Научная статья
УДК 343.985.5
https://doi.org/10.24412/2073-0454-2025-5-40-44
EDN: https://elibrary.ru/wvznla
NIION: 2003-0059-5/25-373
MOSURED: 77/27-003-2025-05-572

Криминалистическая классификация цифровой информации, используемой при расследовании преступления

Виталий Федорович Васюков
Московский государственный университет международных отношений МИД России (МГИМО), Москва, Россия, vvf0109@yandex.ru

Аннотация. Рассматриваются теоретические и практические аспекты классификации цифровой информации, используемой при расследовании преступлений. Отмечается, что процессы цифровизации существенно изменяют характер криминалистических объектов и требуют адаптации традиционных методик к новым видам электронных данных. Особое внимание уделено проблемам получения, фиксации и легализации цифровых сведений, возникающим в условиях трансграничности информационных потоков и высокой технологической сложности цифровых сред. Сделан вывод о необходимости формирования системной криминалистической классификации цифровой информации, учитывающей ее происхождение, функциональные характеристики и степень доступности для следственных органов.

Ключевые слова: цифровая информация, криминалистическая классификация, осмотр электронных носителей, расследование
Для цитирования: Васюков В. Ф. Криминалистическая классификация цифровой информации, используемой при расследовании преступления // Вестник Московского университета МВД России. 2025. № 5. С. 40–44. https://doi.org/10.24412/2073-0454-2025-5-40-44. EDN: WVZNLA.

Original article

Forensic classification of digital information used in crime investigation

Vitaly F. Vasyukov
Moscow State University of International Relations (MGIMO), Moscow, Russia, vvf0109@yandex.ru

Abstract. Theoretical and practical aspects of the classification of digital information used in crime investigation are considered. It is noted that digitalization processes significantly change the nature of forensic objects and require the adaptation of traditional methods to new types of electronic data. Particular attention is paid to the problems of obtaining, fixing and legalizing digital information that arise in conditions of cross-border information flows and the high technological complexity of digital environments. It was concluded that it is necessary to form a systematic forensic classification of digital information, taking into account its origin, functional characteristics and the degree of accessibility for the investigating authorities.

Keywords: digital information, forensic classification, examination of electronic media, investigation
For citation: Vasyukov V. F. Forensic classification of digital information used in crime investigation. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2025;(5):40–44. (In Russ.). https://doi.org/10.24412/2073-0454-2025-5-40-44. EDN: WVZNLA.

В любой отрасли научного знания можно обнаружить большое количество различных классификационных оснований объектов в целях решения актуальных исследовательских задач. Не является исключением и криминалистика. Объектами классификации в ней являются многие явления, связанные как с механизмом подготовки, совершения и сокрытия преступлений, так и с процессом их раскрытия, расследования и предупреждения [1, с. 106].

Между тем, современный этап развития уголовно-правовой сферы характеризуется стремительной цифровизацией, что радикально изменяет методы собирания и использования информации при расследовании преступлений. Не вызывает сомнения, что появление новых электронных средств коммуникации, хранения и обработки данных существенно расширило возможности правоохранительных органов в получении сведений о преступной деятельности.

При всем при том, криминалистическая наука претерпевает трансформацию под влиянием процессов информатизации и цифровизации, стремясь адаптировать классические теории и методики к новым объектам исследования. В этой связи особое внимание уделяется феномену цифровой информации, используемой при расследовании преступлений, — ее сущности, доказательственному значению и классификации в научно-практических целях. Как отмечает М. В. Стояновский, частные криминалистические

классификации представляют собой существенную часть криминалистической систематики и служат не только гносеологическим средством познания, но и инструментом практической деятельности, специально разрабатываемым для борьбы с преступностью [2, с. 267].

Следовательно, можно заключить, что разработка классификации цифровой информации позволяет систематизировать знания об этом сложном объекте, выявить внутренние взаимосвязи различных ее видов и выработать эффективные практические подходы к работе с ними.

