Дата поступления рукописи в редакцию: 27.02.2026 г.
Дата принятия рукописи в печать: 23.03.2026 г.
DOI: 10.24412/2224-9133-2026-2-277-282

ПОСАШКОВ Антон Сергеевич,
заместитель командира взвода
факультета подготовки дознавателей
Белгородского юридического института МВД России
имени И.Д. Путилин,
e-mail: posashkov04@internet.ru

РУДОВ Денис Николаевич,
кандидат юридических наук,
доцент заместитель начальника кафедры уголовного процесса
Белгородского юридического института МВД России
имени И.Д. Путилина,
e-mail: Den.rudov2013@yandex.ru

ПШЕНИЧНЫХ Сергей Николаевич,
научный сотрудник НИО Белгородского юридического
института МВД России имени И.Д. Путилина,
e-mail: pshenichnyx86@mail.ru

ЦИФРОВЫЕ СЛЕДЫ В ДОКАЗЫВАНИИ ПРЕСТУПЛЕНИЙ ЭКОНОМИЧЕСКОЙ НАПРАВЛЕННОСТИ

Аннотация. *В научной статье исследуются ключевые аспекты использования цифровых следов и электронных доказательств в расследовании экономических преступлений. На основе анализа статистических данных сайта МВД России (за 2025 год сотрудники органов внутренних дел выявили почти 25 000 ИТТ-преступлений в сфере экономики) обосновывается актуальность темы. Всего за январь-июль 2025 года зарегистрировано 424 900 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Практически все преступления данного вида (98,2%) выявляются органами внутренних дел РФ. Больше половины ИТТ-преступлений (51,8%) относится к категориям тяжких и особо тяжких. Примечательно, что доля тяжких и особо тяжких преступлений в сфере ИТТ-преступлений продолжает увеличиваться, что требует разработки новых подходов к собиранию доказательств.*

Основные проблемы: отсутствие единого подхода к пониманию экономических преступлений (наличие узкого и широкого подходов); соотношение терминов «компьютерная информация», «цифровой след» и «электронное доказательство»; определение основных квалификаций цифровых следов, имеющих значение для доказывания субъективной стороны преступления. Неоднозначность терминологии создает трудности в правоприменительной практике, особенно по экономическим делам.

Ключевые результаты исследования: сформирована иерархия определений; «компьютерная информация – исходное сырье», «цифровой след – криминалистически значимая информация» и «электронное доказательство – процессуальная форма оформления криминалистически значимой информации»; предложено дополнить статью 5 УПК РФ авторскими определениями пунктом 21.1 (носитель цифровых следов) и 58.1 (цифровой след) соответственно; проанализированы существующие классификации цифровых следов (по способу создания, местонахождению, степени опосредованности пользователя), в том числе классификация А.Г. Себякина (непосредственные и опосредованные следы); выявлена специфика цифровых следов в доказывании экономических преступлений.

Системный подход к пониманию природы и видов цифровых следов – необходимое условие эффективного расследования современных экономических преступлений. Предложенные определения и классификации могут стать основой для совершенствования уголовно-процессуального законодательства и практики его применения.

Ключевые слова: *цифровые следы, электронное доказательство, экономические преступления, расследование преступлений, УПК РФ, носитель цифровых следов, компьютерная информация, информационно-телекоммуникационные технологии.*

POSASHKOV Anton Sergeevich,
Deputy Platoon Commander,
Investigator Training Department Belgorod Law Institute
The Ministry of Internal Affairs of Russia
named after I.D. Putilin

RUDOV Denis Nikolaevich,
Candidate of Law, Associate Professor Deputy
Head of the Criminal Procedure Department
Belgorod Law Institute I.D. Putilin Ministry
of Internal Affairs of Russia

PSHENICHNYKH Sergey Nikolaevich,
Research Fellow, Research Institute,
Belgorod Law Institute, I.D. Putilin Ministry
of Internal Affairs of Russia

