DOI: 10.17803/1729-5920.2023.196.3.100-109

А. Б. Смушкин*,
М. М. Менжега**

Некоторые вопросы цифровизации криминалистики

Аннотация. В рамках цифровизации криминалистики следует подчеркнуть крайне актуальный вопрос поиска разумного баланса между частными и публичными интересами, между сохранением гарантированной Конституцией РФ тайны переписки, тайны личной жизни и т.д. и возможностями дистанционного получения информации без ведома пользователя, перехвата информации, передаваемой по компьютерным сетям, исследования памяти электронных устройств. Незаконные действия с электронной цифровой информацией способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям. Особенностями преступлений в сфере высоких технологий являются их высокая латентность и постоянный рост их количества. Следует отметить также изменение масштаба киберпреступлений. Возможность автоматизации «кибератак» снижает требования к квалификации нарушителя и увеличивает количество преступлений. Сложившаяся в настоящий момент ситуация обусловливает необходимость комплексного исследования не только вопросов расследования преступлений в сфере компьютерной информации, но и цифровизации криминалистики в целом. Технический прогресс XXI в. в сфере киберпространства и электронного документооборота, специфика электронной информации и способов ее изъятия, тактики производства настойчиво требуют расширения объектов криминалистики, а также круга следственных действий, регламентированных в УПК РФ. Однако к подобному расширению круга следственных действий следует подходить крайне взвешенно.
Методологическую основу исследования составили: диалектический метод как общенаучный метод познания; общенаучные и частнонаучные методы теоретического и эмпирического познания (особенностей отражения цифровой информации в информационной среде): описание; анализ и синтез точек зрения криминалистов; сравнительно-правовой метод и метод системного исследования.

Ключевые слова: преступность; киберпреступления; криминалистика; высокие технологии; криминалистическая тактика; расследование; цифровизация; цифровая криминалистика; электронная информация; следствие.

Для цитирования: *Смушкин А. Б., Менжега М. М.* Некоторые вопросы цифровизации криминалистики // Lex russica. — 2023. — Т. 76. — № 3. — С. 100–109. — DOI: 10.17803/1729-5920.2023.196.3.100-109.

* *Смушкин Александр Борисович,* кандидат юридических наук, доцент кафедры криминалистики Саратовской государственной юридической академии (СГЮА)
ул. Чернышевского, д. 104, г. Саратов, Россия, 410028
skif32@yandex.ru

** *Менжега Михаил Михайлович,* кандидат юридических наук, доцент кафедры криминалистики Саратовской государственной юридической академии (СГЮА)
ул. Чернышевского, д. 104, г. Саратов, Россия, 410028
wandol@mail.ru

Some Issues on Forensics Digitalization

Aleksandr B. Smushkin, Cand. Sci. (Law), Associate Professor, Department of Criminalistics, Saratov State Law Academy
ul. Chernyshevskogo, d. 104, Saratov, Russia, 410028
skif32@yandex.ru

Mikhail M. Menzhega, Cand. Sci. (Law), Associate Professor, Department of Criminalistics, Saratov State Law Academy
ul. Chernyshevskogo, d. 104, Saratov, Russia, 410028
wandol@mail.ru

Abstract. Amid forensics digitalization, an extremely urgent issue is to find a reasonable balance between private and public interests, between preserving the secrecy of correspondence, privacy, etc., guaranteed by the Constitution of the Russian Federation and the availability for obtaining information remotely without the user knowing about it, intercepting information transmitted over computer networks, and studying the memory of electronic devices. Illegal actions with electronic digital information can cause serious and irreversible consequences associated not only with property damage, but also with physical harm to people. The peculiarities of high-tech crimes are their high latency and the constant growth of their number. We should note that the scale of cybercrime has changed. The possibility that «cyber attacks» will be automated reduces the requirements for the qualification of the violator and increases the number of crimes. The current situation necessitates a comprehensive study of not only the investigation of crimes in the field of computer information, but also the digitalization of forensics in general. The technological progress of the 21st century in the field of cyberspace and electronic document management, the specifics of electronic information and methods of its seizure, production tactics persistently require the expansion of forensics objects, as well as the range of investigative actions regulated in the Code of Criminal Procedure of the Russian Federation. However, such an expansion of the range of investigative actions should be approached very carefully.
The methodological basis of the study was: dialectical method as a general scientific method of cognition; general scientific and private scientific methods of theoretical and empirical cognition (features of the reflection of digital information in the information environment): description; analysis and synthesis of criminologists' points of view; comparative legal method and method of system research.
Keywords: crime; cybercrime; forensics; high-tech solutions; forensic tactics; investigation; digitalization; digital forensics; electronic information; investigation.
Cite as: Smushkin AB, Menzhega MM. Nekotorye voprosy tsifrovizatsii kriminalistiki [Some Issues on Forensics Digitalization]. *Lex russica*. 2023;76(3):100-109. DOI: 10.17803/1729-5920.2023.196.3.100-109. (In Russ., abstract in Eng.).

