Научная статья
УДК: 343. 973:004

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ЦИФРОВЫХ СЛЕДОВ ПРИ ВЫЯВЛЕНИИ И РАСКРЫТИИ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ

Татьяна Евгениевна Крысина
Орловский юридический институт МВД России имени В. В. Лукьянова, г. Орел, Российская Федерация, 02@mail.ru

Аннотация. Бурное развитие цифровых технологий и их глубокое воздействие на разные аспекты общества сопровождается заметным увеличением числа преступлений, в которых используются новейшие технические устройства. Современные вызовы требуют создания новых методик и рекомендаций, используемых для анализа и толкования цифровых следов, возникающих в виртуальной среде в процессе совершения кредитно-финансовых преступлений. Главным направлением исследований становится изучение следов киберпреступлений, связанных с финансовыми рынками. В статье сформирован подход к пониманию виртуального пространства, используемого при совершении преступлений; рассмотрено понятие «цифровые следы» и их классификация. Кроме того, уделяется внимание исследованию оперативно-значимой информации при изучении теневого сегмента сети «Интернет». В работе рассматриваются методы применения технологии «Больших данных» в рамках обеспечения эффективности оперативно-розыскной деятельности.

Ключевые слова: виртуальное пространство, цифровые следы, «Большие данные», оперативно-розыскная деятельность, оперативно-розыскные мероприятия.

Для цитирования: Крысина, Т. Е. К вопросу об использовании цифровых следов при выявлении и раскрытии экономических преступлений // Криминалистика: вчера, сегодня, завтра. 2026. Т. 38. № 2. С. 86–94.

ON THE QUESTION OF USING DIGITAL TRACES IN THE DETECTION AND DISCLOSURE OF ECONOMIC CRIMES

Tatyana E. Krysina
Oryol Law Institute of the MIA of Russia named after V. V. Lukyanov, Oryol, Russian Federation**,** tatyana.krysina.02@mail.ru

Abstract. The rapid development of digital technologies and their profound impact on various aspects of society is accompanied by a significant increase in the number of crimes involving the latest technological devices. Modern challenges require the development of new methods and recommendations for the analysis and interpretation of digital traces arising in the virtual environment during credit and financial crimes. The main focus of this

research is the study of traces of cybercrimes related to financial markets. This article develops an approach to understanding the virtual space used in crimes and examines the concept of "digital traces" and their classification. Furthermore, attention is paid to the study of operationally significant information when investigating the shadow segment of the Internet. The paper examines methods for applying Big Data technology to ensure the effectiveness of operational investigative activities.

Keywords: virtual space, digital traces, Big Data, operational investigative activities, operational investigative measures.

For citation: Krysina T. E. K voprosu ob ispol'zovanii cifrovyh sledov pri vyyavlenii i raskrytii ekonomicheskih prestuplenij [Article title Article title Article title (On the use of digital traces in identifying and solving economic crimes)]. Kriminalistika: vchera, segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2026, vol. 38 no. 2, pp. 86–94 (in Russ.).

Введение

Уроки прошлого заставляют нас обратить внимание на то, что преступная деятельность обладает неуклонной тенденцией к развитию и трансформации, проявляя способность приобретать все более изощренные и сложные формы. Вследствие этого эволюционного процесса формируется преступный механизм, способный привлекать квалифицированных специалистов, обладающих необходимыми интеллектуальными ресурсами, для совершения противоправных деяний, в частности в области кредитно-финансовых отношений.

В современных условиях рост преступной деятельности в области высоких технологий и цифрового пространства приобретает все более тревожные масштабы. На заседании коллегии МВД президент Российской Федерации Владимир Владимирович Путин подчеркнул, что около четверти всех жертв киберпреступлений в 2024 году составили пенсионеры. Общий материальный ущерб, причиненный киберпреступлениями за указанный период, оценивается приблизительно в 200 миллиардов рублей. Вместе с тем глава государства обратил внимание на снижение уровня раскрываемости подобных преступлений, который за 2024 год составил порядка 23 %. В этой связи президент подчеркнул необходимость активного и адекватного реагирования со стороны МВД на новые методы и возможности, используемые злоумышленниками для совершения преступлений в киберпространстве [1].