DIGITAL TRACES IN PROVIDING ECONOMIC CRIMES

Annotation. *This research article examines key aspects of using digital traces and electronic evidence in investigating economic crimes. The relevance of this topic is substantiated by an analysis of statistical data from the Russian Ministry of Internal Affairs website (in 2025, law enforcement officers identified nearly 25,000 ICT crimes in the economic sphere). A total of 424,900 crimes committed using information and telecommunications technologies or in the field of computer information were registered from January to July 2025. Almost all crimes of this type (98.2%) are detected by law enforcement agencies of the Russian Federation. More than half of ICT crimes (51.8%) are classified as serious and especially serious. It is noteworthy that the share of serious and especially serious ICT crimes continues to increase, requiring the development of new approaches to evidence collection.*

Key challenges: the lack of a unified approach to understanding economic crimes (the presence of narrow and broad approaches); The relationship between the terms "computer information," "digital trace," and "electronic evidence" is explored; the key qualifications of digital traces relevant to proving the subjective aspect of a crime are defined. The ambiguity of terminology creates difficulties in law enforcement practice, particularly in economic cases.

Key findings of the study: a hierarchy of definitions has been established: "computer information is the raw material," "digital trace is forensically significant information," and "electronic evidence is a procedural form for recording forensically significant information." A proposal has been made to supplement Article 5 of the Criminal Procedure Code of the Russian Federation with the author's definitions, including paragraphs 21.1 (digital trace carrier) and 58.1 (digital trace), respectively. Existing classifications of digital traces (by method of creation, location, and degree of user indirection) are analyzed, including A.G. Sebyakin's classification (direct and indirect traces). The specific nature of digital traces in proving economic crimes is identified.

A systematic approach to understanding the nature and types of digital traces is essential for the effective investigation of modern economic crimes. The proposed definitions and classifications can serve as a basis for improving criminal procedure legislation and its application.

Key words: *digital traces, electronic evidence, economic crimes, crime investigation, Criminal Procedure Code of the Russian Federation (CPC RF), digital trace carrier, computer information, information and telecommunication technologies (ICT).*

Руководствуясь статистическими данными МВД России, ущерб от ИТТ-преступлений в 2025 году за семь месяцев увеличился на 16 % - с 100,5 млрд рублей до 119,6 млрд рублей. Всего за январь-июль 2025 года зарегистрировано 424 900 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Практически все преступления данного вида (98,2%) выявляются органами внутренних дел РФ. Больше половины ИТТ-преступлений (51,8%) относится к категориям тяжких и особо тяжких.

В юридической науке отсутствует единое определение составов преступлений, которое можно отнести к экономической направленности.

Ученые выделяют два подхода к понимаю данного термина: узкий (Бойцов А.И., Ларченко В.Д.) – только преступления главы 22 УК РФ, широки (Колесников В.В., Немытина М.В.) – весь раздел 8 УК РФ.

Ведомственная классификация определяется Указанием Генпрокуратуры №35/11, МВД России №1 от 24.01.2020 [2]. В соответствии с ним выделяется три группы преступлений экономической направленности:

1) Безусловные составы (ст. 145.1,146,147 и др.)
2) Преступления с дополнительными условиями (ч. 3 ст. 158, ч.2 ст. 159 и др.)
3) Налоговые преступления (ст. 198-199.4 и др.)

Наше мнение склоняется к признанию широкого подхода, так как он охватывает все экономические отношения. Ключевые признаки данного вида преступлений: специальный субъект, использование законных экономических инструментов, крупный ущерб, угроза экономической безопасности.

Для большего понимания значения понятий «цифровые следы» и «электронное доказательство» нам нужно изучить, в какой взаимосвязи находятся данные понятия. Соотношение «компьютерная информация» с вышеупомянутыми терминами, а также смысловое и процессуальное содержание каждого из них. Их корректное и смысловое разграничение имеет неоценимое значение для правоприменительной практики правоохранительных органов.