В научной, в том числе юридической, литературе можно встретить термины, которые призваны закрепить категориальный аппарат, такие как искусственная реальность, дополненная реальность, цифровая виртуальность. Можно отметить формирование и развитие в криминалистической науке учения о виртуальных следах преступления. Преступность гораздо быстрее криминалистических разработок начала использовать информационную среду, что обуславливает некоторое отставание криминалистики в области разработок, необходимых для расследования и раскрытия преступлений в киберпространстве. В связи с этим можно отметить важность разработок гносеологической природы следов в киберпространстве электронных устройств, их типологии, особенностей выявления, сохранения, изъятия и исследования, непосредственно связанных со специфической природой электронной информации и закономерностями работы с ней. Не менее важной представляется и разработка аппаратно-программного обеспечения для работы с любыми видами следов, а также интеллектуально-справочной помощи следователю и обработки больших массивов информации.

Можно отметить несколько аспектов цифровизации в криминалистике:

1) повышение качества организации работы, управления и взаимодействия различных органов при расследовании преступлений;
2) разработка актуальных, отвечающих требованиям настоящего момента рекомендаций по работе с электронной цифровой инфор-

мацией, информационно-технологическими устройствами и конкретно с виртуальными следами в ходе расследования;

3) активное использование современных цифровых технологий (аппаратно-программного обеспечения) в процессе поисково-познавательной деятельности в ходе расследования преступлений, а также непосредственное внедрение перспективных разработок;
4) применение современных технологий в процессе профессиональной подготовки, переподготовки и повышения квалификации, в сфере обмена опытом.

Зачастую авторы излишне сужают сущность цифровизации. Так, Н. Г. Шурухнов указывает, что «цифровизация непосредственного производства следственных и иных процессуальных действий представляет собой систему приемов, средств, технологий и методических рекомендаций, предназначенных для обнаружения электронных носителей информации, получения содержащихся в них сведений, определения их роли в активизации познавательной деятельности и использования для эффективности дальнейшего расследования преступления»[1]. По нашему же мнению, цифровизация представляет собой специфическое направление технологизации и инновационного развития криминалистики. Цифровизация следственной деятельности, воплощающаяся в насыщении ее цифровыми устройствами обнаружения, фиксации, изъятия, исследования, обработки информации, коммуникации участников судопроизводства, разработке интеллектуальных помощников следователя, выступает одним из неотъемлемых элементов цифровой трансформации.

Есть и те, кто выступает априори против цифровизации, противопоставляя ей создание и развитие духовного человека, в том числе с помощью изменения норм материального и процессуального законодательства[2], или, наоборот, абсолютизирует программную сторону процесса. Так, О. С. Кучин указывает, что «настоящая цифровая криминалистика представляет собой сложную систему, включающую совокупность постоянно работающих программных обеспечений (программ) для исследования цифрового пространства в целях предотвращения и выявления преступлений, анализ цифрового материала, а также направленного исследования конкретных носителей цифровых данных или самих данных (например, логов) для выявления следов конкретного преступления. При этом ведущую роль в цифровой криминалистике, в отличие от науки криминалистики “традиционного” типа, играет именно специализированное программное обеспечение (ПО) и широта его возможностей, а не специалист или эксперт, а проще сказать, не человек (следователь, детектив, полицейский)»[3].

Представляется, что такой подход автора превращает цифровую криминалистику практически только в продвинутое подобие совокупности антивирусного программного обеспечения, сетевых экранов, брандмауэров и иных аналогичных, но чуть более специализированных программ. Выбор инструментария, интерпретация полученной информации, определение ее связи с рассматриваемым событием, доказательственной ценности, проверка с точки зрения относимости, допустимости, достоверности, определение тактики процессуальных действий, связанных с получением и изучением электронной информации и ее носителей, использование в доказывании и многие иные действия, которые не смогут совершить самые продвинутые программно-аппаратные комплексы, автором, видимо, не учитываются.

Нам представляется оптимальной формой наименования, а также определения направлений развития криминалистических знаний по рассматриваемому вопросу: частная тео-

---

1 *Шурухнов Н. Г.* Этапы цифровизации непосредственного производства следственных и иных процессуальных действий // Вестник Томского государственного университета. 2018. № 436. С. 252.

2 *Победкин А. В.* Уголовно-процессуальное законодательство Российской Федерации: оцифровать или одухотворить? // Криминалистика в условиях развития информационного общества (59-е Ежегодные криминалистические чтения) : сборник статей Международной научно-практической конференции. М. : Академия управления МВД России, 2018. С. 217–224.