Таким образом, с момента возникновения первых научных изысканий, посвященных проблематике совершения преступных деяний в виртуальном пространстве, было очевидно, что криминальная деятельность в сфере кредитно-финансовых отношений претерпевает колоссальные изменения в процессе формирования доказательственной базы. Преступления, совершенные в кредитно-финансовой сфере с использованием информационных технологий, оставляют за собой особую категорию следов, отличающуюся от привычных материальных и идеальных. Таким образом, цифровые следы выступают как самостоятельный и уникальный элемент в процессе осуществления деятельности по выявлению и раскрытию рассматриваемой категории экономических преступлений.

Основная часть

В последние годы с развитием IT-технологий в сфере преступлений стал появляться новый вид данных – так называемый «цифровой след». Сегодня в юридической практике существует множество трактовок этого понятия, которые акцентируют внимание на его происхождении и ключевых свойствах. Примечательно, что первые попытки официального закрепления термина в российском праве датируются 2020 годом. В частности, в этот период был опубликован в интернете проект нормативного акта под названием «Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики». В данном законопроекте термин «цифровые следы» обозначает данные, которые человек сознательно размещает в различных информационных платформах [2, с.1].

Информация, которую человек сознательно публикует в Интернете, формирует так называемые цифровые следы. Это могут быть личные фотографии, заполненные анкеты или комментарии в социальных сетях, размещённые на различных серверах виртуального пространства. Таким образом, цифровые следы отражают активность пользователя в информационно-коммуникационной среде. Сотрудники оперативных подразделений должны владеть навыками классификации цифровых данных, выявляемых в ходе раскрытия финансово-кредитных преступлений, разделяя их на две категории: ключевые и вспомогательные. Ключевые данные представляют особую значимость для человека, поскольку обычно создаются им сознательно и непосредственно. Примерами таких материалов служат тексты электронных писем и сопровождающие их вложения (фотографии, видео- и аудиосообщения). Вспомогательная категория данных включает в себя метаданные, которые формируются автоматически, без прямого вовлечения человека [3, с.1]. Например, сведения о времени звонков и отправки сообщений, а также информация о номерах телефонов и IP-адреса устройств, используемых в сети, постоянно фиксируются и могут передаваться третьим лицам.

Стоит отметить, что подразделения экономической безопасности и противодействия коррупции (далее – ЭБ и ПК), входящие в состав Министерства внутренних дел Российской Федерации, выполняют ключевую функцию в противоборстве с преступлениями, связанными с финансовой сферой и кредитованием. Для эффективного выявления и раскрытия преступлений в кредитно-финансовой сфере, а конкретно – незаконного обналичивания и транзита денежных средств, крайне важно чётко определить понятие цифровых следов и выделить их основные характеристики. Проведение анализа и выработка однозначного понимания данного термина с учётом особенностей этих преступлений является необходимым условием для осуществления эффективной борьбы сотрудников ЭБ и ПК с кредитно-финансовыми преступлениями. В рамках оперативно-розыскной деятельности (далее – ОРД) под цифровыми следами понимаются данные, хранящиеся на электронных устройствах и обладающие важностью для успешного проведения оперативно-розыскных мероприятий (далее – ОРМ). Эти сведения служат ключевым источником информации, применяемой для выявления и раскрытия преступлений в сфере кредитно-финансовых операций. Как правило, такие цифровые следы оставляют преступники во время подготовки и совершения преступлений, связан-

ных с финансовыми махинациями. К примеру, это может проявляться в виде дистанционного перевода денежных средств с банковского счета на счет фирмы-однодневки, учрежденной лишь для кратковременной хозяйственной деятельности без намерения продолжать работу в будущем.

В сфере преступлений, затрагивающих кредитно-финансовую деятельность, цифровые следы требуют тщательного упорядочивания по различным характеристикам. Одним из ключевых инструментов для выявления и раскрытия преступных операций, связанных с незаконным обналичиванием и транзитом денег, является грамотно выстроенная классификация этих цифровых следов. Рассмотрим наиболее значимые подходы к систематизации цифровых следов, которые способствуют эффективному противодействию финансовым преступлениям.

