

КРИМИНАЛИСТИКА И КРИМИНОЛОГИЯ. СУДЕБНАЯ ЭКСПЕРТИЗА

DOI: 10.17803/1994-1471.2025.171.2.111-124

А. В. Отогочев*

Виды цифровых следов преступлений на финансовом рынке

Аннотация. Автором разработана криминалистическая классификация наиболее актуальных цифровых следов преступлений на финансовом рынке, установление и изъятие которых имеют большое значение при выявлении и идентификации организаторов преступных схем в условиях цифровой трансформации. Была поставлена задача проанализировать цифровые следы, образуемые при совершении преступлений на финансовом рынке, притом что ряд преступных деяний может совершаться на легальном финансовом рынке при вовлечении финансовых организаций и их сотрудников, а также на нелегальном финансовом рынке, образующем теневой сектор нелегальных финансовых услуг, включая создание финансовых пирамид. В результате исследования был сделан вывод, что цифровые следы в случае преступлений с вовлечением лицензированных финансовых организаций и при участии нелегальных субъектов финансового рынка различаются по содержанию, а также по степени их сохранности от уничтожения, что в ряде ситуаций требует оперативных мер по их фиксации и изъятию. Автор заключил, что успешное расследование преступлений на финансовом рынке во многом зависит от результатов экспертных исследований цифровых следов экономического содержания и компьютерной информации, для которых необходимо проведение комплекса судебных экспертиз.

Ключевые слова: криминалистика; цифровые следы; виды цифровых следов; цифровизация; компьютерная информация; финансовые расследования; финансовый рынок; судебно-экономическая экспертиза; судебная компьютерно-техническая экспертиза; расследования преступлений на финансовом рынке; нелегальная деятельность на финансовом рынке; финансовые пирамиды; схемы Понци; криптовалюта.

Для цитирования: Отогочев А. В. Виды цифровых следов преступлений на финансовом рынке // Актуальные проблемы российского права. — 2025. — Т. 20. — № 2. — С. 111–124. — DOI: 10.17803/1994-1471.2025.171.2.111-124.

© Отогочев А. В., 2025

* Отогочев Александр Викторович
a.otogochев@mail.ru

Types of Digital Traces of Crimes in the Financial Market

Aleksandr V. Otogochev

a.otogochev@mail.ru

Abstract. The author has developed a forensic classification of the most relevant digital traces of crimes in the financial market, the establishment and seizure of which is of great importance in identifying and detecting the organizers of criminal schemes in the context of digital transformation. The author sets the task to analyze digital traces that appear in the process committing crimes in the financial market. It is taken into account that a number of criminal acts can be committed in the legal financial market with the involvement of financial organizations and their employees, as well as in the illegal financial market, which forms the shadow sector of illegal financial services, including the formation of financial pyramids. The result of the study is the conclusion that digital traces in the case of crimes involving licensed financial organizations and involving illegal entities of the financial market differ in their content, as well as in the degree of their preservation from destruction, which in some cases requires prompt measures to record and seize them. The author concluded that successful investigation of crimes in the financial market largely depends on the results of expert studies of digital traces of economic content and computer information, which require a range of forensic examinations.

Keywords: forensics; digital traces; types of digital traces; digitalization; computer information; financial investigations; financial market; forensic economic examination; forensic computer-technical examination; investigation of crimes in the financial market; illegal activity in the financial market; financial pyramids; Ponzi schemes; cryptocurrency.

Cite as: Otogochev AV. Types of Digital Traces of Crimes in the Financial Market. *Aktual'nye problemy rossijskogo prava*. 2025;20(2):111-124. (In Russ.). DOI: 10.17803/1994-1471.2025.171.2.111-124.

В условиях стремительной цифровизации различных сфер современной жизни общество всё сильнее зависит от информационно-телекоммуникационных сетей. В инвестиционной деятельности, как и в иных сферах экономической деятельности, широко используются современные финансовые технологии и ИТ. Вместе с тем одновременно с легальными формами такой деятельности на финансовом рынке образуется теневой сектор нелегальных финансовых услуг, подрывающий экономическую безопасность государства.

В соответствии со Стратегией экономической безопасности Российской Федерации на период до 2030 г.¹ к основным вызовам и угрозам экономической безопасности в том числе относятся сохранение значительной доли теневой экономики и высокий уровень криминализации и коррупции в экономической сфере.

Финансовый рынок является неотъемлемой частью экономической системы, и его развитие во многом зависит от модели развития российской экономики, подходов к решению стоящих перед ней задач и преодолению вызовов. Важные факторы развития финансового рынка — это доверие и конкурентное взаимодействие между его участниками. Согласно разработанному Банком России «Основным направлениям развития финансового рынка Российской Федерации на 2024 год и период 2025 и 2026 годов»² значимым фактором формирования доверия на финансовом рынке в том числе является обеспечение высокого уровня защиты от недобросовестных практик и мошенничества.

Организованная преступность в условиях цифровизации на постоянной основе совершенствует способы совершения преступлений на финансовом рынке, используя дистанционные каналы связи и средства коммуникации, а также

¹ Указ Президента РФ от 17.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // СЗ РФ. 2017. № 20. Ст. 2902.

² Вестник Банка России. 2024. № 5.

приемы социальной инженерии, что создает риски и угрозы для потребителей финансовых продуктов и услуг. Дистанционные способы совершения преступлений, позволяющие исключить взаимодействие между участниками преступных групп и их жертвами (потерпевшими), использование способов анонимизации пользователей в сети Интернет, осуществление взаиморасчетов за незаконные финансовые услуги с использованием счетов подставных лиц, так называемых дропов, и криптовалют требуют от уполномоченных органов выработки соответствующих мер и подходов.

