании сетевых преступлений, однако назначается она, как правило, в тех ситуациях, когда применение компьютерной техники и (или) информационно-телекоммуникационных сетей прямо поименовано законодателем либо в качестве квалифицирующего признака состава преступления, либо в качестве обстоятельства, отягчающего ответственность[1].

Целью данного вида экспертиз является получение сведений относительно совершения таких противоправных действий, как: перехват данных и кража оплаченного времени в информационно-телекоммуникационных сетях; несанкционированный доступ в информационные системы; преднамеренное распространение вирусов; распространение детской порнографии через Интернет; нарушение авторских и смежных прав в области системного программного обеспечения и аудио- видеоигровых носителей информации; мошенничество с использованием банкоматов и платежных систем; мошенничество в сфере компьютерной телефонии и мобильных платформ и платежей (фрикинго); изготовление и распространение (продажа) специальных технических средств, включая радиомониторинг; незаконное распространение содержащих конфиденциальную информацию баз данных; сетевой экстремизм в информационных сетях и их использование в террористических целях.

К объектам компьютерно-технической экспертизы относятся аппаратное обеспечение (в которое входят персональные компьютеры, периферийные устройства, сетевые аппаратные средства, встраиваемые системы, интегрированные системы, любые их комплектующие, запоминающие устройства и носители данных и др.), системное и прикладное программное обеспечение, информационные данные (в различных форматах), включающие различные виды текстовых и графических документов.

В связи с бурным развитием компьютерной техники, периферийных устройств и приборов, изготавливаемых и работающих на основе технологий построения персональных компьютеров, множатся проблемы определения объектов судебной экспертизы компьютерной техники и программных продуктов. Постоянно совершенствуются применяемые в преступной деятельности программно-аппаратные средства. Производство компьютерно-технических экспертиз осложняется также тем, что цифровые (виртуальные) следы преступлений кардинально отличаются от обычных материальных следов [12, с. 134], так как первые обладают меньшими

[1] *Определение* Верховного Суда Российской Федерации от 22 марта 2018 г. № 303-ЭС17-16652 по делу № А73-8184/2016. Доступ из СПС «КонсультантПлюс».

криминалистически значимыми характеристиками, что значительно затрудняет процесс их отождествления или диагностики. При этом механизм следообразования в цифровой среде имеет особенности, что отражается на процессе выявления следов и установления способов подделки электронных документов в отличие от традиционных документов.

Следует отметить, что на этапе назначения КТЭ следователю (дознавателю, суду) необходимо выяснить следующие моменты:

– подвергалась ли данная информация обработке (передавалась, изменялась) с помощью конкретного программного устройства;

– какой вид (модель, марка, тип) аппаратных и программных средств использовался при операциях с данными;

– к какому типу или более узкой классификационной группе относится представленная компьютерная информация (среди типов необходимо назвать текстовые файлы, программы, вирусы и т. д.; к подтипам или подвидам относятся редакции тестового файла, версии программы, системное или прикладное программное обеспечение);

– каков общий источник происхождения информации, имеющейся на разных носителях (создание ее определенной программой и т. п.).

Кроме того, согласно теории судебной экспертизы, задачи, решаемые КТЭ, основаны на ее предмете и делятся на диагностические и идентификационные. При решении последних идентифицируется система, устанавливается аутентичность информации на электронных носителях через исполнителя (по определенным характеристикам места его расположения) и через общий источник происхождения (или производства) программного продукта. Диагностические задачи более объемны, поскольку при их разрешении определяются свойства и состояние изучаемых объектов (факса, принтера, копира, текстов, изготовленных с применением компьютерной системы), цикл работы неизвестных компьютерных систем, реконструируется и прогнозируется поведение систем, их надежность и устойчивость, системно анализируется обстановка места происшествия, устанавливается факт интеллектуального взлома системы и проч.

В настоящее время отечественная теория КТЭ активно формируется, что предопределено потребностями судебно-следственной практики и взаимосвязано с развитием экспертно-информационных средств и платформ. Предметом исследования КТЭ являются фактические данные, устанавливаемые посредством анализа закономерностей создания и работы компьютерно-технических средств, обеспечивающих работу информационных процессов, сведения о которых содержатся в материалах гражданских, уголовных дел или дел об административных правонарушениях.