В качестве ключевого признака цифровых следов следует рассматривать порядок обеспечения доступа к ним с целью их документального закрепления и последующего изъятия. В рамках систематизации цифровых следов А. В. Отогочев предлагает классификацию по трем критериям. Первый критерий основан на характере получения доступа к цифровым следам в целях их фиксации и изъятия. Применительно к сфере кредитно-финансовых преступлений данная классификация приобретает особую значимость и предусматривает следующую дифференциацию цифровых следов:

– доступные неограниченному кругу лиц – цифровые следы, доступ к которым не ограничен юридическими, техническими или иными барьерами (например, данные в открытых реестрах, публикации в социальных сетях с публичным доступом, официальные отчеты финансовых организаций);

– доступные уполномоченным лицам в пределах предоставленных законом полномочий – цифровые следы, доступ к которым строго регламентирован и возможен исключительно для определенных субъектов при соблюдении установленных процедур (банковские выписки, внутренняя документация финансовых учреждений, логи защищенных систем и т.д.) [4, с.4].

Такая классификация отражает специфику финансового рынка, где значительная часть данных защищена законодательством о банковской, коммерческой и служебной тайне, и позволяет оптимизировать процесс сбора доказательств в ходе расследования.

Таким образом, стоит отметить, что недостаток законных оснований и полномочий для изъятия цифровых следов, охраняемых законодательством РФ, существенно затрудняет выявление и пресечение преступлений на финансовом рынке. Это обусловлено действующими правовыми ограничениями, регламентирующими доступ к подобным данным и исключающими их изъятие без соблюдения установленных процедур. В деятельности подразделений ЭБ и ПК данная проблема выступает ключевым барьером при выявлении и раскрытии преступлений в сфере кредитно-финансовых отношений.

Рассматривая первый критерий классификации, можно отметить, что цифровые следы доступны неограниченному кругу лиц в любое время. К таким данным относятся сведения, открытые для публичного доступа, которые содержат важную оперативную информацию о лицах, участвующих в совершении кредитно-финансовых преступлений, либо о самих событиях, связанных с этими правонарушениями. В российском

правовом поле, регулирующем информационные технологии и защиту данных[1], под общедоступной информацией понимаются сведения, которые являются широко распространенными и доступными для каждого без ограничений. К тому же, к этой группе относятся данные, которые их законные владельцы публикуют в Интернете в формате, позволяющем автоматизированную обработку без необходимости ручного редактирования, и предназначенные для многократного применения.

К общедоступным данным, которые могут способствовать эффективному выявлению и раскрытию кредитно-финансовых преступлений на финансовом рынке, предлагаем отнести следующие:

– информация, получаемая из открытых официальных реестров (например: реестр поднадзорных Банку России финансовых организаций, список компаний с выявленными признаками нелегальной деятельности на финансовом рынке [5], единые государственные реестры юридических лиц, индивидуальных предпринимателей и т. п.);

– информация, находящаяся в открытом доступе и связанная с коммерческой деятельностью (например: сведения о предприятиях, эмитентах ценных бумаг, а также данные о результатах торгов на бирже. Кроме того, к таким источникам относятся специализированные финансовые новостные порталы и другие ресурсы, посвящённые рынкам капитала);

– публичные коммерческие данные (например: информация о компании, эмитенте ценных бумаг, результаты биржевых торгов, сайты информационных агентств, специализирующихся в сфере финансовых рынков, и др.);

– материалы средств массовой информации (например: статьи, интервью и др.);

– информация с веб-сайтов (например: документы, фотографии, видео- и аудиофайлы и др.), в том числе с их сохраненных копий;

– социальные сети (например: учетные записи пользователей от социальных сетей; визуальные материалы (фотографии и видеозаписи); сведения о местонахождении (город, регион); идентификационные данные лиц (имена или никнеймы лиц); контактные номера абонентов; IP-адрес).