Согласно отчету ФКУ «Главный информационно-аналитический центр Министерства внутренних дел Российской Федерации» о состоянии преступности в России за первое полугодие 2024 г., отмечается рост числа преступлений с использованием информационно-телекоммуникационных технологий на 15,8 % (всего 368,8 тыс.) по сравнению с аналогичным периодом предыдущего года, из которых четыре преступления из пяти (82,4 %) совершаются с использованием сети Интернет. По сравнению с первым полугодием 2023 г. на 0,8 % сократилось число преступлений экономической направленности. Всего выявлено 66,8 тыс. преступлений данной категории, из которых 8,1 тыс. (12,1 %) связаны с финансово-кредитной системой. Материальный ущерб от преступлений экономической направленности составил 153,5 млрд руб.³

Одним из прямых следствий цифровой трансформации современной преступности стало появление особого вида криминалистически значимой информации, получившей название «цифровые следы». В настоящее время дано множество определений цифровых следов и уже есть первые попытки законодательного закрепления такого понятия. В опубликованном проекте «Концепции комплексного регулиро-

вания (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики», предложенной Институтом законодательства и сравнительного правоведения при Правительстве РФ, «цифровые следы» трактуются как данные, формируемые пользователем в информационных системах и вследствие работы программного обеспечения⁴.

По нашему мнению, в криминалистическом значении «цифровые следы» — более широкое понятие. Если рассмотреть следственные ситуации преступлений на финансовом рынке, очевидно, что, помимо цифровых следов в информационно-телекоммуникационных сетях, вещественными доказательствами также выступают финансовые операции, история взаимодействия финансовых организаций и их клиентов и др.

С точки зрения криминалистики наиболее подходящее определение цифровых следов было дано Е. Р. Россинской и И. А. Рядовским, которые относят цифровые следы к *криминалистически значимой компьютерной информации о событиях или действиях, отраженной в материальной среде, в процессе ее возникновения, обработки, хранения и передачи*⁵.

Данное определение наиболее полно охватывает информационные процессы, связанные с получением, хранением, обработкой и передачей компьютерной информации, содержащейся как в сети Интернет, так и на отдельных носителях. Стоит также отметить, что компьютерная информация — это сведения, существующие в виде электромагнитных сигналов, возникающих в процессе функционирования компьютеров, электронных средств связи, информационно-телекоммуникационных систем, и такая информация может быть доступна осознанию человека исключительно с использованием специализированных программных и аппаратных средств. Таким образом, фиксация и изъятие

³ Состояние преступности в Российской Федерации за январь — июнь 2024 г. // Главный информационно-аналитический центр МВД России. URL: <https://xn--b1aew.xn--p1ai/reports/item/53218362/> (дата обращения: 19.08.2024).

⁴ URL: <https://clck.ru/3DPVmm> (дата обращения: 19.08.2024).

⁵ *Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике* // Аубакировские чтения : материалы международной научно-практической конференции (19 февраля 2019 г.). Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗЖРБЖҰБ, 2019. С. 7.

цифровых данных требуют соблюдения определенного порядка действий с целью обеспечения их сохранности, достоверности и дальнейшей возможности использования в качестве вещественных доказательств по делу.

Цифровые следы могут быть классифицированы по разным основаниям, и на сегодняшний день в научных работах введено множество видов цифровых следов. Мы предлагаем особую классификацию цифровых следов, наиболее актуальную для расследований преступлений на финансовом рынке. Цифровые следы преступлений на финансовом рынке можно разделить по трем критериям.

К первой классификации предлагаем отнести цифровые следы, выделяемые по характеру получения к ним доступа в целях их фиксации и изъятия.

Цифровые следы на финансовом рынке могут быть доступны:

- неограниченному кругу лиц;
- уполномоченным лицам в пределах предоставленных законом полномочий.

Данная классификация актуальна при выявлении цифровых следов на финансовом рынке по ряду причин, и главная — это невозможность изъятия цифровых следов, доступ к которым ограничен законодательством Российской Федерации. Отсутствие законных полномочий и оснований изъятия охраняемых законом цифровых следов зачастую становится серьезным препятствием для выявления и пресечения преступлений на финансовом рынке.

В первом случае цифровые следы могут быть доступны неограниченному кругу лиц в любой момент. К таким цифровым следам относится общедоступная информация, содер-

жащая криминалистически значимую информацию о событиях преступления или лице, его готовящем, совершающем или совершившем. Согласно действующему законодательству об информационных технологиях и защите информации⁶ понятие «общедоступная информация» определяется как «общеизвестные сведения и иная информация, доступ к которой не ограничен», а также «информация, размещаемая ее обладателями в сети “Интернет” в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования» (общедоступная информация, размещаемая в форме открытых данных).

Таким образом, цифровые следы в виде общедоступной информации неограниченно доступны любому лицу в любой момент, пока данные не уничтожены правообладателями такой информации либо владельцами сетевых устройств, на которых она хранится.

К общедоступным данным, которые могут быть использованы в качестве доказательственной информации при расследовании преступлений на финансовом рынке, предлагаем отнести следующие:

— информацию из открытых официальных реестров (реестр поднадзорных Банку России финансовых организаций, список компаний с выявленными признаками нелегальной деятельности на финансовом рынке⁷, платформа «Знай своего клиента»⁸, единые государственные реестры юридических лиц, индивидуальных предпринимателей и т.п.);

— публичные коммерческие данные (информацию о компании, эмитенте ценных бумаг, раскрытие информации эмитентами ценных бу-

⁶ Ч. 1 и 4 ст. 7 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

⁷ 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: 20.09.2024)).