Понятие «компьютерная информация» является исходным, наиболее широким, которое лежит в основе всех остальных. Компьютерная информация – совокупность данных, сведений, представленных в форме, пригодной для автоматической обработки компьютерными средствами. Данное определение является самостоятельным и находит свое отражение в статье 272 УК РФ (под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи). Сама информация в данном виде представляет собой массив данных, а её правовой статус представляет собой «сырье», потенциальный носитель следов и информации, имеющей значение для дела (объем данных на жестком диске, сообщения на электронной почте и в мессенджерах, логфайл сервера за определенный период).

Само понятие «цифровой след» является следующей ступенью конкретизации. Цифровой след – это криминалистически значимая информация, зафиксированная в электронной форме и отражающая факты совершения экономических операций, действий пользователей в информационных системах, процессы обработки, хранения и передачи данных.

Приговор №1-180/2025 от 28 апреля 2025 г. по делу № 1-180/2025 Тосненским городским судом Ленинградской области в отношении ФИО1, обвиняемого в совершении преступлений предусмотренных ч. 3 ст. 160 УК РФ, ч. 1 ст. 160 УК РФ. Ярким примером использования цифрового следа является изъятый цифровой носитель – DVD-диск с записями камер видеонаблюдения, который в установленном законом порядке был осмотрен и признан вещественным доказательством, протокол осмотра предмета был приобщен к материалам уголовного дела.

Е.Р. Россинская и И.А. Рядовский определяют цифровой след как криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде в процессе ее возникновения, обработки, хранения и передачи [1]. Данное понятие использует узкое определение «компьютерной информации», но имеет указание на процессуальный аспект.

А.В. Ростовцев рассматривает цифровой след как значимую информацию, оставленную в виртуальном пространстве и на электронно-цифровых устройствах, которая представлена в форме электрических сигналов и обнаружена с помощью программно-технических устройств [2]. Точным является акцент на выраженность посредством сигналов, но привязка к виртуальномупространству чрезмерно сужает данное определение.

Согласно позиции А. М.Багмета, цифровой (виртуальный) след –любая криминалистически значимая компьютерная информация, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[3]. Вводится в определение динамический аспект (электрические сигналы), но акцент сводится к криминалистической значимости, что может сужать применение понятия в других правовых сферах.

По мнению А.А. Бессонова цифровые следы – информация, содержащаяся в электронно-вычислительных машинах и иных цифровых устройствах, а также в средствах подвижной радиотелефонной связи и на различных носителях цифровой информации, зафиксированная в цифровом формате. Данное определение отличается современностью и широтой охвата, правильно перечисляя источники и носители, но не объясняет причину криминалистической значимости [4].

Электронное доказательство представляет собой процессуальную форму, в которую в кото-

рую верифицируется цифровой след и разновидность иных документов или вещественных доказательств, закрепленных на материальном носителе. По намешу мнению электронное доказательство – это цифровой след, который прошел процедуру легализации в рамках уголовного процесса, гарантирующую его неизменность и достоверность.

В рамках расследования дел в сфере экономики наиболее распространены следующие виды цифровых следов: электронные бухгалтерские и финансовые документы (файлы баз данных систем автоматизированного учета, 1Cv8/KDN в 1С:Бухгалтерия); данные о цифровых финансовых активах (переводы через криптовалютные кошельки, международные переводы и транзакции); данные интернет-ресурсов (скриншоты переписок, информация о регистрации домена, информация с сайтов в файлах); сведения из социальных сетей и мессенджеров (история переписок, контакты в мессенджерах, аккаунты в социальных сетях); информация с устройств фиксации (запись видеорегистраторов, камер наблюдения, диктофонов); метаданные файлов (время создания, изменения, авторство), журналы событий и систем (история, фиксирующая действия пользователей).

Приговор № 1-11/2024, 1-29/2023, 1-300/2022, 1-8/2025, от 10 апреля 2025 г. по делу № 1-11/2024по ч. 4 статьи 159 УК РФ, где доказательством послужил протокол осмотра и фототаблицы, содержащие данные базы С1 (компания с запросом на коммерческое предложение о покупке светильников не обращалась, но денежные средства на освещение участка дорожного полотна на счет ООО «Стройпремьер» поступили в размере 4 819 274,10 по гос. контракту).