В контексте сказанного необходимо обратить внимание на мнения Ю. В. Гаврилина и А. В. Шмонина, которые считают, что в современных условиях развития общества социальные сети содержат большое количество оперативно значимой информации. Прежде всего, это контент, который пользователи сами размещают на своей страничке в социальной сети. Сотрудниками оперативных подразделений при проведении тщательного анализа содержимого информационных ресурсов предоставляется возможность выявить социальные связи интересующего лица, его профессиональную деятельность, хобби, а также образ жизни в целом. Стоит отметить, что данный процесс способствует установлению вероятного уровня дохода, определению географических перемещений, статуса в семейном положении, состава домохозяйства и даже используемых транспортных средств. Таким образом, с помощью систематического изучения цифровых следов, оставляемых личностью в социальной сети, сотрудниками оперативных подразделений формируется всесторонняя характеристика пользователя [6, с. 105–111].

[1] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

Другой вид цифровых следов является доступным только уполномоченным лицам в пределах полномочий, предоставленных законодательством Российской Федерации. Следовательно, от уровня доступа к ограниченным сведениям, содержащим цифровые следы, пропорционально зависит и эффективность раскрытия преступления. Для категории преступлений в сфере кредитно-финансового рынка оперативные сотрудники для получения оперативно-значимой информации зачастую проводят следующие ОРМ: наведение справок, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях; исследование предметов и документов; обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.

Одним из способов получения оперативными сотрудниками ЭБ и ПК оперативно-значимой информации о совершении незаконных финансовых операций посредством цифровых следов выступает отслеживание криптовалютных транзакций. Стоит отметить, что в современном обществе наблюдается устойчивая тенденция использования криптовалют в противоправных целях. В усложненной динамике мировых взаимоотношений наблюдается усугубление обстоятельств, связанных с незаконными операциями по обналичиванию и транзитированию как традиционных денежных средств, так и их цифровых аналогов. Преступники предпочитают обращаться к централизованным биржам для проведения операций по легализации средств ввиду их высокой ликвидности и простоты превращения цифровых активов в обычные деньги, а также интеграции с традиционными финансовыми сервисами, способствующими перемешиванию незаконно нажитых средств с легальной деятельностью [7, с. 3]. Согласно отчету Банка России, за первое полугодие 2024 года, 59 % выявленных субъектов, демонстрирующих признаки финансовых пирамид, осуществляли привлечение клиентских средств именно в цифровых валютах. Указанные финансовые инструменты обеспечивают злоумышленникам возможность сохранять анонимность, что в свою очередь значительно затрудняет деятельность оперативных сотрудников по выявлению и раскрытию рассматриваемой категории преступлений [8].

В рамках ОРД оправдано применение всех предусмотренных законом гласных и негласных методов поиска и сбора оперативно-значимой информации, включая использование данных, доступных в общественном пространстве сети Интернет. Установление сведений об интересующем лице представляет собой задачу особой сложности, решение которой требует, с одной стороны, применения специализированных поисковых средств, а с другой – значительного временного ресурса.

В рамках использования оперативными сотрудниками концепции «Больших данных» в деятельности по раскрытию кредитно-финансовых преступлений требуется внедрение инновационных статистических методов и современных информационных технологий, что трансформирует традиционные подходы к поиску и обработке информации. В отличие от классических процедур, где данные подвергаются предварительному исследованию и обработке, здесь анализ проводится непосредственно на исходных наборах данных в их первоначальном виде. Процесс выявления взаимосвязей между элементами данных носит интерактивный характер и охватывает полный объем доступной информации до достижения заданных критериев результата.

Данная методология обеспечивает возможность выполнения анализа в режиме реального времени, позволяя обрабатывать информацию по мере ее поступления без существенных задержек [9, с. 3].

«Большие данные» содержат особенности, которые подчиняются требованиям к информационной модели, характерной для ОРД:

– значительный физический объем данных, превышающий возможности его обработки обычными программными средствами за разумное время;

– данные постоянно обновляются, что предполагает их постоянную обработку;

– разнообразные данные, как правило, разнородны, неструктурированы или структурированы не полностью.