⁸ С 1 октября 2024 г. Банк России открыл сервис, который позволяет по запросу получить справочную информацию о том, относится ли на платформе «Знай своего клиента» (ЗСК) индивидуальный предприниматель или юридическое лицо к группе высокого уровня риска совершения подозрительных операций (URL: <https://www.cbr.ru/press/event/?id=21020> (дата обращения: 20.09.2024)).

маг, результаты биржевых торгов (итоги торгов ценными бумагами, в том числе на фондовом, срочном, валютном, товарном рынках и др.), сайты информационных агентств, специализирующихся в сфере финансовых рынков, и др.);

- материалы средств массовой информации (статьи, интервью и др.);

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

- социальные сети (аккаунты пользователей с рядом идентификационных данных о лице, в том числе его фото-, видеоизображения, аудиоданные, сведения о местоположении (геолокации) размещенных постов, публичные сообщения, подписи к постам, комментарии, сведения о контактах).

Ю. В. Гаврилин и А. В. Шмонин обращают внимание на то, что социальные сети содержат большое количество криминалистически значимой информации. Прежде всего, это контент, который выкладывают пользователи на свои страницы сайта социальной сети. Анализ контента позволяет определить круг общения пользователя, его образ жизни, увлечения, род занятий, возможный уровень доходов, географию перемещений, семейное положение и состав семьи, используемый автотранспорт и пр.⁹

На практике при проведении предварительной проверки по сообщению о преступлении, когда доказательственная информация находится на страницах социальных сетей пользователей в сети Интернет, следователи руководствуются статьями 176, 177 УПК РФ, т.е. осуществляют осмотр и последующую фиксацию, изъятие цифровых следов преступления в рамках

проведения такого следственного действия, как осмотр предметов (документов)¹⁰.

Как отмечают исследователи, в Российской Федерации за последние годы почти каждое 20-е зарегистрированное преступление совершается с использованием сети Интернет¹¹. Общедоступная информация в сети Интернет, включая средства массовой информации, может помочь связать исследуемые события, а также определить мотив, умысел и цели совершения тех или иных действий.

В качестве примера значимой и общедоступной информации, хранящейся в сети Интернет, стоит привести результаты проверки Банком России неправомерного использования инсайдерской информации и манипулирования рынком ценных бумаг. Так, акционеры и инсайдеры авиакомпании «Трансаэро», обладая инсайдерской информацией, во избежание убытков свыше 200 млн руб. от продажи акций эмитента на фоне аннулирования сертификата эксплуатанта, на основании которого эмитент осуществлял авиаперевозки, *сделали заявления в средствах массовой информации о возможном возобновлении основной деятельности эмитента, что способствовало поддержанию спекулятивных настроений инвесторов*. По итогам финансового расследования Банк России установил, что «указанная инсайдерская информация не была раскрыта, что дало возможность продать Акции широкому кругу инвесторов на анонимных биржевых торгах по текущим рыночным ценам»¹².

Другой вид цифровых следов данной классификации *доступен исключительно уполномоченным лицам в пределах предоставленных законом полномочий*. От уровня доступа к информации, содержащей цифровые следы,

⁹ 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). С. 108–109.

¹⁰ Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей или мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 109.

¹¹ Гужаева В. А., Прокофьева Е. В., Прокофьева О. Ю. Преступность в сети Интернет: криминологические характеристики // Вестник экономической безопасности. 2019. № 4. С. 112.

¹² Об установлении фактов неправомерного использования инсайдерской информации и манипулирования рынком обыкновенных акций ОАО «АК «Трансаэро» // URL: https://cbr.ru/press/PR/?file=27062019_163000sbrfr2019-06-27T16_21_57.htm (дата обращения: 27.08.2024).

зависят эффективность собирания цифровых следов и, как следствие, успех в раскрытии преступления. Например, для получения вещественных доказательств следователю требуются данные, получение которых затрагивает конституционные права граждан. Для категории дел в отношении преступлений на финансовом рынке зачастую это мероприятия, связанные с производством выемки документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, или, например, получение информации о соединениях между абонентами и (или) абонентскими устройствами. Так, в соответствии с ч. 3 ст. 183 УПК РФ выемка предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну, предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, а также вещей, заложенных или сданных на хранение в ломбард, производится на основании судебного решения, принимаемого в порядке, установленном статьей 165 УПК РФ.

Другим примером получения цифровых следов, содержащих сведения о финансовых операциях, является отслеживание транзакций с криптовалютами, и, как правило, для запроса таких данных требуются соответствующие полномочия. В последние годы прослеживается устойчивая тенденция использования в преступных целях цифровых валют (криптовалют). Если в 2011 г. криптовалютой в редких случаях оплачивались наркотические средства в крупных и особо крупных размерах, то в настоящее время взаиморасчеты за наркотические средства производятся преимущественно в криптовалютах, в том числе за розничные дозы. Тем не менее преступления на финансовом рынке также совершаются с использованием криптовалюты. По данным Банка России, в первом полугодии 2024 г. 59 % выявленных субъектов с признаками «финансовых пирамид» привлекали средства клиентов в криптовалютах: «Такие инструменты позволяют злоумышленникам со-

хранять анонимность, а пострадавшие клиенты не могут потом доказать обман»¹³.

И всё же управление криптокошельком и осуществление операций с криптовалютами не так анонимны, как считают многие. В большинстве случаев производится обязательная процедура идентификации личности пользователя криптокошелька, как это предусмотрено большинством зарубежных криптобирж в рамках процедуры «Знай своего клиента» (англ. Know your customer, KYC), являющейся многоэтапной операцией, включающей сбор и анализ личной информации клиентов. В то же время есть зарубежные площадки, на которых возможны транзакции с криптовалютами без идентификации личности либо посредством упрощенной идентификации, позволяющей проводить операции и не проходить процедуру KYC, но до установленных лимитов. Впрочем, даже в таких случаях пользователь оставляет цифровые следы, с помощью которых правоохранительные органы смогут установить его личность.