КТЭ возможно классифицировать по родовому признаку за счет необходимости исследования компонентов, которые обеспечивают практически любое современное компьютеризированное радиоэлектронное устройство, такое, как смартфон, компьютер, коммуникатор. При этом выделяется аппаратная (техническая), программная («софт»), информационная (данные, созданные пользователем) и сетевая КТЭ.

Как представляется, исследование таких экспертных объектов, как электронные средства и системы, посредством изучения их технологических и эксплуатационных свойств, не только является перспективным направлением, но и может стать отдельным, новым родом информационно-технологических экспертиз.

Непосредственная подготовка к назначению судебной компьютерно-технической экспертизы состоит из:

– постановки задач экспертизы (экспертные задачи);

– определения материалов уголовного дела, содержащих исходные сведения для экспертизы и подлежащих копированию и представлению в распоряжение эксперта;

– отбора объектов экспертизы;

– формулирования и процессуального оформления решения (постановления, определения) о назначении экспертизы;

– выбора экспертного учреждения.

В нормативных правовых источниках не содержится специальных требований относительно производства компьютерно-технической экспертизы, поэтому КТЭ осуществляется по общим принципам. Отметим, что в литературе указывается на такую типичную ошибку, связанную с формулированием вопросов эксперту, как постановка вопросов правового характера (например, «является ли установленное на данном устройстве программное обеспечение контрафактным?»), что недопустимо в силу процессуальных требований, поскольку приводит к смешению компетенции суда как субъекта

процесса, отвечающего в выносимом им акте на вопросы правового характера, и эксперта как носителя специальных знаний (но не правовых) [11, с. 278]. Тем не менее практически во всех изученных нами материалах уголовных дел о нарушении авторских прав суды ставят перед экспертом именно такие вопросы. Как представляется, корректна следующая формулировка подобного вопроса: «Является ли установленное программное обеспечение лицензионным?», «Имеются ли признаки нарушения условий лицензии изготовителя при инсталляции и (или) ином использовании такого программного обеспечения?».

Качество, полнота и правильность экспертного исследования в целом и заключения эксперта, в частности, зависят не только от квалификации конкретных экспертов, которым поручено проведение экспертизы, но и от правильной постановки вопросов, выносимых на разрешение эксперта. Затруднения при формулировании вопросов, выносимых на КТЭ, обусловлены потребностью применения знаний большого объема технической терминологии при расследовании преступлений в сети Интернет, в связи с чем даже изложение вопросов для экспертизы в корректной форме невозможно без помощи специалиста. Вопросы, выносимые на КТЭ, должны быть сформулированы так точно и полно, чтобы ответы на них позволили суду (судье), не обладающему специальными знаниями в области информационно-вычислительных технологий и электронно-вычислительной техники, вынести мотивированный, законный и обоснованный судебный акт.

В зависимости от вида КТЭ вопросы, предлагаемые эксперту для разрешения, можно сгруппировать следующим образом:

– диагностические вопросы о параметрах электронно-вычислительных устройств и их комплектующих (технические характеристики самого устройства, его деталей и периферийных устройств);

– диагностические вопросы о технических характеристиках информационно-вычислительной сети и/или пригодности конкретного оборудования для использования в информационно-телекоммуникационных сетях;

– диагностические вопросы о факте внесения изменений в конструкцию электронно-вычислительных устройств, носителей информации и проч.;

– диагностические вопросы о технических характеристиках и параметрах программного обеспечения, установленного в электронно-вычислительном устройстве;

– диагностические вопросы о факте наличия или отсутствия тех или иных следов (в том числе виртуальных) совершения конкретных действий с информацией, хранящейся на электронно-вычислительном устройстве (например, имеются ли на устройстве стертые файлы, возможно ли их восстановление и каково их содержание; применялись ли для ограничения доступа к информации пароли, скрытые файлы, программы защиты; предпринимались ли попытки несанкционированного доступа, подбора паролей или взлома защитных средств);

– идентификационные вопросы об установлении принадлежности сетевого адреса, адреса электронной почты, id-адреса страницы в социальной сети конкретному лицу.

