УДК 343.982.9

ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ СО СПЕЦИАЛИСТОМ В ХОДЕ НАЗНАЧЕНИЯ И ПРОИЗВОДСТВА КОМПЬЮТЕРНЫХ ЭКСПЕРТИЗ В СИСТЕМЕ МВД РОССИИ

Елена Юрьевна Родина*, Василий Николаевич Москаленко**
* Санкт-Петербургский университет МВД России,
Санкт-Петербург, Россия, elena_rodina1981@mail.ru
** ГУ МВД России по г. Санкт-Петербургу и Ленинградской области,
Санкт-Петербург, Россия, lashpartuns@yandex.ru

Аннотация. В процессе активной цифровизации всех сфер жизни человека цифровой мир стал представлять собой гигантский массив данных, состоящий из облачных технологий, систем и алгоритмов анализа необходимой информации. Повседневная жизнь каждого члена общества неразрывно связана с возможностями, которые нам дает цифровой мир: онлайн-шопинг, приложения и QR-коды для бесконтактной оплаты услуг, сервисы медицинских учреждений, налоговых служб, транспортные карты и многое другое.

Электронные устройства функционально предназначены для облегчения повседневных задач человека и общества в целом, но вместе с тем делают их более уязвимыми перед противоправными деяниями. Мероприятия, направленные на предотвращение распространения новой коронавирусной инфекции в 2020–2022 гг., специальная военная операция, произошедшие теракты в очередной раз сфокусировали внимание на том, что преступная деятельность переместилась в сферу информационно-телекоммуникационных технологий. Это привело к неизбежному росту изъятий средств вычислительной техники и, соответственно, назначенных судебных компьютерных экспертиз в рамках расследования преступлений разной направленности.

Ключевые слова: компьютерная экспертиза, информационно-телекоммуникационные технологии, цифровые следы

Для цитирования: Родина Е. Ю., Москаленко В. Н. Особенности взаимодействия со специалистом в ходе назначения и производства компьютерных экспертиз в системе МВД России // Судебная экспертиза. 2024. № 4 (80). С. 19–30.

FEATURES OF THE APPOINTMENT AND PRODUCTION OF COMPUTER EXAMINATIONS IN THE SYSTEM OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Elena Yuryevna Rodina*, Vasily Nikolaevich Moskalenko**

* Saint Petersburg University of the Ministry of the Interior of Russia, Saint Petersburg, Russia, elena_rodina1981@mail.ru

** Forensic Center of the Ministry of Internal Affairs of Russia in Saint Petersburg and Leningrad region, Saint Petersburg, Russia, lashpartuns@yandex.ru

Abstract. In the process of active digitalization of all spheres of human life, during which the digital world has become a giant data array consisting of cloud technologies, systems and algorithms for analyzing the necessary information. The daily life of every member of society has become inextricably linked with the opportunities that the digital world gives us: online shopping, applications and QR codes necessary for non-contact payment for services, services of medical institutions, tax services, transport e-cards and much more.

Electronic devices are functionally designed to facilitate the daily tasks of a person and society as a whole, but at the same time make a person and the tasks they perform more vulnerable to illegal acts. Activities aimed at preventing the spread of a new coronary infection in 2020–2022, special military operation, the terrorist attacks have once again focused attention on the fact that criminal activities have moved into the sphere of information and telecommunication technologies. This has led to an inevitable increase in the seizure of computer equipment and, accordingly, assigned forensic computer expertise in the investigation of crimes of different focus.

Keywords: computer expertise, information and telecommunication technologies, digital traces

For citation: Rodina E. Yu., Moskalenko V. N. Features of the appointment and production of computer examinations in the system of the Ministry of Internal Affairs of Russia. Forensic Examination, 19–30, 2024. (In Russ.).

Более 20 лет преступления, которые совершаются с использованием компьютерных средств и систем, объединены понятием «компьютерные преступления», что имеет значение не в уголовно-правовом аспекте, так как это только затруднит квалификацию деяния, а в криминалистическом, поскольку связано со способом совершения преступления и, соответственно, с методикой его раскрытия и расследования [1].