В настоящее время существуют методы деанонимизации транзакций криптовалюты путем отслеживания всей цепочки их проведения, поскольку данные транзакций криптовалют, хранящиеся в публичных блокчейнах, доступны общественности. *Блокчейн*, также известный как децентрализованный цифровой реестр, представляет собой специальный тип базы данных, которая безопасно хранит записи в компьютерной сети, делая их *прозрачными, неизменяемыми и защищенными* от взлома. Каждый «блок» содержит определенные данные и связан с предыдущим «блоком» в хронологической цепочке, обеспечивая защиту с помощью криптографии.

Хотя блокчейн может хранить различные типы информации, наиболее распространенным его применением является реестр транзакций криптовалют. *Децентрализованность* означает, что блокчейн позволяет распределять данные в базе данных между несколькими сетевыми узлами — компьютерами или устройствами, на которых запущено программное обес-

¹³ Банк России выявил в первом полугодии 2024 года почти 3,5 тысячи нелегалов // URL: <https://cbr.ru/press/event/?id=18871/> (дата обращения: 29.08.2024).

печение для блокчейна. Узлы блокчейна позволяют предотвратить изменение информации в цепочке блоков. *Прозрачность* блокчейна означает, что все транзакции можно просматривать, используя обозреватели блокчейнов, которые позволяют видеть транзакции, происходящие в реальном времени. Например, в мире было много случаев взлома криптобирж, что приводило к потере больших сумм криптовалюты. Несмотря на анонимность хакеров, криптовалюту, которую они извлекли, легко отследить, поскольку адреса кошельков хранятся в блокчейне. Разумеется, хранящиеся в блокчейне записи зашифрованы, поэтому пользователи блокчейна могут оставаться анонимными.

Согласимся с мнением Ю. В. Гаврилина и И. С. Бедерова о том, что эффективная борьба с преступлениями, совершаемыми с использованием криптовалют, возможна при активном использовании в расследовании криминалистически значимой информации, полученной в процессе анализа больших данных. Это означает, что эффективность раскрытия преступления зависит от использования совокупности цифровых следов, полученных как из общедоступных источников информации, так и при взаимодействии с уполномоченными органами¹⁴.

Ко второй классификации цифровых следов на финансовом рынке предлагаем отнести *виды данных, выделенные по степени их сохранности: статические и динамические*.

Цифровые следы несут значимую для следствия информацию о событиях преступления, и первоочередная задача следователя — оперативно обеспечить их фиксацию и сохранность. Цифровые следы могут быть полностью уничтожены, заблокированы либо модифициро-

ваны, что впоследствии существенно снижает эффективность расследования.

В постановлении Пленума Верховного Суда РФ от 15.12.2022 № 37 дается определение таким понятиям, как «уничтожение», «блокирование» и «модификация компьютерной информации»¹⁵.

Уничтожение компьютерной информации — это приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена. Под *блокированием* компьютерной информации понимается воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме. Под *модификацией* компьютерной информации подразумевается внесение в нее любых изменений, включая изменение ее свойств, например целостности или достоверности.

В силу дуалистической природы цифровых следов их возникновение и характер обусловлены, с одной стороны, используемой в информационной системе технологией записи информации, а с другой — требованиями действующего законодательства к субъектам цифровой инфраструктуры: интернет-провайдерам, операторам связи, кредитно-финансовым организациям и др.¹⁶

Статические цифровые следы защищены от изменения и уничтожения в силу требований законодательства или иных нормативных

¹⁴ Гаврилин Ю. В., Бедеров И. С. Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учеб. пособие. М. : Академия управления МВД России, 2022.

¹⁵ Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”» // URL: <https://vsrf.ru/documents/own/31913/> (дата обращения: 18.08.2024).

¹⁶ Гаврилин Ю. В., Салеева Ю. Е. Развитие учения о криминалистической регистрации в условиях цифровой трансформации преступности // Труды Академии управления МВД России. 2023. № 2 (66). С. 99–105.

документов, регламентов, порядков. Например, отзыв лицензии у кредитной организации и прекращение ее деятельности как финансовой организации, обслуживающей своих клиентов, вовсе не означают, что следователь не сможет получить необходимые сведения в отношении конкретных расчетных счетов или операций. После отзыва у банка лицензии в порядке, установленном законодательством Российской Федерации, Банком России назначается временная администрация, которая является органом управления банка до вынесения арбитражным судом решения об открытии конкурсного производства или о начале процедуры ликвидации. Для получения сведений, подтверждающих совершение денежно-расчетных операций в кредитной организации, у которой отозвана лицензия на осуществление банковских операций, следователю необходимо обратиться в установленном законодательством порядке к руководителю временной администрации, назначенной после отзыва у кредитной организации лицензии, либо к ликвидатору кредитной организации. В случае если ликвидационные процедуры в отношении кредитной организации завершены, сведения, образовавшиеся в ходе деятельности кредитной организации (в том числе документы, подтверждающие совершение расчетных операций), сроки хранения которых не истекли, хранятся в архивных учреждениях¹⁷.

Динамические цифровые следы имеют свойство изменения во времени в силу непосредственного внешнего воздействия или при наступлении определенных условий. Этот тип цифрового следа не защищен и может быть умышленно уничтожен, изменен или приведен в непригодное состояние. Например, в 2020 г. Банком России была выявлена «финансовая пирамида» «Antares Trade»¹⁸, которая является одной из самых крупных в России после краха всем известной «МММ», причем пострадавшие от деятельности указанной «финансовой

пирамиды» есть за пределами России. Компания «Antares Trade» — это весьма показательный пример динамических цифровых следов по ряду причин. Компания позиционировала себя как цифровой маркетплейс, предоставлявший продукты и услуги компаний-партнеров по получению доходности до 2 % в сутки. Взаимодействие клиентов с компанией осуществлялось с использованием платформы на интернет-сайте, приложения на смартфоне и каналов в мессенджере Telegram. Для того чтобы воспользоваться услугами компании, потенциальному клиенту требовалось пройти регистрацию на сайте, а также процедуру верификации посредством предоставления персональных данных. Денежные средства граждан привлекались в криптовалюту, а также путем перевода денежных средств с использованием зарубежных электронных платежных систем.