Приведенные вопросы могут быть скорректированы в зависимости от фабулы расследуемого сетевого преступления.

Как отмечают В. В. Поляков и А. В. Шебалин, «при составлении постановления о назначении компьютерно-технической экспертизы следователи в названии этого документа обычно не указывают вид назначаемой компьютерно-технической экспертизы, ограничиваясь родовым названием, о виде экспертизы можно получить представление из анализа вопросов, ставящихся перед экспертом и предоставляемых в распоряжение эксперта материалов» [5, с. 83]. Отмеченный недостаток как таковой не является нарушением процессуального законодательства, однако неуказание в постановлении о назначении экспертизы конкретного ее рода и вида либо некорректное указание такой информации свидетельствует, на наш взгляд, о том, что следователь не обладает точным и полным пониманием того, к какому процессуальному результату он стремится, назначая исследование. Последствиями этого является некорректная формулировка поставленных перед экспертом вопросов, в свою очередь влекущая необходимость повторной компьютерно-технической экспертизы (в нарушение принципов разумного срока судопроизводства и обеспечения доступа к правосудию), либо признание заключения эксперта недопустимым доказательством по делу (ст. 75 Уголовно-процессуального кодекса Российской Федерации (далее –УПК РФ)).

В постановлении надлежит также указать, что в случае целесообразности эксперт, который будет проводить исследование, может корректировать вопросы либо добавлять свои (в соответствии с правилами, предусмотренными ч. 2 ст. 204 УПК РФ). Делается это по причине того, что эксперт, в отличие от следователя, обладает большим объемом информации по объекту, представленному на экспертизу, и в силу специфичности своей деятельности большими специальными познаниями.

Согласимся с Е. Р. Россинской, что в организационном плане серьезной проблемой является увеличение различных негосударственных экспертных учреждений, позиционирующих себя специалистами в области судебных КТЭ, таковыми по сути не являющимися [7, с. 39], что влечет за собой множество экспертных ошибок.

При выборе экспертного учреждения или конкретного эксперта следователь (дознаватель, суд) должен установить, нет ли оснований, исключающих их участие в производстве экспертизы.

Такими основаниями (в качестве примера приведем положения ст.ст. 61 и 70 УПК РФ) являются: предыдущее участие в этом же уголовном деле в качестве властного субъекта процесса либо иного участника (кроме предыдущего участия в качестве эксперта или специалиста по этому же делу); родственные связи с одним из участников судопроизводства; иные обстоятельства, устанавливающие личную прямую или косвенную заинтересованность в результатах уголовного дела.

Согласно ч. 2 ст. 195 и ст. 198 УПК РФ выбор экспертного учреждения должен осуществляться назначающим судебную экспертизу правоприменителем с учетом мнения заинтересованных участников процесса (подозреваемого, обвиняемого, защитника, потерпевшего и его представителя). Однако порядок (процедура) выбора судебно-экспертного учреждения отечественное уголовно-процессуальное законодательство не предусматривает. Исключение составляют положения о выборе экспертов для производства повторной экспертизы (ч. 2 ст. 207 УПК РФ устанавливает, что ее производство поручается другому эксперту). Применение приведенных норм в правовом единстве приводит к выводу, что властный субъект и заинтересованные участники уголовного судопроизводства вправе выбрать экспертное учреждение по своему усмотрению и сложившемуся обыкновению. При этом ни один из названных участников процесса специальными знаниями не обладает. В силу указанных обстоятельств и в связи с отсутствием конкретных требований к компьютерно-техническим экспертам (даже в части надлежащей квалификации) гипотетически возможна ситуация, когда проведение экспертизы не даст криминалистически значимых результатов, например, вследствие недостаточной квалификации эксперта, которому поручено проведение компьютерной экспертизы, а в случае проведения экспертизы некомпетентным специалистом может привести к повреждению или утрате аппаратных устройств или данных, следовательно, – к утрате доказательств.

