РАЩУПКИНА ВАЛЕНТИНА АЛЕКСЕЕВНА
Экспертно-криминалистический центр МВД России
(Москва, Россия)

vdudchenko4@mvd.ru

О СОВЕРШЕНСТВОВАНИИ ПРОЦЕССУАЛЬНОГО ПОРЯДКА СОБИРАНИЯ ДОКАЗАТЕЛЬСТВ В КОМПЬЮТЕРНЫХ СЕТЯХ

Аннотация. Данная статья направлена на обозначение такого проблемного аспекта, как процессуальный порядок собирания доказательственной информации в компьютерных сетях. Автором рассматриваются некоторые ранее выдвинутые научные предложения, направленные на разрешение проблемных вопросов касательно условий и порядка проведения следственных действий с целью визуального восприятия и исследования информации, размещенной на локальных и сетевых электронных носителях, а также в компьютерных сетях. Дается определение принудительного обследования информационной системы, находящейся на электронных носителях за пределами места производства следственного действия. Приводится перечень действующего законодательства и актуальных нормативных правовых актов, направленных на регулирование отношений, возникающих при взаимодействии органов предварительного следствия и операторов связи, оказывающих услуги подключения к информационно-коммуникационным сетям, а также организаторов распространения информации в сети Интернет. Особое внимание уделено рассмотрению проблем и перспектив получения такого вида криминалистически значимой информации, как cookie-файлы. Дается их определение, приводится классификация основных видов. Обозначена необходимость дополнения состава информации, подлежащей хранению организатором распространения информации в сети Интернет, с целью профилактики и противодействия преступности в Российской Федерации.

Ключевые слова и словосочетания: цифровая криминалистика, компьютерные сети, расследование преступлений, собирание доказательственной информации, субъекты информационно-телекоммуникационной инфраструктуры

Для цитирования: Ращупкина В.А. О совершенствовании процессуального порядка собирания доказательств в компьютерных сетях // Вестник ВИПК МВД России. – 2023. – № 3(67). – С. 141-145; doi: 10.29039/2312-7937-2023-3-141-145.

RASCHUPKINA VALENTINA A.
Expert Forensic Center of the Ministry of Internal Affairs of Russia
(Moscow, Russia)

ON IMPROVING THE PROCEDURAL PROCEDURE FOR COLLECTING EVIDENCE IN COMPUTER NETWORKS

Annotation. This article is aimed at identifying such a problematic aspect as the procedural procedure for collecting evidentiary information in computer networks. The author considers some previously put forward scientific proposals aimed at resolving problematic issues

regarding the conditions and procedure for conducting investigative actions for the purpose of visual perception and research of information placed on local and network electronic media, as well as in computer networks. The definition of compulsory examination of an information system located on electronic media outside the place of the investigative action is given. The list of current legislation and current regulatory legal acts aimed at regulating relations arising from the interaction of preliminary investigation bodies and telecom operators providing connection services to information and communication networks, as well as organizers of the dissemination of information on the Internet is given. Particular attention is paid to the problems and prospects of obtaining such criminally significant information as cookies. Their definition is given; the classification of the main types is given. The necessity of supplementing the composition of the information to be stored by the organizer of the dissemination of information on the Internet for the purpose of preventing and combating crime in the Russian Federation is indicated.

Key words and word combinations: digital forensics, computer networks, investigation of crimes, collection of evidentiary information, subjects of information and telecommunications infrastructure

For citation: Rashchupkina V.A. On improving the procedural procedure for collecting evidence in computer networks // Vestnik Advanced Training Institute of the MIA of Russia. – 2023. – № 3(67). – P. 141-145; doi: 10.29039/2312-7937-2023-3-141-145.

Использование достижений научно-технического прогресса, а именно современных возможностей применения криминалистических средств и методов стало одним из ключевых направлений формирования эффективных мер по раскрытию и расследованию преступлений различных категорий. Технико-криминалистическое обеспечение и применение новейших разработок криминалистической техники позволяют решать большинство задач, связанных с раскрытием и расследованием преступлений, в том числе задач, направленных на сбор значимой криминалистической информации и иных доказательств. Вместе с тем внедрение современных достижений естественных и технических наук, информационных технологий сопровождается появлением новых теоретических пробелов, требующих от научного сообщества оперативного вмешательства и разрешения [6, с. 135].

