

## СЕКЦИЯ 5 ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ В ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЕ НА СОВРЕМЕННОМ ЭТАПЕ

УДК 343.98:004

**Карепанов Николай Васильевич,**  
кандидат юридических наук, доцент,  
Уральский государственный юридический университет,  
г. Екатеринбург, Российская Федерация  
*karepanovvv@gmail.com.*

### **Технология поиска и исследований цифровых следов**

*В статье изложены положения об особенностях и разнообразии информационных технологий поиска и исследования цифровых следов. Технологией поиска и исследования цифровых следов в криминалистике посвящено достаточно много научных статей, монографий и даже новое криминалистическое учение. В статье цифровой след представляется как достаточно новый объект поиска и исследования, который, в частности, следует понимать как своеобразную криминалистически значимую компьютерную информацию о каких-либо событиях. Подчеркивается ее неразрывная связь с ситуационным подходом. Рассматривается также вопрос о статусе компьютерной программы в системе цифровых следов. Указывается на неоправданное преувеличение ее значения некоторыми авторами, признающими ее самостоятельным объектом исследования (так как она производит ряд важных манипуляций с данными: создает, обрабатывает, удаляет и др.). Вместе с тем, как утверждается в статье со ссылкой на технических специалистов, компьютерная программа всегда представлена только как совокупность инструкций и не более. Технология поиска цифровых следов предполагает некоторую подготовку к нему и строго определенный порядок действий.*

**Ключевые слова:** цифровые следы, технология, поиск, исследование, компьютерная информация, программное обеспечение, алгоритм действий.

**Kararepanov Nikolai Vasilyevich,**  
candidate of legal sciences, associate professor,  
Ural State Law University,  
Yekaterinburg, Russian Federation

### **Technology for searching and researching digital traces**

*The article outlines the provisions on the peculiarities and diversity of information technologies for the search and study of digital traces. Quite a lot of scientific articles, monographs and even a new forensic doctrine are devoted to the technologies of search and research of digital traces in forensics. In the article, the digital footprint is presented as a fairly new object of search*

*and research, which, in particular, should be understood as a kind of forensically significant computer information about any events. It is emphasized that it is inextricably linked with the situational approach. The question of the status of a computer program in the system of digital traces is also considered. It is pointed out that its importance is unjustifiably exaggerated by some authors who recognize it as an independent object of study (since it produces several important manipulations with data: it creates, processes, deletes, etc.). At the same time, as stated in the article with reference to technical specialists, a computer program is always presented only as a set of instructions and no more. Technology searching for digital traces involves some preparation for it and a strictly defined procedure.*

**Keywords:** *digital traces, technology, search, research, computer information, software, algorithm of actions.*

Цифровизация во всех сферах деятельности общества оказала существенное влияние на судопроизводство вообще, и на особенности и разнообразие информационных технологий поиска и исследования цифровых следов на специфических компьютерных носителях, в частности [1, с. 6–9; 2, с. 31–44]. Законодатель определяет их «как процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов» [7, ст. 39]. Технологиям поиска и исследования цифровых следов в криминалистике посвящено новое криминалистическое учение «Криминалистическое исследование компьютерных средств и систем» [3, с. 745–759]. В этом учении и в системообобщенной его теории информационно-компьютерного обеспечения криминалистической деятельности обоснованы понятия цифровых следов, описаны их виды и способы собирания [4, с. 193–202; 5, с. 106–123]. Несмотря на серьезность представленных научных трудов, самую большую распространенность цифровых следов сегодня пока отсутствует хорошая теоретическая база их исследования.

Цифровой след как достаточно новый объект поиска и исследования следует представлять как криминалистически значимую компьютерную информацию о каких-либо событиях, действиях или актах, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи [6, с. 263]. Цифровые следы не отделимы от носителей: устройств для записи и хранения сведений; для ввода/вывода информации; ее обработки, передачи по каналам связи; систем обработки информации или отдельных функциональных устройств таких систем; системных блоков персональных компьютеров, ноутбуков, нетбуков; машинных носителей (накопителей на жестких и гибких магнитных дисках, флэш-накопителей, карт памяти, оптических дисков; мобильных телефонов сотовой связи, смартфонов, планшетов, SIM-карт; навигаторов, трекеров; платежных пластиковых карт и скимминговых устройств; плат игровых автоматов; видеорегистраторов и др. Познания технологии поиска и исследования цифровых следов содержат их классификацию, общие положения технологии работы и правила обращения с ними и их носителями в целях их сохранности и пригодности. Кроме того, познания в этой области науки разрешают множество сложных проблем, возникающих в связи с их интеграцией и дифференциацией в системе IT-технологий. Одна из таких проблем представляется в виде комплексности цифровых следов. Родовая классификация цифровых

следов и их носителей включает в себя технические (аппаратные) средства компьютерных систем; программное обеспечение; компьютерные данные; сетевая информация; фоно и фотоизображения. Технология поиска и исследования цифровых следов неразрывно связана с ситуационным подходом. Исследование отдельных носителей (жесткого магнитного диска (HDD), флэш-карты, лазерного диска и пр.) осуществляется с использованием методов в рамках комплексной методики. Так же как и поиск цифровых следов в компьютерных системах и сетях, планшетах, мобильных коммуникаторах, на серверах, в облачных хранилищах. Кроме случаев их агрегирования или исследования, не требующего технической расшифровки сведений. Достаточно часто в качестве цифровых следов выступают электронные документы (сомнительные или не вызывающие сомнения в их подлинности), которые анализируются в соответствии с задачами исследования. Созданные с помощью программных продуктов образы цифровых следов на бумажных носителях (распечатки скриншотов, электронных документов и др.) исследуются с использованием различных графических процессоров и пр.