Абсолютное отсутствие в действующем законодательстве квалификационных требований, определяющих компетентность эксперта, на наш взгляд, является значительным пробелом, требующим скорейшего устранения. Даже наличие технического образования и многолетнего опыта работы не дает основания предполагать, что имеющиеся у такого эксперта специальные знания позволят квалифицированно, достоверно и четко ответить на вопросы КТЭ. Например, эксперт может быть опытным аппаратным специалистом (т. е. хорошо разбираться в технических характеристиках электронно-вычислительных устройств), но не обладать знаниями в сфере сетевых технологий и, соответственно, не сможет установить относящиеся к делу обстоятельства использования такого оборудования в целях совершения сетевого преступления.

Таким образом, современное развитие науки и техники в целом и информационно-сетевых технологий в частности обусловливает необходимость проверять, соответствуют ли опыт и знания конкретного эксперта тому роду и виду КТЭ, который планируется провести.

При проведении экспертного исследования объекты экспертизы сначала должны быть изучены раздельно. Должны быть подвергнуты анализу их общие и частные признаки и свойства, решены диагностические и идентификационные задачи. При этом ряд вопросов возможно решить только посредством проведения экспертных экспериментов. При решении идентификационных задач проводится сравнительное исследование в целях выявления совпадения или различия признаков объектов, сравниваемых

между собой, а также путем сопоставления их с образцами или эталонами. В целях проверки выводов эксперта ему может направляться необходимая для этого информация, содержащаяся в ответах на запросы банков, операторов сотовой связи, провайдеров.

На этапе подведения итогов исследования компьютерных средств формулируются логические выводы КТЭ в виде ответов (умозаключений) на поставленные перед экспертом вопросы на основе представленных эксперту или выявленных им данных об исследуемом объекте КТЭ и общих научных положений электроники, радиотехники, программирования, т. е. соответствующей отрасли знания

Подводя итоги, подчеркнем, что основными проблемами в части законодательного регулирования и порядка назначения и проведения КТЭ являются:

– отсутствие нормативных требований к квалификации эксперта, которому поручается производство КТЭ;

– отсутствие требований к экспертным учреждениям, которым поручается производство КТЭ;

– отсутствие руководящих инструкций, методик по порядку производства КТЭ экспертными учреждениями.

В связи с этим при назначении КТЭ и практическом использовании ее результатов в целях расследования и раскрытия преступлений остро стоят вопросы наличия у правоприменяющих субъектов хотя бы общих технических знаний о функционировании современной техники, информационно-телекоммуникационных сетей и информационных технологий; корректного определения рода и вида назначаемой КТЭ; надлежащего формулирования вопросов для КТЭ как с правовой, так и с технической точки зрения; установления компетентности конкретного эксперта и (или) экспертного учреждения, которому поручается проведение КТЭ, и пригодности именно этого эксперта для проведения КТЭ; квалифицированной оценки полученного заключения КТЭ на предмет его относимости и допустимости в качестве доказательства по уголовному делу.

Компьютерно-техническая экспертиза представляет собой проводимое в установленном порядке процессуальное действие, осуществляемое компетентным специалистом в целях установления закономерностей возникновения, регистрации, сбора, накопления, ввода, вывода, приема, передачи, хранения, уничтожения, модификации, блокирования, копирования, преобразования, отображения и сокрытия электронно-цифровых следов совершения преступных действий в сети Интернет.

Таким образом, назначение и производство компьютерно-технической экспертизы представляет собой следственное действие, состоящее в принятии надлежащим должностным лицом (властным участником судопроизводства) решения о привлечении сведущего лица (специалиста в области электровычислительной техники, программирования, сетевого администрирования, автоматизации) для производства исследования в целях получения фактических данных посредством установления закономерностей разработки и эксплуатации компьютерных средств для реализации информационных процессов при совершении преступных действий в сети Интернет.

Учитывая сложность цифровой информации как объекта исследования и многообразие цифровых (виртуальных) следов, подлежащих установлению при расследовании преступлений в сети Интернет, в некоторых случаях криминалистически значимые обстоятельства могут быть установлены только в результате назначения и проведения комплексной КТЭ.

Для разрешения этих и других связанных с исследованием цифровых следов проблем требуется программное обеспечение, сертифицированное для экспертных нужд и обновляемое в постоянном режиме. Кроме того, судебные эксперты должны владеть современными компьютерными технологиями, для чего систематически проходить переподготовку и повышать свою квалификацию.