Процесс становления судебной компьютерной экспертизы очень длителен. В настоящее время человечество не мыслит себя без вычислительной техники и информационных технологий. Стремительно меняются и способы совершения преступлений, таких как кражи, мошенничества, преступления в сфере экономических преступлений и др.: от «традиционных» к более современным – с использованием информационных технологий (далее – ИТ). Как справедливо отмечает А. И. Усов, «глобальное распространение этого явления затронуло и юриспруденцию» [2, с. 10], так как сотрудники правоохранительных органов используют ИТ в служебной и научной деятельности.

Активное внедрение ИТ в сферу судопроизводства повлекло, во-первых, возникновение новых и модификацию существующих видов криминалистически значимой информации, находящейся в таком специфическом объекте исследования, как компьютерные носители информации (электронно-цифровые следы) [3]. Во-вторых, цифровизация значительно расширила границы и возможности получения новой доказательственной информации, а также ориентирующих сведений [4]. Данное обстоятельство создает обязательные условия использования специальных знаний в области компьютерных систем и сетей, повышает роль специалистов данной области в процессе расследования преступлений и правонарушений.

Рассматриваемая нами судебная экспертиза в различных источниках именуется по-разному. Так, Т. В. Аверьянова называла ее «судебная экспертиза компьютерных средств» (2001 г.), позднее именовала «компьютерной экспертизой» (2006 г.). Е. Р. Россинская подвергает данные названия, на наш взгляд, обоснованной критике, указывая, что они слишком узкие и не учитывают всех возможностей исследования компьютерных систем. По мнению Е. В. Россинской, «под компьютерной (вычислительной) системой понимается совокупность взаимосвязанных компьютерных средств, взаимодействующих для решения задач обработки информации и других функциональных задач» [5, с. 60]. В связи с этим она предлагает именовать данную экспертизу не иначе как «судебная компьютерно-техническая экспертиза». В настоящее время ведется немало научных дискуссий по данному поводу, и ученые до сих пор не пришли к единому мнению.

Ведомственная несогласованность по этому вопросу тоже вносит некое непонимание среди сотрудников правоохранительных органов, а также обучающихся при подготовке к учебным занятиям, так как в реестрах МВД России (ГУ ЭКЦ) и Минюста России (ГУ РФЦСЭ) название рассматриваемой экспертизы указывается по-разному. Так, согласно приказу МВД России от 29 июня 2005 г. № 511, экспертиза называется «судебная компьютерная экспертиза», а в приказе Минюста России от 14 мая 2003 г. № 114 именуется как «судебная компьютерно-техническая экспертиза».

Ведомственные отличия, по мнению Е. Р. Россинской, не существенны и легко объясняются разной родовой составляющей данных экспертиз. Квалификация расследуемых в ведомствах уголовных дел влечет закономерное использование разных родов судебных экспертиз. В ЭКЦ ГУ МВД России назначается компьютерная экспертиза, в ходе которой исследованию подвергаются файловые массивы, базы данных, программное обеспечение, при этом отдельно назначается радиотехническая экспертиза, в ходе которой исследуется техническое состояние радиотехнических устройств и систем. В ГУ РФЦСЭ Министерства юстиции Российской Федерации назначаются компьютерно-сетевая, аппаратно-компьютерная экспертизы и т. д., что и обусловливает появление в названии термина «техническая».

В данной статье мы подробно остановимся на особенностях назначения и производства судебной компьютерной экспертизы (далее – КЭ) в системе МВД России.

В процессе КЭ эксперт воспроизводит картину следообразования, принимая во внимание характер отображенных цифровых (виртуальных) следов, и одновременно с этим исследует и механизм взаимодействия следов, и возможность его осуществления в определенных ситуациях.