3 *Кучин О. С.* О некоторых тенденциях развития мировой криминалистики // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : сборник статей XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае». Вып. XVI / Министерство науки и высшего образования РФ, Алтайский государственный университет ; отв. ред. С. И. Давыдов, В. В. Поляков. Барнаул : Изд-во Алт. ун-та, 2020. С. 28.

рия собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств, более компактно — «электронная цифровая криминалистика».

Второй стороной проблемы можно отметить отсутствие в криминалистике всеми признаваемого однозначного термина, характеризующего преступления, связанные с использованием высоких технологий. Так, употребляются термины «киберпреступность», «компьютерная преступность», «преступления в сфере компьютерной информации», «информационные преступления» и пр.

Часто такие понятия не совсем корректно, по нашему мнению, используются как синонимы, а некоторые применяются неверно. Законодатель, приняв в 1996 г. Уголовный кодекс РФ, в гл. 28 применил термин «преступления в сфере компьютерной информации». Однако в литературе его часто подменяют словосочетанием «компьютерные преступления», что, на наш взгляд, не является верным.

Так, с одной стороны, преступления в сфере компьютерной информации — более широкое понятие, поскольку уже достаточно давно произошла взаимная интеграция компьютеров с иными электронными устройствами и компьютерная информация свободно передается от компьютеров к мобильным телефонам, контрольно-кассовым аппаратам, телевизорам и прочим устройствам, и, к примеру, неправомерный доступ к информации, хранящейся на планшете (или внедрение в контрольно-кассовые аппараты вредоносной программы, которая искусственно занижает сумму выручки за смену), является не менее опасным. Такие преступления на практике квалифицируются по гл. 28 УК РФ, хотя фактически указанные выше устройства и не являются компьютерами.

С другой стороны, понятие «компьютерное преступление» охватывает иную сферу преступной деятельности, не имеющую отношения к гл. 28 УК РФ. Так, к «компьютерным преступлениям» можно отнести квартирную кражу, в результате которой похищен компьютер, изготовление поддельных денег при помощи соответствующего программного обеспечения и цветного принтера и пр. Некоторые авторы предлагают относить к таким преступлениям «мошенничество с применением банковских карт; мошенничество с выманиванием персональных данных; незаконное пользование услугами связи и иной обман в области услуг связи; промышленный и иной шпионаж и т.д.»[4], но предлагают исключить из разряда компьютерных преступлений «такие преступления, в которых компьютерная техника используется не в качестве таковой, а всего лишь как материальная ценность, потребитель электроэнергии и т.п.»[5]. Однако обоснование такого исключения, к сожалению, не приводится, и, на наш взгляд, буквальное толкование термина «компьютерное преступление» все-таки ближе к трактовке Н. Н. Федотова. Таким образом, использование термина «компьютерные преступления», на наш взгляд, является некорректным.

В мировом сообществе в настоящее время активно применяется термин «киберпреступность», в частности, он употребляется в Конвенции о киберпреступности, принятой Советом Европы в ноябре 2001 г. [6]

Определения киберпреступности, которые можно встретить в работах российских ученых, на наш взгляд, зачастую излишне широкие. Например, определение, предлагаемое Н. Н. Федотовым: «Киберпреступление — уголовное правонарушение, для расследования которого существенным условием является применение специальных знаний в области информационных технологий»[7]. На наш взгляд, без подобных знаний, например, затруднительна или вообще невозможна поимка преступника, похитившего сотовый телефон, да и расследование любого традиционного преступления, на этапе подготовки к которому использовались информационные технологии. В литературе также есть примеры, когда цифровое алиби способствовало реабилитации подозреваемого в вооруженном ограблении: исследование электрон-

---

4 *Тимошенко Е. А.* Компьютерная форензика и ее роль в процессе раскрытия и расследования преступлений в условиях глобальной цифровизации // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». 2022. Т. 4. № 14-2. С. 180.

5 *Федотов Н. Н.* Форензика — компьютерная криминалистика. М. : Юридический мир, 2007. С. 37.

6 Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) (Российская Федерация в настоящей Конвенции не участвует) // URL: https://base.garant.ru/4089723/ (дата обращения: 15.12.2022).

7 *Федотов Н. Н.* Указ. соч.

ного оборудования подозреваемого позволило установить, что в момент ограбления он работал в социальной сети Facebook со стационарного компьютера, расположенного по иному адресу[8].

Таким образом, приведенное выше определение киберпреступлений представляется нам излишне широким ввиду того, что знания в области информационных технологий в настоящее время могут быть существенным условием для расследования практически любых преступлений.