Таким образом, для ОРД представляет интерес анализ разнородных баз данных для получения и последующего использования выявленных закономерностей, которые подтверждают или опровергают версию совершения лицом кредитно-финансового преступления. В данном контексте следует отметить, что наиболее целесообразным принято считать получение информации оперативным путем посредством проведения комплекса гласных и негласных ОРМ.

Выводы и заключение

Результаты проведенного исследования однозначно демонстрируют важность применения цифровых следов в интересах ОРД при выявлении, предупреждении, пресечении и раскрытии преступлений в сфере финансов и кредитования. В процессе анализа необходимо выделить основные выводы, представляющие особую ценность для совершенствования практики ОРД:

– цифровые следы в ОРД – это информация, сохранённая на электронных устройствах, которая имеет существенное значение для выявления и раскрытия экономических преступлений. Такие данные составляют ключевую часть информационной базы, используемой при подготовке и реализации комплекса негласных ОРМ. Изучение цифровых следов помогает сотрудникам подразделений ЭБ и ПК своевременно выявлять и раскрывать преступления, связанные с кредитно-финансовой сферой;

– рассмотрена наиболее популярная классификация цифровых следов, которую принято разделять на две категории: доступные неограниченному числу субъектов и предоставляемые исключительно уполномоченным лицам в рамках установленных законодательством полномочий;

– в целях повышения эффективности выявления и раскрытия преступлений в сфере кредитно-финансовой деятельности оперативные подразделения вынуждены интегрировать передовые информационные технологии и прогрессивные методы статистического анализа. Предложенное нововведение способствует глубокой трансформации устоявшихся алгоритмов сбора и обработки данных, что значительно расширяет возможности по использованию концепции «Больших данных» в правоохранительной практике.

СПИСОК ИСТОЧНИКОВ

1. Официальный сайт: Пятый канал – Главные новости России и мира сегодня. URL: https://www.5-tv.ru/news/5017405/putin-userbotkiberpresuplen-ijv2024m-sostavil-okolo-200-milliardov-rublej/ (дата обращения 09.12.2025).

2. Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики // Подготовлена некоммерческой организацией «Фонд развития центра разработки и коммерциализации новых технологий» на основе отчета Федерального Государственного научно-исследовательского учреждения «Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации». URL: file:///C:/Users/admin/Downloads/10.06.2020_КНПР_доработанная_после_РГ.pdf (дата обращения: 09.12.2025);

3. *Карпика, А. Г.* Актуальные вопросы поиска и анализа цифровых следов в оперативно-розыскной деятельности // ЮП. 2019. №3 (90). URL: https://cyberleninka.ru/article/n/aktualnye-voprosy-poiska-i-analizatsifrovyhsle-dovvoperativno-rozysknoy-deyatelnosti (дата обращения: 09.12.2025);

4. *Отогочев, А. В.* Виды цифровых следов преступлений на финансовом рынке // Актуальные проблемы российского права. 2025. №2 (171). URL: https://cyberleninka.ru/article/n/vidy-tsifrovyh-sledov-prestupleniy-na-finansovom-rynke (дата обращения: 09.12.2025);

5. Банк России раскрывает список компаний с выявленными признаками «финансовой пирамиды», нелегального кредитора, нелегального профессионального участника рынка ценных бумаг (в том числе нелегального форекс-дилера) и иных нелегальных участников финансового рынка (URL: https://cbr.ru/ inside/warning-list/ (дата обращения: 09.12.2025));

6. *Гаврилин, Ю. В., Шмонин, А. В*. Использование информации, полученной из сети Интернет, в расследовании преступлений экстремистской направленности // Труды Академии управления МВД России. 2019. № 1 (49);

7. *Васюков, В. Ф., Старжинская, А. Н.* Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют // Российское право: образование, практика, наука. 2024. № 4. С. 68–78. DOI: 10.34076/2410-2709-2024- 142-4-68-78;

8. Банк России выявил в первом полугодии 2024 года почти 3,5 тысячи нелегалов // URL: https://cbr.ru/ press/event/?id=18871/ (дата обращения: 09.12.2025);

9. *Батраченко, Д. А., Васюков, В. Ф*. Некоторые вопросы получения оперативно значимой и криминалистической информации из облачных хранилищ // юридическая наука и практика: Вестник Нижегородской Академии МВД России. 2025. Т. 1 № 69

REFERENCER

1. Official website: Channel Five - The main news of Russia and the world today. URL: https://www.5-tv.ru/news/5017405/putin-userbotkiberpresuplen-ijv2024m-sostavil-okolo-200-milliardov-rublej/ (дата обращения 09.12.2025).