Объектом исследования судебной КЭ является информация, содержащаяся на различных электронных носителях, например: накопителях на жестких магнитных дисках (НЖМД, HDD), накопителях на гибких магнитных дисках (НГМД, FDD), твердотельных накопителях (ТН, SSD), оптических дисках (CD, DVD, BD), USB-флеш-накопителях, картах памяти, запоминающих устройствах мобильных телефонов, носимых устройствах (смарт-часах) и иных машинных носителях. Далее в тексте под носителем информации будет подразумеваться носитель, характерный для предоставленной на исследование единицы техники (ноутбуки, системные блоки, серверные системные блоки, сетевые накопители, мобильные телефоны и т. д.) [6].

По данным ЭКЦ ГУ МВД г. Санкт-Петербурга и Ленинградской области (далее – ЭКЦ), специалисты 11-го отдела ЭКЦ привлекались для производства компьютерных исследований по письменному заданию руководителей оперативных подразделений до возбуждения уголовного дела, судебных компьютерных экспертиз и различных следственных действий (обыск, выемка и др.) (см. таблицу).

Таблица показателей результативности работы специалистов 11-го отдела ЭКЦ ГУ МВД России за период с 2020 по 2024 г.

	2020 г.	2021 г.	2022 г.	2023 г.	11 месяцев 2024 г.
Компьютерные экспертизы	576 (результативных более 60 %)	560 (результативных более 65 %)	270 (результативных более 67 %)	309 (результативных более 70 %)	606 (результативных более 85 %)
Компьютерные исследования	22	18	8	7	17
Следственные действия	276	309	174	802 (результативных более 50 %)	1 051 (результативных более 57 %)

Необходимо учитывать тот факт, что данная судебная экспертиза является наиболее трудоемкой и требующей больших временных затрат с участием высококвалифицированных специалистов и технико-криминалистических средств. При изучении правоприменительной практики Санкт-Петербурга и Ленинградской области установлено, что следователи ГСУ ГУ МВД России (далее – ГСУ) не обращаются на постоянной основе в ЭКЦ в целях доэкспертной оценки материала для назначения и проведения экспертиз и исследований, тогда как данное обстоятельство существенно влияет на сроки производства экспертизы и объем работы экспертов.

Проведение доэкспертной оценки возможно в двух формах.

1. Привлечение сотрудников отдела компьютерных экспертиз к участию в следственных действиях для осмотра электронных устройств. Данное взаимодействие позволяет сузить круг объектов, представляющих криминалистический интерес, в краткие сроки получить необходимую информацию, хранящуюся в памяти исследуемых объектов, без оформления материалов судебной экспертизы.

2. Консультация следователей перед назначением судебной экспертизы для согласования формулировки поставленных на разрешение эксперту вопросов. Уточняются сведения о значениях разблокировочных паролей, осуществляется

подбор носителей информации для записи результатов проведенных исследований. Такая форма взаимодействия позволяет получить наиболее информативные результаты, а также максимально сократить сроки проведения дальнейших исследований.

В ходе изучения правоприменительной практики установлено, что в 2021 г. эксперты по специальности «Компьютерная экспертиза» привлекались к обеспечению 309 следственных действий, инициированных сотрудниками ГСУ и следственных подразделений территориальных органов ГУ МВД России по г. Санкт-Петербургу и Ленинградской области. Осмотру подлежало 220 мобильных телефонов, 31 ноутбук, 27 системных блоков, 3 серверных блока, 52 накопителя на жестких магнитных дисках, 12 планшетных компьютеров, 19 флеш-карт. По результатам проведенных следственных действий на экспертизу направляется не более 25 % исследуемых объектов[1]. Информация, извлеченная с остальных объектов, после фиксации в протоколе следственного действия приобщается к материалам уголовного дела. Данные сведения подтверждают необходимость проведения доэкспертной оценки объектов в ходе следственных действий, так как это позволяет существенно сократить количество направляемых на экспертное исследование объектов и выбрать наиболее эффективную тактику проведения судебной экспертизы.