Проанализировав мнение ряда авторов, Т. Л. Тропина предлагает следующее определение преступления, совершенного в киберпространстве (то есть киберпреступления): «Это виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству»[9]. Настоящее определение также излишне широкое — сложно согласиться с тем, что киберпреступлениями будут «иные противоправные общественно опасные деяния, совершенные с помощью компьютеров». Так, подделка официального документа в целях его использования (ст. 327 УК РФ) с помощью компьютерной техники, по нашему мнению, всё же не является киберпреступлением.

В международной Конвенции о киберпреступности выделяются следующие разновидности таких преступлений:

1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;
2) правонарушения, связанные с использованием компьютерных средств;
3) правонарушения, связанные с содержанием данных;
4) правонарушения, связанные с нарушением авторского права и смежных прав.

Подраздел 2 этой Конвенции — «Правонарушения, связанные с использованием компьютерных средств» — ограничивает правонарушение с использованием компьютерных средств случаями «совершения преднамеренно и без права на это — ввода, изменения, стирания или блокирования компьютерных данных, влекущих за собой нарушение аутентичности данных с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных». На наш взгляд, речь идет именно о нарушении аутентичности данных, находящихся в информационно-телекоммуникационной среде, и к таким преступлениям не относятся преступления, которые могут быть совершены с использованием компьютерных средств, например изготовление подложных документов при помощи графического редактора и принтера.

Таким образом, к киберпреступлениям следует относить уголовно наказуемые деяния в сфере движения компьютерной информации, а также преступления, которые совершаются с использованием компьютерной информации, передаваемой посредством информационно-телекоммуникационной сети.

Киберпреступления можно подразделить на две группы: преступления в сфере компьютерной информации и преступления, совершаемые с использованием компьютерной информации, передаваемой посредством информационно-телекоммуникационной сети. В первую группу входят преступления, предусмотренные главой 28 УК РФ, во вторую — любые преступления, связанные с использованием компьютерной информации, передаваемой посредством информационно-телекоммуникационной сети, например мошенничества с использованием сайтов-двойников или призывы в социальных сетях к террористической деятельности.

Что касается тенденций «электронизации» следственных действий, то совершение многих преступлений в настоящее время в двух мирах (материальном и киберпространстве) насущно требует соответствующих процессуальных и непроцессуальных инструментов.

Действующее законодательство основано на примате материальной формы над цифровым

---

[8] См.: *Краснова Л. Б.* Использование особенностей информационных технологий для установления и проверки алиби // Воронежские криминалистические чтения: сборник науч. трудов. Вып. 16. Воронеж, 2014. С. 105.

[9] *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. … канд. юрид. наук. Владивосток, 2007. С. 16.

содержанием. С электронными устройствами в основном предлагается работать аналоговыми следственными действиями. В актуальном (на момент подготовки публикации) законодательстве предусмотрено крайне мало инструментов работы с цифровой информацией. Основным способом получения цифровой информации в ходе следственных действий остается изъятие электронных носителей информации: такой способ составляет 96 % случаев, и только 4 % приходится на копирование цифровой информации[10].

Фактически законодатель называет только 2 основных инструмента — следственное действие «Осмотр и выемка электронных сообщений или иных, передаваемых по сетям электросвязи сообщений» (ч. 7 ст. 185 УПК РФ) и оперативно-розыскное мероприятие «Получение компьютерной информации». При этом для производства указанного следственного действия необходимо соблюдение порядка и процедуры, предусмотренных статьей 185 «Наложение ареста на почтово-телеграфные отправления, их осмотр и выемка», что не всегда возможно в силу специфики электронной информации. Оперативно-розыскное мероприятие включает, «во-первых, негласное применение специального программного обеспечения или оборудования, для конспиративного съема данных с компьютерных устройств, во-вторых, оперативно-розыскной мониторинг сетевых информационных ресурсов. Данный мониторинг реализуется посредством автоматизированного поиска информации сотрудниками органа, осуществляющего оперативно-розыскную деятельность»[11].