### *Список литературы*

1. Андреев Б. В., Пак П. Н., Хорст В. П. Расследование преступлений в сфере компьютерной информации. М. : Юрлитинформ, 2001. 152 с.

2. Бессонов А. А. Особенности использования специальных знаний при расследовании незаконной добычи рыбных ресурсов // Эксперт-криминалист. 2015. № 3. С. 3–5.

3. Вехов В. Б., Васюков В. Ф. Получение компьютерной информации от организаторов ее распространения в сети интернет при расследовании преступлений // Российский следователь. 2018. № 3. С. 11–15.

4. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж : Изд-во Воронеж. гос. ун-та, 2002. 407 с.

5. Поляков В. В., Шебалин А. В. К вопросу о назначении компьютерно-технической экспертизы, объектом которой является смартфон, по преступлениям в сфере компьютерной информации // Сборник материалов криминалистических чтений. 2013. № 9. С. 83–86.

6. Роль компьютерно-технической экспертизы при решении комплексных задач / А. И. Усов, Л. Г. Эджубов, Е. С. Карпухина, Н. А. Хатунцев // Эксперт-криминалист. 2011. № 4. С. 31–35.

7. Россинская Е. Р. Проблемы использования специальных знаний в судебном исследовании компьютерных преступлений в условиях цифровизации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 5 (57). С. 31–44. DOI: 10.17803/2311-5998.2019.57.5.031-044.

8. Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе : моногр. М. : Норма : Инфра-М, 2018. 576 с.

9. Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. М. : Проспект, 2011. 458 с.

10. Ткачев А. В. Исследование компьютерной информации в криминалистике // Эксперт-криминалист. 2012. № 4. С. 5–8.

11. Юбко Ю. М., Скачек Р. В. Производство по материалам о нарушении права интеллектуальной собственности на программный продукт «1С: Предприятие»: организационные и тактические аспекты // Актуальные проблемы уголовного процесса и криминалистики при раскрытии и расследовании преступлений : тез. докл. респ. науч.-практ. конф. (Минск, 15 нояб. 2013 г.). Минск : Акад. МВД, 2013. С. 276–278.

12. Dzhanadilov O. M., Azhibayev M. G. Problems of Countering Criminal Offenses in Information and Communication Networks // Journal of Advanced Research in Law and Economics. 2019. Vol. 10, № 1 (39). P. 134–143. DOI: 10.14505//jarle.v10.1(39).14.

13. Kruger D. The LongPenTM – The World's First Original Remote Signing Device // Journal of Forensic Sciences. 2010. Vol. 55, iss. 3. P. 795–800. DOI: 10.1111/j.1556-4029.2010.01348.x.

14. Voronkova D. K., Voronkov A. S., Pilipchak A. M. Destination features and conduct of a comprehensive computer forensic and video technical expertise // Information Innovative Technologies / eds.: S. U. Uvaysov, I. A. Ivanov. M. : Association of Graduates and Employees of AFEA Named After Prof. Zhukovsky, 2019. P. 286–291.

## *References*

1. Andreev B. V., Pak P. N., Khorst V. P. *Rassledovanie prestuplenii v sfere komp'yuternoi informatsii* [Investigation of Crimes in the Field of Computer Information]. Moscow, Yurlitinform Publ., 2001. 152 p.

2. Bessonov A. A. Osobennosti ispol'zovaniya spetsial'nykh znanii pri rassledovanii nezakonnoi dobychi rybnykh resursov [Peculiarities of Use of Special Knowledge in Investigation of Illegal Harvesting of Fishing Resources]. *Ekspert-kriminalist – Expert-Criminalist*, 2015, no. 3, pp. 3–5.

3. Vekhov V. B., Vasyukov V. F. Poluchenie komp'yuternoi informatsii ot organizatorov ee rasprostraneniya v seti internet pri rassledovanii prestuplenii [Receipt of Computer Information from Organizers of Its Distribution on the Internet in Investigation of Crimes]. *Rossiiskii sledovatel' – Russian Investigator*, 2018, no. 3, pp. 11–15.