Таким спорным положением стало отсутствие в действующем российском законодательстве нормативного правового акта, определяющего процессуальный порядок собирания доказательственной информации, находящейся в компьютерных сетях. Стоит отметить, что вопросы, касающиеся правовой природы и процессуального регулирования следственных действий, направленных на получение и исследование компьютерной информации, отражены в работах В.Б. Вехова, А.Г. Волеводза, Ю.В. Гаврилина, Р.А. Дерюгина, С.В. Зуева, Г.И. Козырева, Е.С. Лапина, В.А. Мещерякова, П.С. Пастухова, С.Б. Россинского, В.Ю. Стельмаха и других авторов. Однако данная проблема по сегодняшний день продолжает существовать и требует проведения всестороннего научного исследования.

В настоящее время собирание доказательственной информации в компьютерных сетях осуществляется преимущественно в рамках следственного осмотра, под которым понимаются непосредственное восприятие и обозрение следователем материальных объектов в целях выяснения обстановки совершения преступления, обнаружения и закрепления следов преступления, получения предметов, которые могут быть вещественными доказательствами, документов и установления иных обстоятельств, имеющих значение для уголовного дела. Сходное определение следственного осмотра как осуществляемого следователем в соответствии с предусмотренной законом процедурой обследования места происшествия, жилища, иного помещения, предметов и документов в целях обнаружения следов преступления, иной, выраженной в физических признаках информации, имеющей значение для дела, ранее давал С.А. Шейфер [7, с. 45].

По мнению А.Г. Волеводза, «действующее уголовно-процессуальное законодательство, регламентируя порядок привлечения специалистов к участию в

следственных действиях, не учитывает особенностей следов в сфере компьютерной информации, не регламентирует особый (с применением программно-аппаратных средств) порядок их фиксации (копирования), не определяет особых условий этого» [3, с. 14].

В свою очередь, А.Л. Осипенко в своих работах отмечает, что процессуальное изучение содержимого, находящегося в сетевой вычислительной системе, в реальности отличается по характеру производимых действий от обыска помещения. Для просмотра файлов, содержащихся в системе, требуются специальные знания, набор специализированных программ и особых аппаратных средств. Кроме того, в некоторых случаях такой просмотр удобнее осуществлять удаленно, т.е. осматривать содержимое одного компьютера, находясь при этом за другим [4, с. 274].

Разделяют представленную точку зрения в своих научных работах Ю.В. Гаврилин и А.А. Балашова. В статье «Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах» авторы формулируют такие понятия, как «дистанционный осмотр информационных ресурсов» и «дистанционный обыск» [2, с.133-135] При этом под дистанционным осмотром информационных ресурсов понимается «следственное действие, состоящее в визуальном восприятии информации, размещенной на сетевых электронных носителях, доступ к которым предоставлен неограниченному числу лиц», а под дистанционным обыском – «следственное действие, состоящее в принудительном обследовании информационной системы, находящейся на электронных носителях за пределами места производства следственного действия, доступ к которым ограничен ее обладателем и осуществляется посредством компьютерных сетей». Кроме того, в проведенном диссертационном исследовании «Электронные носители информации и их использование в уголовно-процессуальном доказывании» А.А. Балашовой выдвигается инициатива о дополнении глав 24 и 25 действующего Уголовно-процессуального кодекса Российской Федерации ст. 1781 «Дистанционный осмотр электронных (цифровых) информационных ресурсов» и ст. 182 «Дистанционный обыск» [1, с. 132].

В данном аспекте мы считаем обоснованными выдвинутые предложения. Также хотелось бы отметить, что помимо собирания доказательственной информации в процессе проведения таких следственных действий, как осмотр места происшествия, обыск и выемка, определяющей ролью в расследовании и раскрытии преступлений, совершаемых в компьютерных сетях, является активное сотрудничество правоохранительных органов с субъектами, обеспечивающими функционирование информационно-телекоммуникационной инфраструктуры: интернет-провайдерами, операторами связи, кредитно-финансовыми организациями и др.