Прежде всего, следует определиться с терминологией и объемом понятия. На практике и в теории используются различные понятия: говорят о «цифровых следах», «электронных следах», «виртуальных следах», «электронно-цифровых следах», «информационных следах» и т. д. [3, с. 104].

Все эти термины, по сути, обращаются к одному явлению — криминалистически значимой компьютерной (цифровой) информации о событиях или действиях, полученной и зафиксированной посредством цифровых технологий. Однако единообразие в толковании данных дефиниций пока отсутствует: разные авторы предлагают различные формулировки, акцентируя те или иные аспекты. Как видно из исследований, до настоящего времени отсутствует доминирующая позиция относительно сущности цифровых следов и единый подход к формулировке основных понятий [4, с. 5].

На наш взгляд, данное многообразие терминов отражает сложность и новизну самого феномена, а также междисциплинарный характер знаний, необходимых для его понимания. Вместе с тем, можно утверждать, что в самом общем виде цифровая информация, используемая при расследовании, — это совокупность данных в цифровой форме, которые содержат сведения о фактах, обстоятельствах, участниках и механизмах преступления. Иными словами, речь идет о данных, сохраняющихся или генерируемых в компьютерных системах, сетях связи, электронных устройствах и иных цифровых средах, способных отразить фактические обстоятельства, имеющие значение для расследуемого события.

Особенностью цифровой информации является ее нематериальная природа при одновременной физической обусловленности носителем. Цифровые данные существуют в виде бинарного кода (последовательностей электронных сигналов), не воспринимаемого непосредственно человеческими чувствами. Тем не менее, этот код фиксируется и сохраняется на материальных носителях — магнитных, оптических, полупроводниковых и иных устройствах памяти, благодаря чему информация становится доступной для последующего извлечения и исследования [5, с. 56].

В сущности, любой цифровой след представляет собой результат преобразования первичных электронных сигналов в сохраняемые данные, характеризующиеся пространственно-временными параметрами (например, время и место записи файла, привязка к устройству или аккаунту) и доступные к восприятию лишь после обратного преобразования (декодирования) техническими средствами. Необходимо подчеркнуть, что данное обстоятельство требует применения специальных знаний и технологий при обращении с электронными сведениями: чтобы обнаружить, скопировать и проанализировать цифровую информацию следователю часто необходима помощь специалистов, программные средства и криминалистическая техника. С нашей точки зрения, именно технологическая сложность работы с цифровыми данными и потребность в специальных навыках отличают цифровую информацию от традиционных видов вещественных доказательств, накладывая отпечаток на порядок ее собирания и исследования [6, с. 174].

Рассматривая цифровую информацию через призму уголовно-процессуального закона, следует отметить, что российское законодательство постепенно вырабатывает нормативные подходы к ее использованию в доказывании. Так, в УПК РФ электронные данные получили признание, прежде всего, в форме электронных документов — документов на электронных носителях информации. Согласно правовой позиции, отраженной в доктрине, электронный документ по всем основным признакам отвечает понятию документа как источника доказательств. Иными словами, если информация зафиксирована в виде файла (текстового, графического, аудиовидеофайла и т. п.), удостоверенного надлежащим образом, то такой файл в электронном виде или распечатке может выступать доказательством наравне с традиционным документом на бумажном носителе [7, с. 243].

Однако электронные документы обладают и существенной особенностью: их изготовление и использование требуют определенной технологической грамотности, соблюдения специальных правил оформления и подтверждения подлинности электронной подписью и иными средствами. Вместе с тем, на практике их применение пока носит ограниченный и осторожный характер.

Можно констатировать, что использование цифрового формата доказательств в уголовном судопроизводстве еще переживает этап становления, обусловленный необходимостью совершенствования как нормативной базы, так и технической оснащенности следственных органов.