Проводя компаративистское исследование зарубежного законодательства по рассматриваемому вопросу, несложно заметить, что иностранный законодатель во многом имеет более совершенные инструменты. Так, например, уголовный процесс Германии содержит: розыск по базам данных полиции (поиск в сети) (нем. Rasterfahndung. § 98a, 98b); машинное (автоматическое) сопоставление с существующими данными (нем. Maschineller Abgleich mit vorhandenen Daten, § 98c); контроль телекоммуникаций (нем. Telekommunikationsüberwachung, § 100a); онлайн-поиск (онлайн-обыск) (нем. Online-Durchsuchung, § 100b); сбор данных о трафике (нем. Erhebung von Verkehrsdaten, § 100g); технические следственные действия в отношении мобильных устройств (нем. Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten, § 100i); отчет о данных (нем. Bestandsdatenauskunft, § 100j); сбор данных об использовании телемедийных услуг (нем. Erhebung von Nutzungsdaten bei Telemediendiensten, § 100k); осмотр документов и электронных носителей информации (нем. Durchsicht von Papieren und elektronischen Speichermedien, § 110). При производстве отдельных следственных действий возможна дистанционная установка на компьютер подозреваемого специальной вирусной программы, записывающей всю интересующую следствие информацию[12]. В уголовном процессе Испании с 2015 г. предусмотрен целый спектр новелл в этом направлении: компьютерный агент под прикрытием, перехват телематических сообщений, регистрации устройств массового хранения информации и удаленных записей на компьютерном оборудовании, сбор данных о трафике лица, идентификация терминала подозреваемого по его IP-адресу или идентификация терминала путем захвата идентификационных кодов устройства или его компонентов и т.д.[13]

---

[10] *Крюкова Т. С.* Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики // Использование информационных технологий в уголовном судопроизводстве: проблемы теории и практики. 2016. № 4. С. 62.

[11] *Баженов С. В.* Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД. 2017. № 2. С. 32.

[12] Уголовное уложение (нем.: Strafgesetzbuch) от 15.05.1871 (в ред. 11 июля 2022 г.) // URL: http://www.gesetze-im-internet.de/stgb/BJNR001270871.html#BJNR001270871BJNG000102307 (дата обращения: 12.12.2022).

[13] Органический закон 13/2015 от 05.10.2015 «О внесении изменений в закон об уголовном судопроизводстве в целях укрепления процессуальных гарантий и регулирования технологических следственных мер» // Глава государства. 2015. № 239 (исп. Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica // Jefatura del Estado «BOE» núm. 239, de 6 de octubre de 2015). URL: https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10725-consolidado.pdf (дата обращения: 23.08.2022).

Как указывает А. Н. Яковлев, «внимательное изучение научно-технических публикаций по теме аналитической обработки общедоступной информации в современном цифровом обществе позволяет составить в первом приближении перечень такой информации:

— обезличенные сведения о соединениях абонентов мобильной связи;
— обезличенные сведения об IP-адресе сетевого оборудования;
— обезличенные сведения об имени Wi-Fi сети;
— обезличенные сведения о государственных регистрационных знаках автомобилей;
— иные обезличенные массивы информации»[14].

Как мы уже отмечали ранее, «представляется, что с помощью такого сетевого поиска можно как собрать информацию, необходимую для заведения дела оперативного учета или возбуждения уголовного дела, так и предположить планы изучаемого лица, выявить скрываемые связи или имущество»[15].

На этапе проверки сообщения о преступлении в порядке ст. 144 УПК РФ М. С. Сергеев указывает на то, что «электронные доказательства» могут быть получены в результате производства: 1) изъятия документов, предметов; 2) осмотра документов, предметов; 3) оперативных мероприятий; 4) истребования документов, предметов»[16]. В качестве самостоятельных «электронных» следственных действий данный автор называет «электронный осмотр» (а также «осмотр сайта»), «электронную выемку (копирование)»[17].

Нам представляется, что осмотр страниц в сети Интернет будет иметь существенную специфику по сравнению с осмотром материального объекта. Осмотр интернет-объекта возможен с любого терминала без личного нахождения на месте происшествия или изъятия материального объекта — сервера. С учетом специфики электронной информации в данном случае сто́ит принимать во внимание несколько мест происшествия: место совершения преступления, место наступления преступных последствий, сетевые адреса действий и наступления последствий (место происшествия в цифровой среде), место обнаружения преступного события, место нахождения следов в материальном и цифровом мире. Следует учитывать, что доступ к одному и тому же месту цифрового мира возможен из любого места материального мира, а также что доступ возможен с различных устройств одновременно. Задача следователя при расследовании дополняется доказыванием участия конкретного пользователя в совершении преступления, ведь использование его оборудования или его аккаунтов в сетях может быть даже без его ведома (взлом аккаунта, включение оборудования в бот-сети для DDoS-атак).

Спецификой рассматриваемых следственных действий можно также считать возможность доступа к интересующему объекту не только с изъятием материального объекта (сервера) или личным прибытием на место нахождения электронного устройства. Следователь может получить доступ к чужим страницам в сети Интернет со своего рабочего места. С использованием специализированных служебных программ («служебных вирусов», как в Германии) можно и дистанционно изучать чужие устройства. Во многих случаях вообще нет необходимости в изъятии материального объекта — сервера. Так, при размещении экстремистской информации на странице в социальной сети изъятие сервера может принести ущерб провайдерам, операторам сети, владельцам ресурса. При расследовании необходимо будет, на наш взгляд, снятие снимка экрана — скриншота и последующее блокирование (удаление) экстремистской информации, а также получение информации у провайдера и собственника социальной сети о владельце страницы и принадлежности определенного IP-адреса.