Возросшая потребность в проведении КЭ в настоящее время обусловила следующие проблемы:

– малая численность высококвалифицированных экспертов конкретных специальностей;

– недостаточная штатная численность экспертов определенных специальностей;

– большая нагрузка экспертов, которая сказывается на сроках производства экспертиз;

– случаи неоправданного, не сопряженного с необходимостью назначения судебной экспертизы, в том числе повторных экспертиз для получения определенных выводов;

– отсутствие должной квалификации при работе с объектами КЭ у следователей [7].

На наш взгляд, решение данной проблемы возможно не только путем обязательной регламентации доэкспертной оценки криминалистически значимых объектов в ведомственных нормативных правовых актах, но и расширения штатного количества экспертов ЭКЦ.

На стадии подготовки и проведения КЭ возникают проблемы, связанные не только с недостаточной квалификацией сотрудников правоохранительных органов при работе с объектами КЭ, но и отсутствием необходимого дорогостоящего оборудования в территориальных подразделениях, что влечет накопление неочевидных уголовных дел. Данное обстоятельство подтверждается правоприменительной практикой. Например, в Красносельском районе Санкт-Петербурга в производстве только одного следователя находится порядка 200 уголовных

[1] Отчет 1нтп ЭКЦ ГУ МВД России по Санкт-Петербургу и Ленинградской области // Официальный сайт ГИАЦ МВД России. URL: http://xn--blaew.xn--plai/reports/item/26421097/. Режим доступа: для зарегистрир. пользователей.

дел, в процессе расследования которых необходимо исследование объектов КЭ. Имеет место и некорректное формулирование вопросов экспертам. Сотрудники правоохранительных органов совершают недопустимые ошибки при работе с объектами, например включение изъятых компьютеров, на которых в ходе самостоятельного осмотра пытались обнаружить (набрать, распечатать и т. д.) электронную информацию, имеющую доказательственный характер, и др. По мнению экспертов, даже открытие и просмотр файлов, не говоря про их изменение, ограничит в дальнейшем эффективность проведения повторной экспертизы из-за невозможности установления существовавших удаленных файлов. В связи с этим нами сформулированы практические рекомендации по направлениям, где нарушений выявляется больше всего.

Одним из важнейших этапов работы с доказательствами является изъятие криминалистически значимых объектов, так как от него зависит весь ход судебной экспертизы. Изъятие объектов КЭ имеет свои специфические особенности, которые необходимо учитывать при изъятии данных объектов. Рассмотрим их подробнее.

1. Системные блоки, ноутбуки и моноблоки (ПЭВМ) могут представлять собой рабочие станции, на которых сохраняются данные, и использоваться для удаленного (терминального) доступа к серверу, при этом пользовательские данные на локальной машине, как правило, сохраняться не будут, поэтому недопустимо:

– исследовать электронные носители информации при включенном системном блоке, ноутбуке, моноблоке и т. д.;

– отключать питание объекта (некорректно завершать работу операционной системы);

– извлекать (или менять местами) НЖМД системные блоки, если есть основания полагать, что они сконфигурированы в RAID-массив[1] (такой системный блок изымается целиком).

Изъятие ПЭВМ рекомендуется выполнять после корректного завершения работы операционной системы, направленной на сохранение имеющейся на ПЭВМ информации[2]. Интерфейсные кабели необходимо бережно отключать от системного блока (ноутбука, моноблока), после чего упаковывать его. Например, если специалистом установлено, что выключение ПЭВМ при помощи средств операционной системы может привести к утрате информации, то целесообразно рассмотреть вариант завершения работы с использованием режима гибернации. В дополнение к указанным объектам необходимо изымать адаптеры питания, в протоколе и пояснительной записке указывать имена учетных записей и пароли к ним. Изъятие НЖМД ПЭВМ допускается, если они не являются частью RAID-массива. Для упаковки необходимо использовать плотные полимерные пакеты (мешки) либо картонные коробки, при этом данная упаковка подойдет для системных блоков, сетевых накопителей и серверных системных блоков.

[1] RAID-массив – программно или аппаратно реализуемая система массива дисков, определяется специалистом во время проведения следственного действия.