4. Meshcheryakov V. A. *Prestupleniya v sfere komp'yuternoi informatsii: osnovy teorii i praktiki rassledovaniya* [Crimes in theField of Computer Information: The Foundations of the Theory and Practice of Investigation]. Voronezh, Voronezh State University Publ., 2002. 407 p.

5. Polyakov V. V., Shebalin A. V. K voprosu o naznachenii komp'yuterno-tekhnicheskoi ekspertizy, ob"ektom kotoroi yavlyaetsya smartfon, po prestupleniyam v sfere komp'yuternoi informatsii [On the Question of the Appointment of a Computer-Technical Examination, the Object of Which Is a Smartphone, on Crimes in the Field of Computer Information]. *Sbornik materialov kriminalisticheskikh chtenii – Collection of Materials of Forensic Readings*, 2013, no. 9, pp. 83–86.

6. Usov A. I., Edzhubov L. G., Karpukhina E. S., Khatuntsev N. A. Rol' komp'yuterno-tekhnicheskoi ekspertizy pri reshenii kompleksnykh zadach [Role of Computer-techniques Expert Evaluation in Solution of Complex Task]. *Ekspert-kriminalist – Expert-Criminalist*, 2011, no. 4, pp. 31–35.

7. Rossinskaya E. R. Problemy ispol'zovaniya spetsial'nykh znanii v sudebnom issledovanii komp'yuternykh prestuplenii v usloviyakh tsifrovizatsii [Problems the Use of Special Knowledge for the Judicial Investigation of Computer Crimes in the Conditions of Digitalization]. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA) – Courier of Kutafin Moscow State Law University (MSAL)*, 2019, no. 5 (57), pp. 31–44. DOI: 10.17803/2311-5998.2019.57.5.031-044.

8. Rossinskaya E. R. *Sudebnaya ekspertiza v grazhdanskom, arbitrazhnom, administrativnom i ugolovnom protsesse* [Forensic Examination in Civil, Arbitration, Administrative and Criminal Proceedings]. Moscow, Norma Publ., Infra-M Publ., 2018. 576 p.

9. Rossinskaya E. R., Galyashina E. I. *Nastol'naya kniga sud'i: sudebnaya ekspertiza* [Handbook of a Judge: Forensic Examination]. Moscow, Prospekt Publ., 2011. 458 p.

10. Tkachev A. V. Issledovanie komp'yuternoi informatsii v kriminalistike [Investigation of Computer Information in Criminalistics]. *Ekspert-kriminalist – Expert-Criminalist*, 2012, no. 4, pp. 5–8.

11. Yubko Yu. M., Skachek R. V. Proizvodstvo po materialam o narushenii prava intellektual'noi sobstvennosti na programmnyi produkt «1S: Predpriyatie»: organizatsionnye i takticheskie aspekty [Production Based On Materials on Violation of Intellectual Property Rights to the Software Product "1C: Enterprise": Organizational and Tactical Aspects]. *Aktual'nye problemy ugolovnogo protsessa i kriminalistiki pri raskrytii i rassledovanii prestuplenii – Actual Problems of Criminal Procedure and Forensic Science in the Disclosure and Investigation of Crimes*. Minsk, MIA Academy Publ., 2013, pp. 276–278.

12. Dzhanadilov O. M., Azhibayev M. G. Problems of Countering Criminal Offenses in Information and Communication Networks. *Journal of Advanced Research in Law and Economics*, 2019, vol. 10, no. 1 (39), pp. 134–143. DOI: 10.14505//jarle.v10.1(39).14.

13. Kruger D. The LongPenTM – The World's First Original Remote Signing Device. *Journal of Forensic Sciences*, 2010, vol. 55, iss. 3, pp. 795–800. DOI: 10.1111/j.1556-4029.2010.01348.x.

14. Voronkova D. K., Voronkov A. S., Pilipchak A. M. Destination features and conduct of a comprehensive computer forensic and video technical expertise. *Information Innovative Technologies*. Moscow, Association of Graduates and Employees of AFEA Named After Prof. Zhukovsky, 2019, pp. 286–291.

Дата поступления статьи | Article received date
19.09.2020

Дата поступления после рецензирования и доработки | Article after peer review and revision received date
17.11.2020

Дата приема к публикации | Article accepted date
24.11.2020