УДК 343.98

Д. А. Свиридов
начальник кафедры уголовного права,
уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

ТИПЫ ЦИФРОВЫХ СЛЕДОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ

Информационные технологии, проникая во все сферы нашей жизни, не только открывают новые горизонты для развития общества и государства, но и ставят перед правоохранительной системой новые задачи. Цифровой прогресс, безусловно, приносит и новые вызовы, ведь злоумышленники умело используют передовые разработки для достижения своих преступных целей. Криминальные организации демонстрируют удивительную способность быстро усваивать новейшие технологии, что, в свою очередь, позволяет им эффективно адаптироваться и эволюционировать в динамичной цифровой экономике.

Чтобы понять, какие цифровые следы чаще всего встречаются в ходе расследований экономических преступлений, нужно сначала разобраться в самом понятии «цифровой след». Согласно одной из распространенных интерпретаций, цифровой след — это вся информация, которая остается в информационной среде [1, с. 79]. Такое определение популярно, так как оно наиболее точно отражает то, как люди обычно понимают цифровые следы в повседневном использовании Интернета. Когда говорят о цифровых следах, обычно имеют в виду информацию, которую люди оставляют в различных онлайн-средах: мессенджерах, интернет-магазинах, почтовых сервисах, мобильных приложениях, на социальных платформах и веб-сайтах. По этой причине выделяют два основных вида цифровых следов: активные и пассивные. Активные следы — это данные, которые пользователь добровольно размещает в цифровых системах во время своей онлайн-деятельности, пассивные следы возникают естественным образом в процессе функционирования программ или систем, не требуя вмешательства пользователя [2].

Определения понятия цифровых следов акцентируют внимание на их генезисе во время взаимодействия с информационно-коммуникационными сетями. Вместе с тем в ходе расследования экономических преступлений необходимо учитывать не только данные, оставленные в Сети, но и широкий спектр электронных финансовых записей и других цифровых отпечатков, которые могут быть созданы вне контекста Интернета и сетевых платформ.

Видится верным использовать определение, данное Е. Р. Россинской и И. А. Рядовским, согласно которому цифровой след определяется как информация, имеющая значение для расследования, которая фиксирует события или

действия, связанные с преступлением, и сохраняется в компьютерных системах во время их создания, обработки, сохранения и передачи [3, с. 7–8]. Некоторые криминалисты рассматривают цифровой след как любую компьютерную информацию, обладающую криминалистическим значением и существующую в форме электрических сигналов, независимо от используемых для ее сохранения, обработки и передачи технологий [4, с. 168]. Это расширяет классическую концепцию цифрового следа, выходя за рамки лишь информационно-коммуникационных сетей и признавая его появление в других электронных пространствах, при этом сохраняя фокус на информационном характере данных.

Бухгалтерский учет в настоящее время преимущественно осуществляется в электронном виде, а автоматизация процессов на предприятиях осуществляется посредством специализированных программных комплексов. Каждая финансовая транзакция фиксируется в базе данных, создаваемой этими программами. Экономические преступления порождают широкий спектр цифровых следов, которые несут в себе ценную доказательственную информацию. К ним относятся компьютерные файлы и базы данных, фиксирующие нюансы бизнес-процессов, историю финансовых операций и транзакций, а также показатели, применяемые для определения налоговой нагрузки и других финансовых показателей.

Популярность интернет-платформ, включая социальные сети, маркетплейсы и онлайн-магазины, в сфере ведения бизнеса неуклонно растет. Однако злоумышленники все чаще выбирают именно этот формат для своих противоправных действий, поскольку он позволяет им сохранить определенную степень скрытности. Хотя преступники и пытаются действовать скрытно, создавая интернет-сайты для своих противоправных целей, они неизбежно оставляют цифровой след. Данные о деятельности на таких сайтах хранятся на серверах, а также могут быть зафиксированы в цифровом виде, например, в виде скриншотов, что позволяет отследить их действия.

Рост популярности криптовалют и электронных валют в экономике как платежных инструментов порождает новые проблемы, обусловленные их специфическими свойствами. Анонимность, децентрализованная природа и скрытность транзакций делают криптовалюты привлекательными для злоумышленников, стремящихся легализовать незаконно полученные средства. Несмотря на то, что противоправные действия в цифровой среде обладают повышенной степенью сложности, они неизбежно оставляют за собой цифровые отпечатки, содержащие критически важные данные для криминалистического расследования.

