

Научная статья
УДК 343.14

ОЦЕНКА ПРОКУРОРОМ ЦИФРОВЫХ (ЭЛЕКТРОННЫХ) ДОКАЗАТЕЛЬСТВ В ДОСУДЕБНОМ ПРОИЗВОДСТВЕ ПО УГОЛОВНЫМ ДЕЛАМ

София Игоревна СОКОЛОВСКАЯ

Санкт-Петербургский юридический институт (филиал)
Университета Прокуратуры Российской Федерации, Санкт-Петербург,
Россия
itssokolovskaya@mail.ru

Научный руководитель профессор кафедры уголовного процесса и криминалистики Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент **Елена Владимировна ЕЛАГИНА**, yelagina@bk.ru

Аннотация. В статье рассматриваются некоторые особенности оценки прокурором цифровых доказательств на досудебных стадиях уголовного судопроизводства. В частности, исследуются вопросы установления допустимости и достоверности электронных доказательств с учетом процессуального порядка получения и фиксации цифровых следов, установления первоисточника электронной информации, обеспечения ее сохранности в течение проведения всего предварительного расследования. Определены основные критерии оценки цифровых доказательств, которые имеют значение для принятия решения прокурором о направлении уголовного дела в суд.

Ключевые слова: цифровые доказательства, цифровая информация, оценка прокурором доказательств, досудебное производство

PROSECUTOR'S ASSESSMENT OF DIGITAL (ELECTRONIC) EVIDENCE IN PRE-TRIAL PROCEEDINGS IN CRIMINAL CASES

Sofia I. SOKOLOVSKAYA

St. Petersburg Law Institute (branch)
University of the Prosecutor's Office of the Russian Federation
itssokolovskaya@mail.ru

Scientific adviser — Professor of the Department of Criminal Procedure and Criminalistics of the St. Petersburg Law Institute (branch) University of the Prosecutor's Office of the Russian Federation, Candidate of Law, Associate Professor, **E. V. Elagina**, yelagina@bk.ru

Abstract. The article examines certain features of the prosecutor's assessment of digital evidence at the pretrial stages of criminal proceedings. In particular, it explores the issues of establishing the admissibility and reliability of electronic evidence, taking into account the procedural procedure for obtaining and recording digital traces, identifying the source of electronic information, and ensuring its integrity throughout the entire preliminary investigation. The main criteria for assessing digital evidence that are important for the prosecutor's decision to refer a criminal case to court are identified.

Keywords: digital evidence, digital information, prosecutor's assessment of evidence, pretrial proceedings

Закономерным этапом глобальной цифровизации общественных отношений и условием ее развития является перевод социальной коммуникации, экономических, управленческих и организационных процессов в цифровое пространство, следствием чего является активное использование информационных технологий современным человеком, в частности, для осуществления криминальной деятельности. Неслучайно в последние годы отмечается рост числа преступлений, совершенных с применением электронных устройств и информационных систем: показатели зарегистрированных киберпреступлений за 2023-2026 годы остаются высокими по сравнению с количеством деяний, совершенных с использованием информационных технологий, за тот же период прошлых лет¹. Использование преступником цифровых «инструментов» влечет отображение любых его действий на материальных объектах – электронных носителях. Это значит, что информация, которая может быть получена в ходе изучения особенностей следообразования виртуальных следов на различных стадиях совершения преступления, будет иметь в том числе и уголовно-процессуальное значение [1, с. 130]. Обоснованным представляется мнение ученых, полагающих, что «исследование современной цифровой преступности позволя-

¹Состояние преступности в Российской Федерации // Министерство внутренних дел Российской Федерации. URL: <https://мвд.рф/reports/1/> (дата обращения: 24.09.2026).

ет говорить об особом виде доказательств – цифровых доказательствах» [2, с. 27].

Действительно, в современных условиях информация, имеющая доказательственное значение в уголовном судопроизводстве, часто выражается в цифровой форме. К таким сведениям относятся, например, данные геолокации, информация о соединениях между абонентами (биллинг), логи, файлы, записи камер видеонаблюдения, переписки в информационных системах, электронные документы и иные финансовые операции. Отметим, что информационная составляющая воспроизводится и становится доступной для восприятия исключительно с помощью прикладных программно-аппаратных систем, средств вычислительной техники, а также с использованием ввода-вывода [2, с. 28].

Для признания цифровых следов допустимыми и достоверными доказательствами по уголовному делу субъекту доказывания, а равно прокурору необходимо понимать сущность цифровой информации, ее признаки, а также специфику правил обращения с электронными данными.