Независимо от существующих ситуаций поиска и исследования цифровых следов необходимо иметь представление о технологии их выявления, фиксации и изъятия, обладать умениями и навыками правильно оценивать пригодность, сохранность и достаточность этих объектов для производства исследования и формирования обоснованного вывода.

Любые цифровые следы с точки зрения криминалистики являются компьютерной информацией, необходимой для хранения определенных сведений, их обработки и передачи посредством вычислительной техники. Не простым, но важным представляется вопрос о статусе компьютерной программы. Некоторые авторы признают ее самостоятельным объектом исследования, которая производит ряд манипуляций с данными (создает, обрабатывает, удаляет и др.). Вместе с тем, по утверждениям технических специалистов, программа всегда представлена совокупностью инструкций и не более. Такая позиция способствует правильному применению ряда криминалистических понятий (идентификация, классификация, диагностика) к компьютерной информации. Так, для проведения идентификации объекта по компьютерной информации нужно представить в цифровой форме сведения об идентификационных свойствах объекта. Программы же можно диагностировать (устанавливать свойства процессов), классифицировать (устанавливать наименования, сведения о правообладателях, авторах и др.).

Технология поиска цифровых следов предполагает некоторую подготовку к нему, в процессе которой следует выяснить: необходимость проведения предварительных оперативно-технических мероприятий (установление местонахождения и функционального значения цифрового оборудования; наличия средств защиты и способы доступа); способы изъятия компьютерной информации (копирование, изъятие носителей и др.); состав оборудования необходимый для поиска; особенности и порядок действий (последовательность, привлечение персонала, порядок отключения устройств и др.).

Следует учесть ряд достаточно важных обстоятельств. Искомая информация может быть расположена территориально в хорошо охраняемом помещении или облачном хранилище. Цифровые следы преступной деятельности могут быть оставлены территориально удаленно в средствах компьютерной техники, расположенных по всему миру. При этом полностью отсутствуют ограничения для хранения, обработки и передачи информации, что может привести к потере, подмене или уничтожению искомым сведений.

Кроме того, компьютерная информация может быть защищена от несанкционированного доступа (дистанционно управляемые автономные устройства для уничтожения сведений; аппаратные, программные, программно-аппаратные средства криптографической защиты данных). Важным является осведомленность о возможных методах размещения данных на носителях, способах их обработки и форматах представления (хранение возможно в базах данных, специфических файлах и др.; возможно использование узкоспециализированного уникального программного обеспечения).

В конечном итоге, очень важно то, что технология поиска и исследования цифровых следов предполагает строго определенный порядок действий (не просто алгоритм, а именно строгая последовательность поведения). Правильное понимание и точное соблюдение этого постулата является ключом технологического процесса.

### **СПИСОК ИСТОЧНИКОВ**

1. Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы международной научно-практической конференции (19 февраля 2019 г.). Алматы, 2019. С. 6–9.

2. 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.

3. Россинская Е. Р., Семикаленова А. И. Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник Санкт-Петербургского университета. Право. 2020. Т. 11, вып. 3. С. 745–759.

4. Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (99). С. 193–202.

5. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106–123.

6. Россинская Е. Р. Учение о цифровизации судебно-экспертной деятельности в системе частных теорий судебной экспертологии // Теория и практика судебной экспертизы в современных условиях : материалы VIII Международной научно-практической конференции. М. : РГ-Пресс, 2021. С. 263.

7. Федеральный закон № 73-ФЗ от 31 мая 2001 г. «О государственной судебно-экспертной деятельности» (ред. от 26.07.2019). URL: <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102071320> (дата обращения: 30.11.2021).

УДК 34

**Ковтун Карина Александровна,**  
студент, Санкт-Петербургский государственный  
политехнический университет,  
г. Санкт-Петербург, Российская Федерация  
*wertoment@mail.ru*

**Осуществление прокурорского надзора  
в сфере киберпреступности  
в информационно-телекоммуникационной сети Интернет.  
Актуальные тенденции развития**

*В статье предоставлен анализ влияния информационных технологий на состояние преступности в Российской Федерации. В первой части проводится сопоставление статистических данных, свидетельствующих о повышении уровня преступности в информационной сфере. Опираясь на Концепцию, предоставленную Генеральной Прокуратурой Российской Федерации, производится анализ неутешительного прогнозирования, представленного в рамках данной Концепции, а также возможные пути противодействия информационной преступности. Во второй части статьи выделяется проблематика необходимости урегулирования законодательной базы, осуществляющей контроль за информационной сферой. В заключении предоставляется вывод о проделанном исследовании, а также приводятся примеры усовершенствования деятельности прокуратуры в сфере информационной безопасности.*

**Ключевые слова:** статистика, угрозы, информационные технологии, деятельности прокуратуры, тенденции развития, мошенничество, государственная поддержка, эффективные способы правового воздействия.

**Kovtun Karina Alexandrovna,**  
student, Saint Petersburg State Polytechnic University,  
Saint Petersburg, Russian Federation

**Implementation of prosecutorial supervision in the field of cybercrime  
in the information and telecommunications network of the Internet.  
Current development trends**

*The article provides an analysis of the impact of information technology on the state of crime in the Russian Federation. In the first part, a comparison of statistical data indicating an increase in the level of crime in the information sphere is carried out. Based on the Concept provided by the Prosecutor General's Office of the Russian Federation, the analysis of the disappointing forecasting presented within the framework of this Concept, as well as possible ways to counter in-*