[2] Информационное письмо ЭКЦ МВД России «Анализ программного обеспечения, применяемого при совершении преступлений», 2021.

Вопросы сохранения дампа оперативной памяти (для целей дальнейшего исследования) должны оговариваться заранее, чтобы специалист мог подготовить необходимое программное обеспечение, а руководитель следственного действия мог подготовить носители для копирования дампа. В обязательном порядке сохранение дампа оперативной памяти производится, если в ней имеется следующая информация:

– ключи для расшифровки примонтированных криптоконтейнеров;

– последние сообщения из социальных сетей, сообщений, переданных с помощью программ мгновенного обмена информацией;

– информация о последних скачанных файлах;

– страницы и изображения с веб-сайтов (в том числе из интернет-браузеров, способствующих установлению анонимного сетевого соединения);

– иная системная информация, которая может иметь значение для расследования дела.

В ходе следственного действия при обнаружении компьютерных объектов с работающим на них интернет-браузером, который позволяет устанавливать анонимное сетевое соединение, необходимо производить фотофиксацию активных окон, всех вкладок и иной криминалистически значимой информации. Данная информация прилагается к протоколу следственного действия в виде фототаблиц.

2. Алгоритм действий с серверными системными блоками, системами хранения данных (СХД) определяет вид и качество помещений, количество сотрудников и парк ПЭВМ организации, а также количество организаций в здании (например, арендаторы могут использовать единое серверное помещение), так как перечисленные обстоятельства могут оказать существенное влияние на функции, количество и местонахождение серверов и СХД. В связи с этим недопустимо:

– извлекать электронные носители информации при включенном сервере, СХД;

– изымать электронные носители информации отдельно от серверного системного блока, системного блока, СХД, где они установлены; менять их местами или устанавливать в другие монтажные отсеки устройств;

– отключать питание объекта до корректного завершения работы операционной системы [8].

В ходе изъятия серверного оборудования и СХД производится копирование криминалистически значимой информации на чистый электронный носитель информации. В протоколе и приложении к нему фиксируется схема подключения серверов, факт использования фото- или видеофиксации, при этом обязательной фиксации подлежат конфигурация RAID и его состояние. Данные объекты изымаются с кабелем сопряжения устройств. При возможности необходимо установить пароль доступа к операционной системе сервера, который также указывается в процессуальных документах и приложениях к ним. Все схемы, содержащие информацию о взаимодействии и подключении серверов, их роли, дублируются в пояснительных записках на упаковке, фиксируются на корпус объекта электронно-вычислительной техники (далее – ЭВТ). Небольшие объекты, извлекаемые из USB-разъемов, изымаемые из серверных системных блоков (USB-флеш-накопитель или электронный ключ защиты, жесткие или твердо-

тельные диски подлежат отдельной упаковке в полимерные пакеты или бумажные конверты, снабженные пояснительной записью с указанием системного блока, из которого данные объекты были извлечены. После чего их необходимо приклеить при помощи клейкой ленты к серверному системному блоку, чтобы упредить возможность оказания давления на данные объекты или их повреждение.

Взаимодействие со специалистами, которые отвечают за информационную безопасность организации в ходе работы с указанными объектами, может принести как положительные, так и отрицательные результаты, и в связи с этим необходимо учитывать все возможные риски. Сетевое оборудование (роутеры) могут содержать техническую информацию, представляющую криминалистическое значение для расследования, поэтому считаем целесообразным изымать информацию с данных устройств, но только при участии специалиста, тогда как изъятие самого устройства нецелесообразно. В случаях принятия решения об изъятии роутера обязательной фиксации подлежит имя учетной записи и пароль администратора.

3. Системные блоки стационарных видеорегистраторов могут выполнять функцию и видеорегистратора (с записью данных на носитель), и системы видеонаблюдения (без записи данных на носитель). При изъятии запрещено:

– извлекать электронные носители информации при включенном системном блоке стационарного видеорегистратора;

– изымать электронные носители информации отдельно от устройств;

– превышать допустимое количество попыток ввода пароля пользователя для конкретной модели устройства.