Порядок такого взаимодействия определен рядом правовых требований, указанных действующим законодательством Российской Федерации, а именно ч. 6 ст. 10.1 Федерального закона от 27.07.2006 № 149-ФЗ[1], постановлением Правительства Российской Федерации от 23.09.2020 № 1526[2] и др. Данные нормативные правовые акты предусматривают состав, правила хранения и порядок представления информации о фактах приема, передачи, доставки, обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» уполномоченным государственным правоохранительным органам.

---

[1] Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ // Собр. зак-ва РФ. 2006. № 31 (ч. 1). Ст. 3448.

[2] О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях и предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации: постановление Правительства РФ от 23.09. 2020 № 1526 // Собр. зак-ва РФ. 2020. № 40. Ст. 6258

Хотелось бы отметить, что законодателем достаточно своевременно внесены поправки в ст. 185 Уголовно-процессуального кодекса Российской Федерации «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка». Федеральным законом от 06.07.2016 № 375-ФЗ данная статья была дополнена ч. 7, которая позволила расширить круг полномочий следователя по получению информации об электронных сообщениях. Надо сказать, что данные положения стали первыми в регулировании отношений, возникающих при взаимодействии органов предварительного следствия и операторов связи, оказывающих услуги подключения к информационно-коммуникационным сетям, а также организаторов распространения информации в сети Интернет.

Помимо информации, указанной в постановлении Правительства Российской Федерации от 23.09.2020 № 1526[3], полагаем необходимым дополнить существующий перечень информацией, хранящейся на стороне браузера, который может использоваться для получения информации или сокрытия преступной деятельности, а также для изучения новых методов совершения преступлений. Браузер хранит такие данные, как: список посещаемых веб-сайтов, время и частота доступа, а также ключевые слова в поисковой системе, используемой злоумышленником, список загрузок и др.

Современные интернет-сервисы используют при регистрации пользователей заполнение электронных форм, которые содержат: имена пользователей, должность и место работы, логины, пароли, паспортные данные, пол, даты рождения, контрольные секретные вопросы и ответы, адреса, социометрические данные и данные об их предпочтениях, а также информацию о действиях пользователей и многое другое. Весь перечисленный перечень информации, как правило, хранится на серверах организаций и активно используется для реализации различных целей, в том числе и при создании новых проектов. Однако, ввиду отсутствия в действующем законодательстве Российской Федерации правовых требований на хранение и прямого указания на передачу такого рода данных правоохранительным органам, зачастую эти сведения остаются неучтенными и неисследованными, что усложняет процесс расследования преступлений и увеличивает его срок.

К информации, хранящейся на стороне браузера, на веб-сайтах, у интернет-провайдеров и в компьютерных сетях также относятся данные, сохраняемые после просмотра пользователем веб-страниц в «приватном режиме», который зачастую используется в преступных целях злоумышленниками с целью сохранения инкогнито. Например, cookie-файлы представляют собой короткую именованную строку, которую сервер ассоциирует с браузером. Cookie-файлы используются для идентификации пользователя, а также отслеживания его действий и активности посещения тех или иных веб-страниц [5, с. 186].

В настоящий момент существуют несколько видов cookie-файлов. Сессионные (временные) хранятся на компьютере пользователя только в течение текущей сессии браузера и удаляются после закрытия браузера. Они обычно используются для хранения временных данных, таких как содержимое корзины покупок, чтобы пользователь мог продолжить покупки на следующих страницах сайта. Постоянные cookie-файлы хранятся на компьютере пользователя в папках браузера, который их сформировал, в течение заданного периода времени. Используются для запоминания предпочтений пользователя на сайте или для предоставления рекламы, которая соответствует интересам пользователя, а также содержат авторизационные данные для различных сайтов.

Основные cookie-файлы устанавливаются на устройстве пользователя через сайт, доменное имя которого отображается в адресной строке браузера. Сторонние cookie-файлы хранятся на сторонних серверах и используются рекламными сервисами, например, для сохранения рекламных баннеров или аналитических скриптов. «Super-cookie» хранятся только у провайдера и недоступны пользователям.