2. The concept of comprehensive regulation (legal regulation) of relations arising in connection with the development of the digital economy//Prepared by the non-profit organization "Fund for the Development of the Center for the Development and

Commercialization of New Technologies" based on the report of the Federal State Research Institution "Institute of Legislation and Comparative Law under the Government of the Russian Federation." URL: file :///C :/Users/admin/Downloads/ 10.06.2020 _ KNPR _ revised _ after _ WGpdf (accessed: 09.12.2025).

3. Karpika, A. G. Aktual'nyye voprosy poiska i analiza tsifrovykh sledov v operativno-rozysknoy deyatel'nosti [Topical issues of search and analysis of digital traces in operational-search activities]. UP. 2019. №3 (90). URL: https://cyberleninka.ru/article/n/aktualnye-voprosy-poiska-i-analizatsifrovyhsle-dovvoperativno-rozysknoy-deyatelnosti (дата обращения: 09.12.2025).

4. Otogochev, A. V. Vidy tsifrovykh sledov prestupleniy na finansovom rynke [Types of digital traces of crimes in the financial market]. // Aktual'nyye problemy rossiyskogo prava – Actual problems of Russian law. 2025. №2 (171). URL: https://cyberleninka.ru/article/n/vidy-tsifrovyh-sledov-prestupleniy-na-finansovom-rynke (дата обращения: 09.12.2025).

5. The Bank of Russia discloses a list of companies with identified signs of a "financial pyramid," an illegal lender, an illegal professional participant in the securities market (including an illegal forex dealer) and other illegal participants in the financial market (URL: https://cbr.ru/ inside/warning-list/ (circulation date: 09.12.2025)).

6. Gavrilin, Yu. V., Shmonin, A. V. Ispol'zovaniye informatsii, poluchennoy iz seti Internet, v rassledovanii prestupleniy ekstremistskoy napravlennosti [Use of information obtained from the Internet in the investigation of extremist crimes]. Trudy Akademii upravleniya MVD Rossii. – Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2019. № 1 (49).

7. Vasyukov, V.F., Starzhinskaya, A.N. Ob operativno-rozysknykh i sledstvennykh merakh protivodeystviya legalizatsii prestupnykh dokhodov s ispol'zovaniyem kriptovalyut [On operational-search and investigative measures to counter the legalization of criminal proceeds using cryptocurrencies]. Rossiyskoye pravo: obrazovaniye, praktika, nauka. – Russian law: education, practice, science. 2024. № 4. Pp. 68 – 78.

8. The Bank of Russia identified almost 3.5 thousand illegal immigrants in the first half of 2024//URL: https://cbr.ru/ press/event/?id=18871/ (circulation date: 09.12.2025);

9. Batrachenko, D. A., Vasyukov, V. F. Nekotoryye voprosy polucheniya operativno znachimoy i kriminalisticheskoy informatsii iz oblachnykh khranilishch [Some issues of obtaining promptly significant and forensic information from cloud storage] yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoy Akademii MVD Rossii. – Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2025. VOL. 1 NO. 69 (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Крысина Татьяна Евгениевна, адъюнкт. Орловский юридический институт МВД России имени В. В. Лукьянова. 302027, Российская Федерация, г. Орел, ул. Игнатова, 2.

INFORMATION ABOUT THE AUTHOR

Tatyana E. Krysina, Adjunct. Oryol Law Institute of the MIA of Russia named after V.V. Lukyanov. 2, Ignatova St., Oryol, Russian Federation, 302027.