Законодатель делает шаги в этом направлении: введена специальная ст. 164.1 УПК РФ, предусматривающая особенности изъятия электронных носителей информации и копирования с них данных. Данное нововведение призвано обеспечить баланс между потребностью изъятия цифровых сведений и сохранением функционирования компьютерных систем, из которых производится копирование. Признавая цифровую информацию частью доказательственной основы, закон требует соблюдения определенных процедур, гарантирующих достоверность и относимость этой информации.

Изучение криминалистической литературы позволило сделать вывод о том, что цифровая информация, значимая для расследования, может быть подразделена по ряду оснований.

Одним из базовых подходов является разделение информационных источников на процессуальные и непроцессуальные. Как известно, доказательственная информация приобретает юридическую силу только при условии, что она получена и закреплена в порядке, предусмотренном УПК РФ (в ходе следственных действий, по установленным правилам).

Соответственно, цифровые данные, ставшие известными правоохранительным органам, выступают либо в роли доказательств (например, электронные документы, протоколы осмотров устройств с приложенными копиями файлов, заключения компьютерных экспертиз и т. д.), либо в роли ориентирующей, оперативно-розыскной информации, которая используется для выявления и раскрытия преступления, но непосредственно доказательством не является.

Следует подчеркнуть, что многие цифровые сведения изначально поступают к следователю именно в результате проведения негласного контроля переписки в сети Интернет, данные биллинга телефонных соединений, информация из открытых источников (социальных сетей, форумов) и др.

Такая информация зачастую служит отправной точкой расследования, позволяя выдвинуть версии и нацелить следственные действия. При этом впоследствии она требует процессуального закрепления, иначе не сможет приобрести статус доказательства. В то же время, наблюдается сближение оперативных и процессуальных аспектов: законодательно закрепляются механизмы «легализации» цифровых сведений, полученных оперативным путем, чтобы они могли быть приобщены к делу (например, через институт осмотра предметов и документов, выемки электронных носителей или через получение судебных санкций на доступ к данным). В результате формируется комплексный подход, при котором цифровая информация рассматривается как единая по природе (по содержанию это фактические сведения о преступлении), но различная по процессуальному режиму использования — либо сразу вовлекаемая в доказывание, либо предварительно используемая для организации расследования [8, с. 40].

В специальной литературе применяется классификация по способу формирования цифровых данных. Здесь исходят из того, кем и как создана информация, фиксирующая следы преступления. В частности, выделяют: 1) данные, создаваемые самим пользователем электронного устройства (умышлено или в ходе обычной деятельности) и сохраняемые на его материальном носителе; 2) данные, возникающие автоматически — без непосредственного участия пользователя, генерируемые самой системой или программным обеспечением; 3) смешанный тип, когда записи формируются техническим устройством в автоматическом режиме, но в ответ на определенные действия или команды пользователя [9, с. 174].

Эта триада основана на работах исследователей, которые предложили разграничивать файлы, созданные пользователем и файлы, являющиеся результатом системной активности компьютера. Следует признать, что подобное деление имеет практический смысл: оно позволяет определить, какие следы зависят от осознанных действий подозреваемого или иного лица (например, текстовые документы, фотографии, электронные письма, сознательно сохраненные на диске), а какие возникают помимо его воли (логи системы, временные файлы, cookie-файлы, данные телекоммуникационных соединений и пр.). Отсюда вывод: при расследовании важно различать умышленные цифровые «следы-отпечатки» преступной деятельности и побочные, фоновые электронные свидетельства, оставляемые технологическими процессами. Такой подход помогает выработать тактику поиска: очевидно, что осознанно созданная преступником информация может быть попыткой сокрытия или искажения, тогда как автоматически фиксируемые данные (например, системные журналы, записи серверов) зачастую сохраняются помимо воли зло-

умышленника и могут служить объективными доказательствами [10, с. 309].