Электронные носители информации в системном блоке видеорегистратора подлежат изъятию для дальнейшего ее копирования на USB-накопитель или оптические диски. В случае невозможности копирования устройство подлежит изъятию вместе с адаптером питания и пультом дистанционного управления (при наличии). Данные действия подлежат фиксации с указанием пароля видеорегистратора, если таковой имеется. Рекомендуется рассмотреть возможность дальнейшего исследования видеорегистратора с привлечением представителя фирмы-производителя видеорегистратора либо в сервисном центре фирмы-производителя. Упаковываются так же, как и вышеуказанные объекты, или в картонные коробки, в зависимости от их размера.

4. Мобильные телефоны, смартфоны и планшетные компьютеры имеют широкое распространение у пользователей, поэтому места их обнаружения в ходе следственных действий могут быть различны [9]. При изъятии запрещается оставлять включенными модули связи, так как это может привести к возможности удаленного доступа к информации, содержащейся на данных устройствах.

Мобильные телефоны, смартфоны и планшетные компьютеры не следует упаковывать вместе с установленными SIM-картами и аккумуляторами в полимерные пакеты, в связи с тем что упаковка не будет блокировать доступ к самому устройству.

При изъятии мобильных телефонов, смартфонов и планшетных компьютеров обязательно необходимо проверить операционную систему устройства в целях установления наличия настроенного второго пространства (private space). Затем устройство переводится в режим «В полете», и только после этого модуль связи

объекта отключается. SIM-карта после извлечения из устройства фиксируется клейкой лентой контактами к крышке устройства, к которому обязательно прилагаются кабели сопряжения. При установлении паролей (для мобильных телефонов, второго пространства, приложений, резервных копий), графических ключей разблокировки данная информация фиксируется в протоколе следственного действия и пояснительной записке на упаковке (картонная коробка). Рекомендуется предварительно выключить у телефона модуль связи, переведя телефон в режим «В полете», отключить питание мобильного телефона и извлечь SIM-карту. Факт отключения модуля связи указывается в протоколе следственного действия.

5. Портативные устройства: видеорегистраторы, навигационные устройства, USB-модемы – чаще всего можно обнаружить при осмотре транспортных средств. Намного реже данные объекты обнаруживают в помещениях (жилых, офисных, складских и др.). В ходе проведения следственных действий, как правило, USB-модемы можно обнаружить в местах, где доступ к сети Интернет осуществляется с использованием услуг сотовых операторов. При изъятии данные устройства выключаются, карты памяти и SIM-карты (при наличии) извлекаются, упаковываются и фиксируются клейкой лентой контактами к крышке.

6. Носимые устройства (смарт-часы, электронные браслеты), на которых наиболее вероятно обнаружить интересующую следствие информацию, могут быть двух видов: синхронизируемые со смартфоном или самостоятельные устройства с SIM-картой и носителем информации. При изъятии данных устройств необходимо изымать кабели питания и сопряжения, если имеется пароль, он указывается в протоколе следственного действия и пояснительной записке на упаковке. SIM-карта из часов, если она там есть, крепится клейкой лентой к задней крышке часов, из которых она была извлечена (контакты SIM-карты должны быть обращены к крышке смарт-часов).

7. Электронные носители информации можно обнаружить в любом месте проведения следственных действий независимо от расположения устройств, предназначенных для работы с ними. Устройства с USB-интерфейсом в обязательном порядке извлекаются из разъема объектов ЭВТ и упаковываются отдельно от них. Мы считаем целесообразным в ходе следственного действия проводить анализ информации, содержащейся на данных носителях, в целях диагностики самого электронного носителя и данных на нем.