Для вовлечения в деятельность «Antares Trade» активно использовались социальные сети, а также модель MLM-реферальных программ (англ. Multi-Level Marketing), когда участники получают проценты от вноса приведенных ими новых участников. Так, в зарубежной социальной сети одним из российских менеджеров «Antares Trade» выложена видеозапись (сторис¹⁹) мероприятия за границей, посвященного годовщине компании, в котором приняло участие «более 400 представителей компании из разных стран» (по данным анонса мероприятия), в том числе из России. Указанная трансляция хранилась лишь 24 часа согласно правилам социальной сети, что подчеркивает важность своевременного выявления и обеспечения сохранения цифровых следов, которые впоследствии могут являться дополнительными вещественными доказательствами по делу, в частности подтвердить нахождение лица (лиц) в конкретное время и в определенном месте.

С точки зрения вещественных доказательств в отношении организаторов «финансовой пира-

¹⁷ Сведения о местонахождении архивов ликвидированных кредитных организаций см.: URL: <https://www.cbr.ru/vfs/credit/LikvidBase/ArchiveDoc.pdf/> (дата обращения: 03.09.2024).

¹⁸ Antares Limited (Antares Trade) // URL: <https://cbr.ru/inside/warning-list/detail/?id=7842> (дата обращения: 03.09.2024).

¹⁹ Сторис (stories) — публикация фото- и видеоизображения, доступного для просмотра 24 часа.

миды» «Antares Trade» все вышеуказанные факты деятельности компании и взаимодействие ее участников, являются цифровыми следами, содержащими криминалистически важную информацию. После прекращения деятельности «Antares Trade» неустановленные лица уничтожили большую часть информации о своей деятельности на интернет-сайте и иных ресурсах, а приложение, в котором участники отслеживали свой доход, было удалено из магазина приложений для мобильных устройств, и у пострадавших лиц остались лишь скриншоты, подтверждающие их участие в данном псевдопроекте. По данным прокуратуры г. Москвы, «один из пострадавших инвестировал по рекомендации знакомого более 3,5 млн руб. в криптовалюту, но впоследствии было обнаружено, что платформа заблокирована, вывести криптовалюту стало невозможным»²⁰.

Указанный пример организации «финансовой пирамиды» подтверждает тот факт, что цифровые следы могут быть уничтожены в целях сокрытия событий преступлений и лиц, их совершивших, что ставит перед правоохранительными органами задачу оперативного выявления и фиксации цифровых следов.

В рамках *третьей классификации* предлагаем разделять цифровые следы на финансовом рынке по способу их формирования:

- сформированные самостоятельно;
- сформированные согласно установленным требованиям.

Цифровые следы, сформированные самостоятельно, — это те данные, которые созданы и зафиксированы по воле самого субъекта — источника цифровых следов. Они формируются в процессе взаимодействия лица с информационными системами и техническими средствами, при этом лицо намеренно оставляет цифровые «отпечатки» в таких системах в виде различной информации о себе и своих действиях. Например, к цифровым следам на финансовом рынке,

сформированным пользователем самостоятельно и позволяющим установить его личность в сети Интернет, относятся:

- имя пользователя, никнейм (сетевой псевдоним пользователя);
- адрес электронной почты, номер телефона, адрес в социальной сети;
- фотография или аватар, видеоизображение;
- геолокационная информация (например, при публикации фотографии в социальной сети);
- публичные переписки и участие в группах, сообществах, «реакции», «лайки» и др.;
- опубликованные финансовые реквизиты (банковская карта, счет, электронный кошелек, криптокошелек).

Данный вид цифровых следов, как правило, важен при расследовании *нелегальной деятельности на финансовом рынке*, т.е. в тех случаях, когда лицо не идентифицировано и требуется найти хоть какую-то зацепку, чтобы с помощью совокупности таких цифровых следов с какой-то долей вероятности определить лицо или перечень лиц для последующей проверки. В отдельных сложных случаях, когда преступник принял меры по анонимизации и сокрытию своей личности, такие цифровые следы могут быть единственными данными, которые смогут помочь в установлении лица.

Цифровые следы, сформированные согласно установленным требованиям, фиксируются независимо от воли лица, поскольку необходимость записи (сохранения) конкретной информации о субъекте, взаимодействовавшем с той или иной информационной системой, — это требование различных правовых норм (федеральных законов, нормативных актов, приказов конкретных предприятий, учреждений, организаций и пр.). Например, эффективное противодействие отмыванию денег и финансированию терроризма, распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ)²¹ обеспечивается посредством организации внутреннего

²⁰ Вести-Москва. Сумма ущерба от пирамиды «Антарес» может исчисляться миллиардами // URL: <https://smotrim.ru/video/2709481> (дата обращения: 03.09.2024).

²¹ Разработкой Международных стандартов в сфере ПОД/ФТ/ФРОМУ и контролем за их выполнением всеми государствами занимается межправительственная организация — Группа разработки финансовых мер борьбы с отмыванием денег (Financial Action Task Force, FATF).