Знание классификации цифровых следов – это не теория, а необходимость для сотрудников органа предварительного расследования и оперативных подразделений. Она позволяет выстраивать эффективную и экономную по временным показателям методику расследования, грамотно проводить и планировать следственные действия, не допускать роковых ошибок при обыске, изъятии предметов и выемке, обеспечивать допустимость доказательств, полученных при помощи осмотра цифровых следов, воссоздать полную картину и последовательность совершения преступного деяния.

Способы классификации цифровых следов, наиболее релевантные для практики расследования и раскрытия преступлений:

1) По способу создания:

– файлы, которые пользователь создал самостоятельно и намеренно сохранил на устройстве (файлы docx, xlsx, zip);
– файлы, сформированные автоматически операционной системой или приложениями без прямого участия человека (журналы событий, файлы кэша, файлы точек восстановления системы);
– файлы, содержимое которых генерируется устройством на основе заданных пользователем команд или сценариев (VBA-скрипт, . MDB, .bat, .ps1).

2) По местонахождению цифровых следов [5]:

– на электронных устройствах потерпевшего или свидетеля;
– на электронных устройствах подозреваемого;
– на оборудовании операторов связи и иных промежуточных серверах.

3) При совершении мошенничества с использованием средств сотовой связи:

4. Цифровые следы, возникающие в мобильных средствах телекоммуникации:
– сведения об оборудовании и абонентах;
– пространственно-временные данные;
– метаданные мультимедийного контента;
– специализированные приложения и программы.
5. Цифровые следы, связанные с использованием банковской карты или счета;
6. Аудиофонограммы.
7. Цифровые следы, связанные с подготовкой, совершением и сокрытием преступного деяния, находящиеся на электронном устройстве преступника.

Классификация предложенная к.ю.н. А.Г. Себякиным в своей диссертации, является одной из фундаментальных и практически полезных, так как основана она на критически важном для расследования критерии – степени опосредованности воздействия пользователя на компьютерную систему.

Классификация цифровых следов по А.Г. Себякину[6]:

1. Непосредственные следы возникают в результате прямого воздействия на компьютерную систему (переписка, публикации, сознательно размещенный продолжительное время определенный вид контента, ряд однотипных транзакций и другое.)
2. Опосредованные следы образуются без прямого участия пользователя, но инициируются его действиями (метаданные, ip-адреса, данные о местоположении, факт перехода по рекламной ссылке, журналы системных событий, файлы cookie и другое).

Таким образом, непосредственные следы прямо свидетельствуют о намерениях, мыслях и

действиях человека. Они являются прямым источником информации о намеренных действиях (переписка о планировании преступления).

Опосредованные следы зачастую служат косвенной информацией, которая подтверждает факт нахождения устройства в определенном месте в определенное время или совершения им конкретных действий, даже если пользователь противодействовал расследованию преступления и пытался скрыть имеющуюся на носителе информацию.

Таким образом, классификация Себякина А.Г. не просто является теоретической квалификацией цифровых следов, а предоставляет следователю методическую разработку и четкий инструмент для оценки, систематизации и использования цифровых следов для собирания доказательств и доказывания субъективной стороны преступления.

На основе проведенного исследования можно сделать вывод:

1) Сформирована четкая терминологическая иерархия. Ключевые понятия «компьютерная информация», «цифровой след» и «электронное доказательство» соотносятся как последовательные стадии преобразования информации в доказательство. «Компьютерная информация» является исходным сырьем, «цифровой след» криминалистически значимой частью информации, а «электронное доказательство» - её процессуально оформленной формой, пригодной для использования в суде.
2) Предложено легальное определение. В целях унификации правоприменительной практики обоснована необходимость закрепления в статье 5 УПК РФ легальных дефиниций «цифровой след» и «носитель цифровых следов», что позволит четко регламентировать действия следствия и исключит разночтения.
3) Классификации носят практико-ориентированный характер.Рассмотренные классификации (по способу создания, местонахождению, степени осознанности) не являются абстрактными, а служат конкретным целям:

– помогают выстроить эффективную стратегию расследования, определяя приоритеты в изъятии и исследовании следов (например, сначала зафиксировать неустойчивые пассивные следы).
– позволяют грамотно планировать следственные действия (обыск, выемку) и определять круг источников доказательств.
– способствуют правильной оценке доказательственного значения: непосредственные следы прямо свидетельствуют о намерениях лица, а опосредованные подтверждают обстоятельства дела.