8. Беспилотные летательные аппараты (дроны) (далее – БПЛА) в настоящее время используются в различных сферах деятельности человека. Существует большое количество разновидностей – заводских (DJI, Parrot), устройств кустарной сборки, а также огромное количество типов дронов (трикоптер, квадрокоптер, гексакоптер и др.). Размеры этих устройств варьируются от размеров крупного насекомого до самолета. Современные технологии позволяют оборудовать такие устройства камерами, системой FPV (видео в режиме реального времени), системой GPS (установление местоположения) и др. В связи с этим на них также может находиться информация, представляющая интерес для сотрудников правоохранительных органов.

При изъятии БПЛА необходимо в первую очередь соблюдать технику безопасности. Соответственно, недопустимо включение устройства с установлен-

ными на нем пропеллерами, его запуск, подключение к нему проводов питания, включение пульта и несанкционированное нажатие кнопок, переключение рычагов и тумблеров, как на пульте, так и на самом устройстве.

Учитывая допускаемые ошибки, рекомендуем изымать БПЛА следующим образом: после отключения пульта управления и БПЛА желательно извлечь аккумуляторы, после чего необходимо снять пропеллеры и извлечь карту памяти, если она имеется. Затем карту памяти необходимо зафиксировать клейкой лентой к корпусу устройства либо упаковать в бумажный конверт. Вместе с устройством изымаются все кабели питания и сопряжения. В качестве упаковки рекомендуется использовать коробки или плотные полимерные пакеты. В отдельную упаковку необходимо помещать выключенный пульт управления, аккумуляторы, провода питания и коммуникации. Пульт управления в упаковке желательно зафиксировать неподвижно, таким образом, чтобы исключить несанкционированные нажатия каких-либо кнопок / тумблеров / рычагов.

В правоприменительной практике нередко допускается нарушение требований, предъявляемых к работе с вещественными доказательствами, прежде всего к их упаковке. Объекты ЭВТ в процессуальном порядке хранятся у ответственных лиц в опечатанном виде в надлежащих условиях, исключающих доступ третьих лиц и гарантирующих их сохранность и сохранность указанной информации (п. 5 ст. 82 Уголовно-процессуального кодекса Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (далее – УПК РФ)), вне зависимости от места хранения (при уголовном деле (п. 1 ст. 82 УПК РФ) или при передаче на хранение (п. 2 ст. 82 УПК РФ; постановление Правительства РФ «Об условиях хранения, учета и передачи вещественных доказательств по уголовным делам» от 8 мая 2015 г. № 449)).

Упаковка объектов должна снабжаться бирками с пояснительными надписями о месте, времени и лицах, участвовавших при изъятии (выемке) или осмотре, информацией о пользовательских паролях, скрепляться оттисками штампов и подписями участвующих лиц.

Резюмируя изложенное, можно сделать следующие выводы:

1. Внедрение практики обязательной доэкспертной оценки объектов позволит сократить сроки нахождения экспертиз в очереди на исполнение с восьми месяцев до одного, а в случае поступления указания от руководства о необходимости ускорения производства экспертиз срок производства не будет превышать установленных 15 суток.

2. Строгое соблюдение тактико-криминалистических рекомендаций по изъятию и упаковке объектов компьютерной экспертизы позволит избежать сомнений в неизменности и модификации информации, сохраненной на вещественных доказательствах; в легитимности вещественного доказательства, так как предотвратит возникновение новых цифровых следов, не связанных с преступным деянием.

Список источников

1. Криминалистика: учеб. для вузов / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская; под ред. Р. С. Белкина. Москва: Норма, 2020. 928 с.

2. Усов А. И. Судебная компьютерно-техническая экспертиза: становление, развитие, методическое обеспечение // Теория и практика судебной экспертизы. 2008. № 3 (6). С. 10–22.

3. 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.

4. Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения: материалы Междунар. науч.-практ. конф. (19 февр. 2019 г.). Алматы, 2019. С. 6–9.

5. Россинская Е. Р. Судебная компьютерно-техническая экспертиза: проблемы становления и подготовки кадров экспертов // Теория и практика судебной экспертизы. 2008. № 3 (6). С. 60–66.