Cookie-файлы содержат значимую криминалистическую информацию (учетные записи, имена, адреса и пароли), что, несомненно, создает потребность в представлении такого рода данных субъектом информационно-телекоммуникационной

---

[3] О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации … .

инфраструктуры. Так, Ленинским районный судом г. Ростова-на-Дону 22 июля 2019 г. был вынесен обвинительный приговор в отношении гражданина Р.Л. Аржановского, который был признан виновным в совершении преступления, предусмотренного ст. 273 Уголовного кодекса Российской Федерации. Аржановский Р.Л. разработал и распространил в сети «Интернет» вредоносное программное обеспечение, предназначенное для копирования паролей и cookie-файлов из баз данных интернет-браузеров без согласия законных владельцев данной компьютерной информации. В ходе судопроизводства в качестве одного из важнейших вещественных доказательств выступила информация, хранимая на стороне браузера, которую в процессе производства следственных действий сравнили с информацией, находящейся в памяти персонального компьютера, изъятого у обвиняемого.

В настоящее время cookie-файлы могут быть получены по запросу от оперативных сотрудников в качестве источника доказательств только в общем массиве данных вместе с историей интернет-посещений и перечнем загрузок файлов, обращение с которым требует применение современных инструментов «big data». Данное обстоятельство вызывает у правоохранительных органов затруднение ввиду отсутствия у следствия специальных знаний в указанной области, высокой загруженности экспертов судебной компьютерной экспертизы, недостаточного материально-технического оснащения и ограничения по времени проведения следственных действий.

Поиск и анализ cookie-файлов с помощью специального программного обеспечения также осуществляется в ходе производства судебных компьютерных экспертиз и исследований, однако, как правило, обнаружить иные виды cookie-файлов, помимо постоянных, не представляется возможным.

Важность исследования такого вида данных, как cookie-файлы, и иной информации, хранящейся на стороне браузера, в рамках расследования преступлений, совершенных с использованием информационных технологий, обозначали в своих работах такие авторы, как: В.Б. Вехов, Ю.В. Гаврилин, Г.З. Гаспарян, В.А. Мещеряков, А.В. Нестеров, Е.Р. Россинская и др.

Разделяя обозначенную точку зрения, считаем актуальным и необходимым исследовать вопрос дополнения состава информации, подлежащей хранению организатором распространения информации в сети «Интернет» при обеспечении функционирования коммуникационного интернет-сервиса, в целях повышения эффективности расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

1. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: автореф. дис. … канд. юрид. наук. – М., 2020.
2. Балашова А.А., Гаврилин Ю.В. Совершенствование процессуального порядка собирания доказательственной информации, содержащейся в сетевых информационных системах // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13).
3. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях // Рос. следователь. 2002. № 1 (13).
4. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт. – М., 2004.
5. Ращупкина В. А. Цифровые следы: понятие, признаки, источники и особенности исследования // Уголовный процесс и криминалистика: теория, практика, дидактика: сб. материалов VIII Всерос. науч.-практ. конф. (Рязань, 16 дек. 2022 г.). – Рязань: Академия ФСИН России, 2023.
6. Романова О.Л., Макарова Е.Н. Современное состояние и перспективы развития криминалистических средств и методов, применяемых в практике расследования преступлений // Государственная научно-техническая политика в сфере криминалистического обеспечения правоохранительной деятельности: сб. науч. ст. по материалам междунар. науч.-практ. конф. «64-е ежегодные криминалистические чтения» (Москва, 26 мая 2023 г.): в 2 ч. / под. ред. Ю.В. Гаврилина. Б.Я. Гаврилова, В.О. Лапина, Ю.В. Шпагиной. – М.: Академия управления МВД России, 2023. Ч. 1.

7. Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение. – М.: Юрлитинформ, 2004.

About the author:

Информация об авторе:

В.А. Ращупкина, *научный сотрудник отдела научных исследований по специальным видам экспертиз и экспертно-криминалистического обеспечения противодействия наркопреступности управления научных исследований*

V.A. Rashchupkina, *researcher at the department of scientific research on special types of examinations and forensic support for combating drug crime, department of scientific research*

Статья поступила в редакцию 25.08.2023