контроля в финансовой организации. На данный момент внутренний контроль некредитной финансовой организации²² по данному направлению должен строиться на основе положения Банка России от 15.12.2014 № 444-П²³, согласно которому организация обязана до приема на обслуживание идентифицировать клиента (физическое или юридическое лицо), запросив от такого лица установленный перечень персональных и иных данных.

Для обеспечения успешного расследования преступлений на финансовом рынке следователю необходимо тщательно проанализировать имеющуюся в материалах уголовного дела информацию об обстоятельствах преступления, чтобы выяснить, какие сведения еще нужно установить или уточнить. Поскольку расследование преступлений на финансовом рынке требует специальных знаний в области рынка ценных бумаг, бухгалтерского учета, а также в сфере ИТ, следователю необходимы заключения исследований, назначенных по обнаруженным и изъятым цифровым следам.

С учетом введенной классификации цифровых следов на финансовом рынке справедливо отметить важность исследований цифровых следов в рамках ряда судебных экспертиз. Как отмечает Е. Р. Россинская²⁴, цифровые следы стали в последние годы объектами исследования во многих видах судебных экспертиз, в первую очередь класса *судебных компьютерно-технических экспертиз*.

На наш взгляд, в большинстве следственных ситуаций объектами исследований преступлений на финансовом рынке будет следующая компьютерная техника:

— различные виды компьютеров и их компоненты, посредством которых совершались банковские операции, подавались поручения на совершение сделок с финансовыми инструментами с использованием торговых терминалов, и др.;

— сетевые технические средства (серверы, рабочие станции и др.);

— средства связи (мобильные телефоны, смартфоны и др.);

— съемные носители информации (USB-накопители, CD-, DVD-диски и др.);

— электронные средства фиксации информации (системы видеонаблюдения, видеокамеры, фотоаппараты и др.);

— иные технические средства, имеющие встроенные микропроцессоры.

Указанные технические устройства как объекты исследований могут содержать криминалистически значимую компьютерную информацию о событиях преступления, а также лицах, причастных к их совершению.

По правовому статусу компьютерная информация подразделяется на два вида: документированная информация (документ) и информация, не имеющая документированной формы (сообщение). По функциональному назначению компьютерная информация подразделяется на текстовые и графические документы, служебную информацию, данные в форматах мультимедиа, информацию в форматах баз данных, программное обеспечение.

Видится, что криминалистически значимые сведения о преступлениях на финансовом рынке содержатся в следующей компьютерной информации:

²² Некредитными финансовыми организациями признаются лица, указанные в ст. 76.1 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (см.: URL: https://www.consultant.ru/document/cons_doc_LAW_37570/ (дата обращения: 05.09.2024)).

²³ Положение Банка России от 12.12.2014 № 444-П «Об идентификации некредитными финансовыми организациями клиентов, представителей клиента, выгодоприобретателей, бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // URL: https://www.consultant.ru/document/cons_doc_LAW_174501/ (дата обращения: 05.09.2024).

²⁴ Россинская Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 2. С. 27–40.

- данных информационного обмена участников финансового рынка;
- раскрытии информации эмитентами эмиссионных ценных бумаг (информация о выпуске (дополнительном выпуске) ценных бумаг, проспект ценных бумаг, отчеты эмитента, сообщения о существенных фактах, консолидированная финансовая отчетность, бухгалтерская финансовая отчетность и др.)²⁵;
- записях о клиентах, а также об их сделках и операциях с денежными средствами, ценными бумагами, иностранными финансовыми инструментами и товарами, образуемых в результате внутреннего учета профессионального участника рынка ценных бумаг (записи внутреннего учета сделок, денежных средств, финансовых инструментов, записи в журнале регистрации поручений (требований) клиента и др.)²⁶;
- сетевых данных (например, списки сетевых адресов, с которых осуществлялись соединения программных комплексов²⁷ клиента с программно-техническими комплексами компании, с указанием IP-адресов, MAC-адресов).

В рамках настоящего исследования мы пришли к выводу, что цифровые следы в виде компьютерной информации в отношении преступлений на легальном и нелегальном финансовых рынках *различаются по содержанию и степени риска уничтожения*. Это прежде всего связано с тем, что в случае цифровых следов преступлений, совершенных на легальном финансовом рынке, в преступные деяния вовлекаются финансовые организации, иначе говоря, участники финансового рынка, имеющие соответствующие лицензии (разрешения) Банка России²⁸, а также их клиенты (юридические и физические лица). В случае нелегального²⁹ финансового рынка в преступные деяния, как правило, вовлечены юридические и (или) физические лица, которые одновременно могут являться клиентами участников финансового рынка, например клиенты брокера, управляющей компании.

Нами представлен неисчерпывающий перечень цифровых следов, как характерных для легального и нелегального финансовых рынков в отдельности, так и встречающихся в обоих случаях.

Легальный финансовый рынок	Нелегальный финансовый рынок
Информация об участниках финансового рынка (отчетность компании (например, эмитента), внутренние документы компании (порядки, регламенты)) и их клиентах (анкеты клиентов, выписки, записи внутреннего учета операций и др.; выписки по счетам из кредитных организаций и пр.)	Информация о клиентах участников финансового рынка (анкеты клиентов, записи внутреннего учета операций; выписки по счетам из кредитных организаций и др.)

²⁵ Перечень раскрытия информации эмитентами эмиссионных ценных бумаг установлен положением Банка России от 27.03.2020 № 714-П «О раскрытии информации эмитентами эмиссионных ценных бумаг» (URL: https://www.consultant.ru/document/cons_doc_LAW_352306/ (дата обращения: 09.09.2024)).

²⁶ Внутренний учет профессионального участника рынка ценных бумаг установлен положением Банка России от 31.01.2017 № 577-П «О правилах ведения внутреннего учета профессиональными участниками рынка ценных бумаг, осуществляющими брокерскую деятельность, дилерскую деятельность и деятельность по управлению ценными бумагами» (URL: https://www.consultant.ru/document/cons_doc_LAW_213942/ (дата обращения: 09.09.2024)).