---

[14] *Яковлев А. Н.* Общедоступная цифровая информация в раскрытии и расследовании преступлений // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений : сборник материалов Всероссийской научно-практической конференции (Воронеж, 24–25 апреля 2014 г.). Воронеж : Воронежский институт МВД России, 2014. С. 28–32.

[15] *Смушкин А. Б.* К вопросу об электронных следственных действиях // Законодательство. 2019. № 11. С. 77.

[16] *Сергеев М. С.* Электронная проверка сообщений о преступлении // Электронные носители информации в криминалистике : материалы круглого стола, МГУ, Москва, 13 мая 2016 г. / под ред. проф. О. С. Кучина. М. : МГУ, 2016. С. 65.

[17] *Сергеев М. С.* Указ. соч. С. 67.

Проведенное нами исследование показывает существенные затруднения на практике с выбором метода изучения электронных отправлений (электронной почты, переписки в чатах, мессенджерах, социальных сетях и т.д.) в режиме реального времени (во время обмена подобными отправлениями)[18].

Характер и способ совершенного преступления может повлиять на доказательственную силу изъятого из электронного устройства материала. С одной стороны, полученная из электронного устройства информация может являться непосредственным предметом доказывания по конкретному уголовному делу (клевета, развратные действия, преступления экстремистского характера и др.), может иметь вспомогательную доказательственную функцию (в подтверждение вины лица, его приготовительных действий, возможных соучастников, в поиске похищенного и др.), а также может носить ориентирующую функцию (идентифицировать личность неопознанного трупа).

С учетом изложенного мы полагаем необходимым дополнить законодательство рядом норм: статьями 178.1 «Осмотр электронного объекта», 184.1 «Дистанционный сетевой обыск», 185.1 «Контроль электронных отправлений и их копирование», 186.2 «Сбор данных о трафике».

Изъятый в ходе обыска или выемки телефон или компьютер сами по себе не представляют интереса для следствия, главная ценность — информация, хранящаяся на этих носителях. Практика сложилась так, что копирование информации, как правило, осуществляется в ходе осмотра. Это привело к тому, что граждане, подвергшиеся обыску и изъятию электронных носителей, стали обращаться с жалобами в суд, так как, по их мнению, дальнейшие действия сотрудников нарушают их право на тайну переписки[19], предусмотренное Конституцией РФ. В данном случае оспаривается не факт изъятия, а факт дальнейшего осмотра носителя информации. Уголовно-процессуальное законодательство предоставляет возможность осмотра отдельных предметов как на месте обнаружения, так и после их изъятия. Такая необходимость обусловлена невозможностью или затруднением осмотра на месте. При этом для проведения осмотра как следственного действия не требуется разрешение суда. Эта норма УПК РФ вступает в противоречие со ст. 23 Конституции РФ, где говорится, что нарушение права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения. Неоднозначную точку в данном споре поставил Конституционный Суд РФ, который отказался принять к рассмотрению жалобу гражданина Д. А. Прозоровского и пояснил, что возможность осмотра электронного носителя информации не нарушает право на тайну переписки, а если лицо считает, что его права всё-таки были нарушены, то остается возможность оспорить следственные действия и процессуальные решения в порядке ст. 125 УПК РФ. Данное решение на первый взгляд выглядит нелогичным, так как проведение такого следственного действия, как получение информации о соединениях между абонентами и (или) абонентскими устройствами, в соответствии со ст. 186.1 УПК РФ допускается на основании судебного решения.

На наш взгляд, при проведении осмотра право на тайну переписки нарушается не в меньшей степени, чем при получении информации о соединениях, поэтому целесообразно было бы и данное следственное действие проводить на основании решения суда. Можно предположить, что, вынося рассматриваемое определение, Конституционный Суд исходил из того, что электронный носитель информации может быть получен сотрудниками правоохранительных органов в результате обыска или выемки. Данные следственные действия проводятся на основании решения суда, поэтому необходимость получения еще одного решения будет препятствовать оперативной работе органов. При этом суд явно не учел, что получить электронный носитель можно в результате такого следственного действия, как осмотр. Это может быть осмотр места происшествия или осмотр жилища. В соответствии со ст. 29 УПК РФ решение суда для производства осмотра жилища необходимо только тогда, когда проживающие в нем лица против проведения осмотра. Таким образом, возможна

[18] *Смушкин А. Б.* К вопросу об электронных следственных действиях // Законодательство. 2019. № 11. С. 78.