Заслуживает внимания классификация цифровой информации по ее функционально-содержательным видам. Здесь критерий деления — характер сведений, их принадлежность к определенной информационной категории внутри компьютерной системы. Так, на основании анализа структуры данных исследователи выделяют следующие группы электронных следов: системные файлы и файлы прикладного программного обеспечения; файлы-конфигурации приложений и операционных систем; журнальные файлы (логи) программных средств и аппаратуры; информационные файлы, возникающие в результате деятельности пользователя (документы, изображения, переписка и иные созданные человеком данные, включая их резервные копии и даже удаленные, подлежащие восстановлению файлы); файлы, обеспечивающие аутентификацию и безопасность (например, файлы ключей, паролей, шифрования); информация, находящаяся в оперативной памяти или файлах подкачки; и, наконец, информация, полученная посредством специальных технических средств или радиоперехвата [11, с. 22].

Можно отметить, что данная детальная классификация отражает многоуровневую структуру компьютерных данных. С одной стороны, она показывает различие между пользовательской информацией и системными метаданными, с другой, — показывает, какие именно пласты цифровой среды могут содержать доказательственные сведения. Например, помимо очевидных файлов-документов, важнейшее значение имеют логи и конфигурации, где фиксируются действия пользователя и работа устройств, а также данные оперативной памяти, которые могут хранить следы недавних операций. Таким образом, классификация по виду информации ориентирует следователя на полный охват всех возможных источников цифровых следов внутри системы — от видимых файлов до скрытых системных записей [12, с. 177].

Представляется, что цифровую информацию целесообразно классифицировать по месту нахождения и типу носителя (локализации следов). Данный критерий связан с тем, где именно обнаруживаются электронные данные, какие субъекты или устройства их содержат. По мнению ряда авторов, по местонахождению цифровые следы делятся на три основных группы: 1) сведения, находящиеся на электронных устройствах потерпевшего (например, в телефоне жертвы преступления могут остаться данные о контактах с преступником, смс-сообщения с угрозами и т. п.); 2) сведения, находящиеся на электронных устройствах самого правонарушителя (компьютеры, ноутбуки, смартфоны подозреваемых, где могут храниться планы, переписка, программы, используемые для совершения преступления и следы их работы); 3) сведения, размещенные на носителях, которые находятся у третьих лиц, прежде всего у операторов связи, интернет-сервисов или облачных хранилищ (т. е. данные, хранящиеся вне устройств непосредственных участников, например, на серверах провайдеров, в учетных записях почтовых сервисов, социальных сетей, в «облаке») [13, с. 95].

Таким образом, не вызывает сомнения, что многообразие форм и условий существования цифровой информации требует многоаспектной классификации. При этом заслуживают рассмотрения различные подходы к систематизации цифровых следов, основанные как на традиционных криминалистических критериях, так и на особенностях функционирования информационных технологий.

Список источников

1. Ким Д. В. Классификация криминалистических ситуаций как разновидность систематизации научного знания // Вестник Томского государственного университета. 2008. № 311. С. 106–112.

2. Стояновский М. В. Принципы криминалистической систематики // Воронежские криминалистические чтения. 2004. № 5. С. 265–275.

3. Перов В. А. Электронный след: понятие, виды, способы обнаружения и фиксации // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: всерос. науч.-практ. конф. М., 2021. С. 103–106.

4. Лукинский И. С. Криминалистическое содержание цифровых, информационных и информационно-коммуникационных технологий // Российский следователь. 2024. № 3. С. 2–7.

5. Бармакова Т. В., Малютина Н. М. Физические основы хранения памяти как важная составляющая современных информационных технологий // Моделирование нелинейных процессов и систем: сб. тезисов четвертой междунар. конф. М., 2019. С. 55–56.

6. Колычева А. Н. Перспективы внедрения искусственного интеллекта в раскрытие и расследование преступлений // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 3 (92). С. 172–179.

7. Морозова Н. В. Некоторые особенности расследования компьютерных преступлений // Совре-

менное уголовно-процессуальное право — уроки истории и проблемы дальнейшего реформирования: сб. мат. междунар. науч.-практ. конф. В 2 ч. Орел, 2022. С. 240–245.