²⁷ В случае торговли на организованных биржевых торгах — информационно-торговая система QUIK или аналоги.

²⁸ Все организации, которые предоставляют финансовые услуги: банки, небанковские кредитные организации, негосударственные пенсионные фонды, страховые организации, управляющие компании, профессиональные участники рынка ценных бумаг (в том числе брокеры, дилеры, инвестиционные советники), операторы финансовых платформ и другие операторы финансовых услуг, микрофинансовые организации, кооперативы (ЖНК, КПК, СКПК), ломбарды, бюро кредитных историй, актуарии и др. Справочник легальных компаний расположен на сайте Банка России (URL: <https://www.cbr.ru/finorg/>).

²⁹ Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке // URL: <https://cbr.ru/inside/warning-list/> (дата обращения: 09.09.2024).

Легальный финансовый рынок	Нелегальный финансовый рынок
Информация о взаимодействии между участниками финансового рынка, а также их клиентами (электронная переписка, запись телефонных переговоров, видеозаписи и др.)	Информация о взаимодействии участников финансового рынка с их клиентами (электронная переписка, запись телефонных переговоров, видеозаписи, копии запросов о предоставлении информации и документов, ответов (объяснений) и др.)
Данные интернет-ресурсов участников финансового рынка	Данные интернет-ресурсов нелегальных участников финансового рынка, социальных сетей, мессенджеров
Сетевые данные (IP-адреса, MAC-адреса, время соединения)	
Данные операторов подвижной радиотелефонной связи (факты приема-передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, информация о местоположении используемых базовых станций, об IP-адресах, используемых для входа в личный кабинет, IMEI (международный идентификатор мобильного оборудования) и др.)	
—	Данные об операциях с криптовалютами

Из приведенного перечня следует, что для легального и нелегального финансовых рынков цифровые следы преступлений *могут различаться по содержанию*. Кроме того, в случае нелегального финансового рынка большая часть цифровых следов, содержащих криминалистически значимую информацию, имеет высокие риски уничтожения.

С учетом введенной нами классификации цифровых следов на финансовом рынке по степени сохранности *динамические цифровые следы*, имеющие свойство временного хранения, наиболее характерны для преступлений, совершаемых на нелегальном финансовом рынке. Таким образом, в случае расследования преступных деяний, совершенных на нелегальном финансовом рынке, следовательно необходимо принимать оперативные меры по фиксации и изъятию динамических цифровых следов.

Другой, не менее значимой судебной экспертизой, которая потребуется для успешного расследования уголовного дела данной направленности, является *судебно-экономическая экспертиза*. А. А. Савицкий считает, что при производстве судебно-экономических экспертиз следует различать понятия «вопросы» и

«задачи», поскольку для решения экспертных задач необходимо проведение исследований по поставленным перед экспертом вопросам, а, несмотря на кажущееся сходство категорий «вопросы» и «задачи», отождествлять их не представляется возможным³⁰.

Предлагаем на примере дел, связанных с организацией «финансовых пирамид», как наиболее распространенного вида мошенничества на финансовом рынке выделить две типовые задачи при производстве судебно-экономической экспертизы:

1. Исследование финансово-хозяйственной деятельности организации на основании анализа информации о финансовых операциях (выписок по банковским и иным счетам), финансовой отчетности, финансово-хозяйственных документов, иных документов.

2. Исследование фактов, свидетельствующих о наличии признаков организации деятельности по принципу «финансовой пирамиды»:

— выплата дохода и (или) предоставление иной выгоды лицам, чьи денежные средства и (или) иное имущество привлечены ранее, осуществляются за счет привлеченных денежных средств и (или) иного имущества иных физических лиц и (или) юридических лиц;

³⁰ Савицкий А. А. Актуальные задачи и вопросы судебной финансово-экономической экспертизы по делам о банкротстве в уголовном и арбитражном процессах // Вестник Университета имени О.Е. Кутафина (МГЮА). 2024. № 3. С. 64–76.

— отсутствие инвестиционной и (или) иной законной предпринимательской или иной деятельности, связанной с использованием привлеченных денежных средств и (или) иного имущества, в объеме, сопоставимом с объемом привлеченных денежных средств и (или) иного имущества.

На наш взгляд, вышеуказанные задачи отражают особенность функционирования «финансовых пирамид», которые за рубежом чаще называются «схемы Понци»³¹. На сегодняшний день в российском законодательстве отсутствует понятие «финансовая пирамида», вместе с тем в 2016 г. УК РФ был дополнен статьей 172.2, предусматривающей наказание за организацию деятельности по привлечению денежных средств и (или) иного имущества. Согласно пояснительной записке³² к законопроекту целью введения новой статьи являлась борьба с «финансовыми пирамидами», ущерб от которых в 2014 г., по данным МВД России, составил 1,7 млрд руб.

Таким образом, на сегодняшний день диспозиция указанной статьи раскрывает понятие и сущность «финансовой пирамиды». При этом ключевым является механизм функционирования «финансовой пирамиды», а именно тот процесс, когда участникам «финансовой пирамиды» выплачивается доход не за счет результатов инвестиционной деятельности компании, а *за счет средств, поступающих от новых участников, причем компанией или лицом не ведется заявленная инвестиционная деятельность в сопоставимом объеме*.

Из вышеизложенного следует, что без назначения судебно-экономической экспертизы установить факты организации «финансовой пирамиды» весьма затруднительно. В особенности, возникают вопросы к *определению полного отсутствия инвестиционной или иной законной экономической деятельности либо наличия такой деятельности, но в объемах, не*

сопоставимых с объемом привлеченных денежных средств. На наш взгляд, вышеуказанное определение носит *оценочный характер*, что значительно усложняет работу экспертов судебно-экономической экспертизы.