[19] Определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации» // СПС «КонсультантПлюс».

следующая ситуация: в результате осмотра жилища с согласия проживающих в нем лиц был обнаружен телефон. В соответствии с ч. 3 ст. 177 УПК РФ, если осмотр предметов на месте затруднен, они могут быть изъяты. Возникает ситуация, при которой изъять телефон или копировать с него информацию в порядке ст. 164.1 УПК РФ возможно и без решения суда. Надо отметить, что, имея в руках телефон, можно получить те же самые сведения, что и при проведении уже упомянутого выше следственного действия «Получение информации о соединениях между абонентами». Разница лишь в том, что для проведения последнего необходимо решение суда, а для ситуации из примера — нет. Таким образом, Конституционный Суд оставил возможность легально избежать судебного порядка при получении определенной информации.

В современных стремительно развивающихся условиях необходимо системное исследование киберпреступности как в целом, так и отдельных, наиболее распространенных ее видов, разработка эффективных мер борьбы и предупреждения преступлений. Таким образом, технический прогресс XXI в. в сфере киберпространства и электронного документооборота, специфика электронной информации и способов ее изъятия, тактики производства настойчиво требуют расширения объектов криминалистики, а также круга следственных действий, регламентированных в УПК РФ. Однако к подобному расширению круга следственных действий следует подходить крайне взвешенно.

БИБЛИОГРАФИЯ

1. *Баженов С. В.* Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД. — 2017. — № 2.
2. *Краснова Л. Б.* Использование особенностей информационных технологий для установления и проверки алиби // Воронежские криминалистические чтения : сборник науч. трудов. — Вып. 16. — Воронеж, 2014.
3. *Крюкова Т. С.* Некоторые вопросы изъятия электронных носителей информации в ходе производства следственных действий: анализ судебной практики // Использование информационных технологий в уголовном судопроизводстве: проблемы теории и практики. — 2016. — № 4. — С. 61–63.
4. *Кучин О. С.* О некоторых тенденциях развития мировой криминалистики // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : сборник статей XVIII Международной научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае». — Вып. XVI / Министерство науки и высшего образования РФ, Алтайский государственный университет ; отв. ред. С. И. Давыдов, В. В. Поляков. — Барнаул : Изд-во Алт. ун-та, 2020.
5. *Победкин А. В.* Уголовно-процессуальное законодательство Российской Федерации: оцифровать или одухотворить? // Криминалистика в условиях развития информационного общества (59-е Ежегодные криминалистические чтения) : сборник статей Международной научно-практической конференции. — М. : Академия управления МВД России, 2018. — С. 217–224.
6. *Сергеев М. С.* Электронная проверка сообщений о преступлении // Электронные носители информации в криминалистике : материалы круглого стола, МГУ, Москва, 13 мая 2016 г. / под ред. проф. О. С. Кучина. — М. : МГУ, 2016. — С. 65.
7. *Смушкин А. Б.* К вопросу об электронных следственных действиях // Законодательство. — 2019. — № 11.
8. *Тимошенко Е. А.* Компьютерная форензика и ее роль в процессе раскрытия и расследования преступлений в условиях глобальной цифровизации // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». — 2022. — Т. 4. — № 14-2. — С. 178–182.
9. *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. … канд. юрид. наук. — Владивосток, 2007.
10. *Федотов Н. Н.* Форензика — компьютерная криминалистика. — М. : Юридический мир, 2007. — 432 с.
11. *Шурухнов Н. Г.* Этапы цифровизации непосредственного производства следственных и иных процессуальных действий // Вестник Томского государственного университета. — 2018. — № 436.
12. *Яковлев А. Н.* Общедоступная цифровая информация в раскрытии и расследовании преступлений // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений : сборник материалов Всероссийской научно-практической конференции (Воронеж, 24–25 апреля 2014 г.). — Воронеж : Воронежский институт МВД России, 2014. — С. 28–32.

Материал поступил в редакцию 20 декабря 2022 г.