8. Гомозова О. Ю., Чаплыгина В. Н. Утечка персональных данных как одна из проблем «цифровой эпохи» расследования // Уголовно-процессуальные и криминалистические проблемы борьбы с преступностью: сб. науч. ст. Орел, 2023. С. 37–44.

9. Проказин Д. Л., Семенов Е. А., Ляпин А. И. Развитие видеотехнологий в уголовном процессе России // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3 (96). С. 171–178.

10. Каширгов А. Х., Семенов Е. А. Некоторые вопросы противодействия преступлениям, совершенным с использованием IT-технологий // Евразийский юридический журнал. 2021. № 9. С. 309–310.

11. Осипенко А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4 (35). С. 20–25.

12. Преступления в сфере высоких технологий и информационной безопасности. М., 2023.

13. Противодействие криптовалютным преступлениям в зарубежных странах. М., 2025.

References

1. Kim D. V. Classification of forensic situations as a type of systematization of scientific knowledge // Bulletin of Tomsk State University. 2008. No. 311. P. 106–112.

2. Stoyanovskiy M. V. Principles of forensic systematics // Voronezh forensic readings. 2004. No. 5. P. 265–275.

3. Perov V. A. Electronic trace: concept, types, methods of detection and recording // Counteracting cybercrimes and crimes in the field of high technologies: All-Russian scientific and practical conf. M., 2021. P. 103–106.

4. Lukinsky I. S. Forensic content of digital, information and information-communication technologies // Russian investigator. 2024. No. 3. P. 2–7.

5. Barmakova T. V., Malyutina N. M. Physical foundations of memory storage as an important component of modern information technologies // Modeling of nonlinear processes and systems: collection of abstracts of the fourth int. conf. M., 2019. P. 55–56.

6. Kolycheva A. N. Prospects for the introduction of artificial intelligence in the detection and investigation of crimes // Scientific Bulletin of the Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V. V. Lukyanov. 2022. No. 3 (92). P. 172–179.

7. Morozova N. V. Some features of the investigation of computer crimes // Modern criminal procedural law — lessons of history and problems of further reform: collection of materials of the international scientific and practical conference. In 2 parts. Orel, 2022. P. 240–245.

8. Gomozova O. Yu., Chaplygina V. N. Personal data leakage as one of the problems of the «digital age» of investigation // Criminal procedural and forensic problems of the fight against crime: collection of scientific articles. Orel, 2023. P. 37–44.

9. Prokazin D. L., Semenov E. A., Lyapin A. I. Development of video technologies in criminal proceedings in Russia // Scientific Bulletin of the Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V.V. Lukyanov. 2023. No. 3 (96). P. 171–178.

10. Kashirgov A. Kh., Semenov E. A. Some issues of counteracting crimes committed with the use of IT technologies // Eurasian Law Journal. 2021. No. 9. P. 309–310.

11. Osipenko A. L. Problems of involving electronic digital traces in criminal proceedings // Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia. 2009. No. 4 (35). P. 20–25.

12. Crimes in the Sphere of High Technologies and Information Security. M., 2023.

13. Counteracting cryptocurrency crimes in foreign countries. M., 2025.

Информация об авторе

В. Ф. Васюков — профессор кафедры уголовного права, уголовного процесса и криминалистики Московского государственного университета международных отношений МИД России (МГИМО), доктор юридических наук, профессор.

Information about the author

V. F. Vasyukov — Professor of the Department of Criminal Law, Criminal Procedure and Criminalistics of the Moscow State University of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO), Doctor of Legal Sciences, Professor.

Статья поступила в редакцию 10.08.2025; одобрена после рецензирования 20.08.2025; принята к публикации 18.09.2025.
The article was submitted 10.08.2025; approved after reviewing 20.08.2025; accepted for publication 18.09.2025.