Нам также видится, что к вышеперечисленным фактам организации «финансовой пирамиды», подлежащим исследованию, следует отнести операции по перечислению денежных средств с расчетных счетов организации на цели, не связанные с хозяйственной или инвестиционной деятельностью организации. Например, компания — эмитент ценных бумаг после первичного размещения облигаций и привлечения денежных средств граждан перечислила денежные средства на счета фирм-однодневок, хотя согласно проспекту ценных бумаг целью привлечения денежных средств являлось строительство спортивного объекта. Таким образом, движение денежных средств может являться существенным фактом, подтверждающим *отсутствие намерений выполнения обязательств перед инвесторами*.

Подводя итог вышеизложенному, следует отметить, что исследование цифровых следов с точки зрения криминалистически значимой информации актуально не только на сегодняшний день, но на годы вперед. Для успешного противодействия преступлениям на финансовом рынке важно различать виды цифровых следов, это должно помочь в том числе в планировании и приоритизации проверочных мероприятий, успешном изъятии цифровых следов. Проведение судебно-экономических и компьютерно-технических экспертиз при исследовании цифровых следов позволит извлекать криминалистически значимую информацию для следственных органов, которая будет основанием для принятия соответствующих процессуальных решений.

³¹ Понятие «схема Понци» связано с именем итальянского иммигранта в США Чарльза Понци, который в 1919 г. обещал своим вкладчикам выплачивать 40 %-ный доход по депозитам на срок в 45 дней.

³² Законопроект № 881156-6 «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации» // URL: <https://sozd.duma.gov.ru/bill/881156-6> (дата обращения: 16.09.2024).

БИБЛИОГРАФИЯ

1. Гаврилин Ю. В., Бедеров И. С. Установление владельцев криптовалютных кошельков при расследовании преступлений в сфере незаконного оборота наркотических средств : учеб. пособие. — М. : Академия управления МВД России, 2022. — 76 с.
2. Гаврилин Ю. В., Салеева Ю. Е. Развитие учения о криминалистической регистрации в условиях цифровой трансформации преступности // Труды Академии управления МВД России. — 2023. — № 2 (66). — С. 99–105.
3. 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). — С. 105–111.
4. Гужаева В. А., Прокофьева Е. В., Прокофьева О. Ю. Преступность в сети Интернет: криминологические характеристики // Вестник экономической безопасности. — 2019. — № 4. — С. 111–114.
5. Россинская Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2022. — № 2. — С. 27–40.
6. Россинская Е. Р., Сааков Т. А. Проблемы собирания цифровых следов преступлений из социальных сетей или мессенджеров // Криминалистика: вчера, сегодня, завтра. — 2020. — № 3 (15). — С. 106–123.
7. Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы международной научно-практической конференции (19 февраля 2019 г.). — Алматы : Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясының ҒЗжРБЖҰБ, 2019. — С. 6–9.
8. Савицкий А. А. Актуальные задачи и вопросы судебной финансово-экономической экспертизы по делам о банкротстве в уголовном и арбитражном процессах // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2024. — № 3. — С. 64–76.

Материал поступил в редакцию 23 сентября 2024 г.

REFERENCES (TRANSLITERATION)

1. Gavrilin Yu. V., Bederov I. S. Ustanovlenie vladeltsev kriptovalyutnykh koshelkov pri rassledovanii prestupleniy v sfere nezakonnogo oborota narkoticheskikh sredstv: ucheb. posobie. — M.: Akademiya upravleniya MVD Rossii, 2022. — 76 s.
2. Gavrilin Yu. V., Saleeva Yu. E. Razvitie ucheniya o kriminalisticheskoy registratsii v usloviyakh tsifrovoy transformatsii prestupnosti // Trudy Akademii upravleniya MVD Rossii. — 2023. — № 2 (66). — S. 99–105.
3. Gavrilin Yu. V., Shmonin A. V. Ispolzovanie informatsii, poluchennoy iz seti Internet, v rassledovanii prestupleniy ekstremistskoy napravlenosti // Trudy Akademii upravleniya MVD Rossii. — 2019. — № 1 (49). — S. 105–111.
4. Guzhaeva V. A., Prokofeva E. V., Prokofeva O. Yu. Prestupnost v seti Internet: kriminologicheskie kharakteristiki // Vestnik ekonomicheskoy bezopasnosti. — 2019. — № 4. — S. 111–114.
5. Rossinskaya E. R. Teoriya informatsionno-kompyuternogo obespecheniya sudebno-ekspertnoy deyatel'nosti kak novaya chastnaya teoriya sudebnoy ekspertologii // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). — 2022. — № 2. — S. 27–40.
6. Rossinskaya E. R., Saakov T. A. Problemy sobiraniya tsifrovyykh sledov prestupleniy iz sotsialnykh setey ili messendzherov // Kriminalistika: vchera, segodnya, zavtra. — 2020. — № 3 (15). — S. 106–123.
7. Rossinskaya E. R., Ryadovskiy I. A. Kontseptsiya tsifrovyykh sledov v kriminalistike // Aubakirovskie chteniya: materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii (19 fevralya 2019 g.). — Almaty: Kazakstan Respublikasy IIM M. Esbolatov atyndaғы Almaty akademiya synyң ҒЗжРБЖҰБ, 2019. — S. 6–9.
8. Savitskiy A. A. Aktualnye zadachi i voprosy sudebnoy finansovo-ekonomicheskoy ekspertizy po delam o bankrotstve v ugovnom i arbitrazhnom protsessakh // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). — 2024. — № 3. — С. 64–76.