Определение свойств цифровой (электронной) информации, в том числе ее достоверности [3, с. 100], сводится к установлению первоначального источника происхождения такой информации. При проверке законности и обоснованности действий и решений следователя (дознателя) в отношении цифровых доказательств прокурору, в первую очередь, следует обращать внимание на процессуальный порядок проведения соответствующего следственного действия, в результате которого было получено доказательство. Универсальными критериями признания цифрового доказательства допустимым являются законность источника компьютерной информации, законность способа получения доказательства, проведение процессуального действия уполномоченным субъектом и надлежащее закрепление результатов следственного действия. По общему правилу, участие специалиста при производстве процессуального действия не требуется, за исключе-

нием случаев, прямо предусмотренных статьями 164.1-164.2 Уголовно-процессуального Кодекса Российской Федерации (далее – УПК РФ). Вместе с тем, вызов специалиста должен осуществляться на усмотрение следователя (дознателя) в соответствии с положениями статьи 58 УПК РФ. В случае наличия сомнений относительно подлинности цифровой информации, субъект доказывания назначает компьютерно-техническую экспертизу. Результаты экспертного исследования, оформленные в виде письменного заключения, так же подлежат исследованию прокурором.

Наряду с этим, процедура оценки электронных доказательств включает проверку прокурором порядка приобщения таких доказательств к материалам уголовного дела. К примеру, в протоколах осмотра предметов должны быть отражены полные сведения о свойствах объекта осмотра. Представляется точным определение критерия допустимости электронных доказательств А.А. Количенко, согласно которому под ним понимается правовое требование, определяющее соответствие полученного в ходе расследования уголовного дела электронного доказательства требованиям о надлежащем субъекте доказывания, источнике получения доказательственной информации, способе и процессуальной форме собирания доказательства, а также установления аутентичности, идентификации, верифицируемости и воспроизводимости электронной информации [3, с. 134].

В целях установления достоверности цифровых данных, в первую очередь, важно обращать внимание на обстоятельства, которые оказывают влияние на содержание электронной информации, а также учитывать, что злоумышленники в целях уничтожения следов нередко прибегают к повреждению электронного устройства, либо блокированию, модификации самой информации с помощью специальных программно-технических средств.

Субъекту доказывания требуется устанавливать ряд параметров, характеризующих конкретные цифровые сведения, то есть в работе с цифровы-

ми следами недостаточно установить факт изъятия электронного устройства и получение файла. Как справедливо замечает Н.В. Гурьева, в этом отношении значимую функцию выполняют метаданные: даже минимальный набор метаинформации позволяет точно фиксировать характеристики, техническое состояние электронного устройства или учетной записи, историю создания и изменения файла, также позволяют идентифицировать его владельца [4, с. 70]. Описание субъектом доказывания в протоколе следственного действия указанных свойств цифровой информации способно устранить сомнения прокурора относительно правдивости представленного доказательства.

Резюмируя изложенное, подчеркнем, что для признания цифрового доказательства допустимым прокурор должен оценивать правомерность действий следователя (дознавателя), а также специалиста по осуществлению технического доступа, извлечению цифровой информации, ее копированию и фиксации. Иными словами, электронное доказательство является допустимым, когда действия субъекта доказывания по получению такого доказательства соответствовали нормам УПК РФ, регламентирующим порядок проведения следственных и иных процессуальных действий. Вместе с тем, целостность электронных данных в ходе осуществления производства по уголовному делу гарантирует достоверность цифровых доказательств. Неизменность цифровой информации доказывают метаданные, которые должны быть отражены в протоколе следственного действия. Из указанного следует, что комплексный подход к оценке цифровых доказательств позволит прокурору сформировать обоснованное внутреннее убеждение относительно их допустимости и достоверности, что создает необходимые предпосылки для принятия решения о направлении материалов уголовного дела в суд и использования цифровых доказательств в судебном разбирательстве.

Список источников

1. Переверзева Е.С., Комов А.В. Механизм слеодообразования виртуальных следов // Вестник Санкт-Петербургского университета МВД России. 2022. №1 (93). С. 128-132.
2. Минаков С.С., Закляров П.В. Информационные технологии и преступления: учеб. пособие. М.: ДМК Пресс, 2023. 160 с.
3. Количенко А. А. Проблемы проверки и оценки электронных доказательств в современном уголовном процессе : дисс. ... канд. юрид. наук. / Количенко Артем Андреевич. Нижний Новгород, 2023. 224 с.
4. Гурьева Н.В. Цифровые (электронные) доказательства: значение и проблемы достоверности в уголовном судопроизводстве России // Вестник Волгоградской академии МВД России. 2026. №2 (77). С. 68-75.

Информация об авторах

С.И. СОКОЛОВСКАЯ — студент 5 курса.

Information about authors

S.I. SOKOLOVSKAYA — 5th year student.