6. Москаленко В. Н. Рекомендации по оптимизации назначения судебной компьютерной экспертизы (на примере ЭКЦ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области) // Санкт-Петербургская школа криминалистики: материалы V Всерос. криминал. форума (Санкт-Петербург, 19–21 окт. 2023 г.) / под общ. ред. А. А. Сапожкова; отв. ред. Е. В. Елагина. Санкт-Петербург: С.-Петерб. юрид. ин-т (филиал) Ун-та прокуратуры РФ, 2024. С. 113–120.

7. Кувычков С. И. О современных проблемах проведения судебно-компьютерных экспертиз в ходе предварительного расследования // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 2 (34). С. 293–298.

8. Москаленко В. Н. Особенности изъятия объектов электронно-вычислительной техники в ходе производства следственных действий // Криминалист. 2021. № 4 (37). 80–87.

9. Типовая методика исследования информации, содержащейся в мобильных телефонах / О. В. Тушканова [и др.]. Москва: ЭКЦ МВД России, 2014. 32 с.

References

1. Averyanova T. V., Belkin R. S., Korukhov Y. G., Rossinskaya E. R. Criminology. Textbook for universities. Ed. by R. S. Belkin. Moscow: Norma; 2020: 928. (In Russ.).

2. Usov A. I. Forensic computer-technical expertise: formation, development, methodological support. Theory and practice of forensic science, 10–22, 2008. (In Russ.).

3. Rossinskaya E. R. Problems of using special knowledge in judicial investigation of computer crimes under digitalization. Courier of the Kutafin Moscow State Law University (MSAL), 31–44, 2019. (In Russ.).

4. Rossinskaya E. R., Ryadovsky I. A. Concept of digital traces in criminology. In: Aubakirov's readings. Materials of the International scientific and practical conference, 19 February 2019. Almaty; 2019: 6–9. (In Russ.).

5. Rossinskaya E. R. Forensic computer-technical expertise: problems of the formation and training of experts. Theory and practice of forensic examination, 60–66, 2008. (In Russ.).

6. Moskalenko V. N. Recommendations for optimization of the appointment of forensic computer expertise (as exemplified by Expert Forensic Center of the Main Department of the Russian Ministry of Internal Affairs in Saint Petersburg and Leningrad region). In: Saint Petersburg School of Criminology. Materials of V All-Russian foren-

sic forum, Saint Petersburg, 19–21 October 2023. General ed. by A. A. Sapozhkov; executive ed. E. V. Yelaghina. Saint Petersburg: St. Petersburg Law Institute (branch) of the University of Prosecutor's Office of the Russian Federation; 2024: 113–120. (In Russ.).

7. Kuvychkov S. I. On the modern problems of conducting forensic computer examinations during preliminary investigation. Legal science and practice: journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, 293–298, 2016. (In Russ.).

8. Moskalenko V. N. Characteristics of the seizure of electronic computing equipment during investigation. Criminologist, 80–87, 2021. (In Russ.).

9. Tushkanova O. V. (et al.) Standard methodology for the investigation of information contained in mobile phones. Moscow: Expert Forensic Center of the MIA of Russia; 2014: 32. (In Russ.).

Родина Елена Юрьевна,
старший преподаватель кафедры криминалистики
Санкт-Петербургского университета МВД России;
elena_rodina1981@mail.ru

Москаленко Василий Николаевич,
начальник экспертно-криминалистического центра
ГУ МВД России по г. Санкт-Петербургу и Ленинградской области;
lashpartuns@yandex.ru

Rodina Elena Yuryevna,
senior lecturer at the department of criminology
of the Saint Petersburg University of the Ministry of the Interior of Russia;
elena_rodina1981@mail.ru

Moskalenko Vasily Nikolaevich,
head of the Forensic Center of the Ministry of Internal Affairs of Russia
in Saint Petersburg and Leningrad region;
lashpartuns@yandex.ru

Статья поступила в редакцию 22.09.2024; одобрена после рецензирования 26.09.2024; принята к публикации 15.11.2024.

The article was submitted 22.09.2024; approved after reviewing 26.09.2024; accepted for publication 15.11.2024.

* * *