REFERENCES

1. Bazhenov SV. Operativno-rozysknoe meropriyatie «Poluchenie kompyuternoy informatsii» [Operational search event «Obtaining computer information»]. *Nauchnyy vestnik Omskoy akademii MVD Rossii [Scientific Bulletin of the Omsk Academy of the MIA of Russia].* 2017;2. (In Russ.).
2. Krasnova LB. Ispolzovanie osobennostey informatsionnykh tekhnologiy dlya ustanovleniya i proverki alibi [Using information technology features to establish and verify an alibi]. *Voronezhskie kriminalisticheskie chteniya: sbornik nauch. trudov [Voronezh forensic readings: Collection of scientific works]*. 2014;16. (In Russ.).
3. Kryukova TS. Nekotorye voprosy izyatiya elektronnykh nositeley informatsii v khode proizvodstva sledstvennykh deystviy: analiz sudebnoy praktiki [Some issues of electronic data storage seizure in the course of investigative actions: Analysis of judicial practice]. *Pravoporyadok: istoriya, teoriya, praktika [Legal Order: History, Theory, Practice].* 2016;4:61-63. (In Russ.).
4. Kuchin OS. O nekotorykh tendentsiyakh razvitiya mirovoy kriminalistiki [On some trends in the development of world criminology]. In: Davydiv SI, Polyakov VV, editors. Problemy borby s prestupnostyu v usloviyakh tsifrovizatsii: teoriya i praktika: sbornik statey XVIII Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Ugolovno-protsessualnye i kriminalisticheskie chteniya na Altae [Problems of combating crime in the context of digitalization: Theory and practice. Proceedings of 18th International Scientific and Practical Conference «Criminal procedure and criminalistic readings in Altay»]. Issue 16. Ministry of Science and Higher Education of the Russian Federation, Altai State University. Barnaul: Altai University Publishing House; 2020. (In Russ.).
5. Pobedkin AV. Ugolovno-protsessualnoe zakonodatelstvo Rossiyskoy Federatsii: otsifrovat ili odukhotvorit? [Criminal procedure legislation of the Russian Federation: Digitize or spiritualize?]. In: Kriminalistika v usloviyakh razvitiya informatsionnogo obshchestva (59-e ezhegodnye kriminalisticheskie chteniya): sbornik statey mezhdunarodnoy nauchno-prakticheskoy konferentsii [Criminalistics in the context of the development of the Information Society (59th Annual Forensic Readings). Proceedings of the International scientific and practical conference]. Moscow: Akademiya upravleniya MVD Rossii Publ.; 2018. Pp. 217–224. (In Russ.).
6. Sergeev MS. Elektronnaya proverka soobshcheniy o prestuplenii [Electronic verification of crime reports]. In: Kuchin OS, editor. Elektronnye nositeli informatsii v kriminalistike: materialy kruglogo stola [Electronic media in criminalistics: Proceedings of the roundtable]. Moscow State University, Moscow, May 13, 2016. Moscow: Moscow State University Publ.; 2016. P. 65. (In Russ.).
7. Smushkin AB. K voprosu ob elektronnykh sledstvennykh deystviyakh [On the issue of electronic investigative activities]. *Zakonodatelstvo [Legislation].* 2019;11. (In Russ.).
8. Timoshenko EA. Kompyuternaya forenzika i ee rol v protsesse raskrytiya i rassledovaniya prestupleniy v usloviyakh globalnoy tsifrovizatsii [Computer forensics and its role in the process of solving and investigating crimes in the context of global digitalization]. *Vestnik studencheskogo nauchnogo obshchestva GOU VPO «Donetskiy natsionalnyy universitet» [Bulletin of the Student Scientific Society of Donetsk National University].* 2022;4(14-2):178-182. (In Russ.).
9. Tropina TL. Kiberprestupnost: ponyatie, sostoyanie, ugolovno-pravovye mery borby: avtoref. dis. … kand. yurid. nauk [Cybercrime: Concept, state, criminal law measures of struggle. Author's abstract of Cand. Sci. (Law) Thesis]. Vladivostok; 2007. (In Russ.).
10. Fedotov NN. Forenzika — kompyuternaya kriminalistika [Forensics — computer criminalistics]. Moscow: Yuridicheskiy Mir; 2007. (In Russ.).
11. Shurukhnov NG. Etapy tsifrovizatsii neposredstvennogo proizvodstva sledstvennykh i inykh protsessualnykh deystviy [Stages of digitalization of direct production of investigative and other procedural actions]. *Vestnik Tomskogo gosudarstvennogo universiteta [Tomsk State University Journal]*. 2018;436. (In Russ.).
12. Yakovlev AN. Obshchedostupnaya tsifrovaya informatsiya v raskrytii i rassledovanii prestupleniy [Publicly available digital information in the disclosure and investigation of crimes]. In: Prestupnost v sfere informatsionno-telekommunikatsionnykh tekhnologiy: problemy preduprezhdeniya, raskrytiya i rassledovaniya prestupleniy: sbornik materialov vserossiyskoy nauchno-prakticheskoy konferentsii (Voronezh, 24–25 aprelya 2014 g.) [Crime in the field of information and telecommunication technologies: Problems of prevention, disclosure and investigation of crimes. Proceedings the All-Russian Scientific and Practical Conference (Voronezh, April 24–25, 2014)]. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia Publ.; 2014. Pp. 28–32. (In Russ.).