4) Выявлена специфика следов в экономических преступлениях. Для данной категории дел наиболее релевантны цифровые следы из систем бухгалтерского учета, данные о финансовых транзакциях (включая криптовалютные), метаданные документов и переписка в мессенджерах, что требует от следователя узкоспециализированных знаний и компетенций.

Таким образом, системный подход к пониманию природы, видов и процессуального оформления цифровых следов является необходимым условием для успешного расследования и раскрытия современных экономических преступлений.

На основании изученных определений, мы предлагаем дополнить статью 5 УПК РФ пунктом 21.1 (носитель цифровых следов) и 58.1 (цифровой след) соответственно:

– цифровой след – криминалистически значимая информация о событии или действии, зафиксированная в цифровой форме на материальном носителе либо в информационно-телекоммуникационной сети «Интернет» в результате функционирования цифрового устройства, системы или сети;
– носитель цифровых следов – материальный объект, на котором информация, составляющая цифровой след, находит свое отображение в виде электрических, магнитных, электромагнитных, оптических или иных физических полей и сигналов (жесткие диски, микросхемы памяти, сервера и т.д.).

Список литературы:

[1] Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков.Теория информационно компьютерного обеспечения криминалистической деятельности //Проспект. 2023. - 352 с.

[2] Ростовцев А. В. Особенности судебно экспертного исследования цифровых следов // Вестник криминалистики. 2019. № 2 (70). С. 67–72.

[3] Багмет А. М., Бычков В. В., Скобелин С. Ю., Ильин Н. Н. Цифровые следы преступлений: монография / Проспект, 2021. - 168 с.

[4] Бессонов А. А. Цифровые следы как объекты криминалистического исследования : монография / А. А. Бессонов. — Москва :Юрлитинформ, 2019. — 240 с

[5] Колычева, А. Н. Фиксация доказательственной информации, хранящейся на ресурсах сети Интернет :дис. ... канд. юрид. наук : 12.00.12 / А. Н. Колычева. — М., 2019. — 200 с.

[6] Себякин, А. Г. Тактика использования знаний в области компьютерной техники в целях получения криминалистически значимой информации :дис. … канд. юрид. наук : 12.00.12 / А. Г. Себякин ; Моск. гос. юрид. ун т им. О. Е. Кутафина (МГЮА). — Москва, 2021. — 234 с.

References:

[1] E. R. Rossinskaya, A. I. Semikalenova, I. A. Ryadovsky, T. A. Saakov. Theory of information computer support of forensic activities//Prospect. 2023. - 352 s.

[2] Rostovtsev A. V. Features of forensic research of digital traces//Bulletin of Criminalistics. 2019. № 2 (70). S. 67-72.

[3] Bagmet A.M., Bychkov V.V., Skobelin S. Yu., Ilyin N. N. Digital traces of crimes: monograph/Prospect, 2021. - 168 s.

[4] Bessonov A. A. Digital traces as objects of forensic research: monograph/A. A. Bessonov. - Moscow: Yurlitinform, 2019. - 240 s

[5] Kolycheva, A. N. Recording of evidentiary information stored on the Internet resources: dis.... cand. jurid. Sciences: 12.00.12/A. N. Kolycheva. - M., 2019. - 200 s.

[6] Sebyakin, A. G. Tactics of using knowledge in the field of computer technology in order to obtain criminally significant information: dis.... cand. jurid. Sciences: 12.00.12/A. G. Sebyakin; Mosk. state. jurid. un t them. O. E. Kutafina (Moscow State Law Academy). - Moscow, 2021. - 234 s.