Чтобы эффективно расследовать преступления в сфере экономики, необходимо повысить квалификацию судебных экспертов, криминалистов и следователей, а также создать инновационные методики анализа цифровых следов.

Ключевым моментом является выявление и изучение различных типов цифровых следов, которые могут раскрыть информацию о совершенных в экономической сфере преступлениях, а также понимание их особенностей и специфики.

Разные подходы к классификации цифровых следов основаны на разнообразных принципах. Например, Е. Р. Россинская предлагает группировать их по их местоположению в хранилище:

– на носителях;

– в компьютерных системах и сетевых коммуникациях.

Во время работы с цифровыми следами часто требуется создавать и применять образы для их запечатления и последующего изучения. В этом контексте Е. Р. Россинская классифицирует образы на два типа: цифровые, получаемые с помощью программных инструментов (такие как скриншоты веб-страниц), и физические, создаваемые в печатном виде (например, распечатки электронных документов) [5, с. 46].

В ходе исследования были выявлены ключевые типы цифровых следов, обладающие высокой информационной значимостью для расследования и пресечения экономических преступлений:

1. Цифровые и печатные носители финансовой и бухгалтерской документации.

2. Данные, собранные с разных интернет-ресурсов, отражающие деятельность по организации и осуществлению нелегальной торговли, например, скриншоты интернет-площадок, информация из баз данных серверов и аналогичные материалы.

3. Данные, полученные из мессенджеров и социальных сетей, могут иметь существенное значение для расследования, так как в них могут быть зафиксированы сведения о денежных переводах и коммерческих сделках.

4. Информация о финансовом благосостоянии лиц, находящихся под подозрением.

В расследованиях экономических преступлений ключевое значение имеют цифровые следы, отражающие совершенные операции. Особую значимость в этом контексте представляют электронные бухгалтерские отчеты и их электронные копии, созданные путем сканирования бумажных носителей. Важно отметить, что эти копии могут быть обеспечены электронной подписью, что повышает их достоверность, или же существовать без такой подписи. В отличие от электронных документов, генерируемых в цифровом пространстве и обеспеченных защитой цифровой подписи, электронные копии бумажных документов лишь имитируют их бумажный оригинал в цифровом виде.

При расследовании уголовных дел, связанных с нелегальным ведением бизнеса онлайн, особое внимание уделяется специфике цифровых следов. Ключевым моментом здесь становится изъятие и изучение данных, оставленных

при организации и функционировании интернет-магазинов без разрешительных документов. Например, скриншоты интернет-страниц могут служить неоспоримым доказательством совершения торговых операций.

Анализ и классификация цифровых следов при расследовании экономических преступлений играют ключевую роль. Это необходимо не только для выработки специализированных методик расследования различных категорий преступлений, но и для создания фундаментальных основ криминалистики в области цифровых следов. Цифровые следы охватывают не только данные, генерируемые в информационно-коммуникационных сетях, но и любую компьютерную информацию, имеющую криминалистическое значение, независимо от того, была ли она создана в рамках сетевых технологий или нет. В расследовании преступлений ключевое значение имеют электронные бухгалтерские записи, информация, публикуемая на интернет-платформах, данные о банковских операциях, а также сведения, полученные из серверов регистрации, используемых злоумышленниками для своих целей.

Для эффективного выявления цифровых следов ключевым шагом является изыскание и последующее изъятие носителей данных, где сосредоточены электронные бухгалтерские записи, информация о финансовых и операционных действиях, учетные данные для доступа к веб-сайтам и приложениям, а также скриншоты с криминалистически важными данными.

1. Бояркина Л. А., Бояркин В. В. Цифровой след и цифровая тень как производные персональных данных // Safety of a person and society as a problem of social sciences and humanities : materials of the III international scientific conference, December 5–6, 2016. Prague: Sociosféra-CZ, 2016. P. 78–81. Вернуться к статье

2. Буйнов Д. О. Виды цифровых следов преступлений в сфере экономической деятельности и особенности их исследования экспертом [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/vidy-tsifrovyh-sledov-prestupleniy-v-sfere-ekonomicheskoy-deyatelnosti-i-osobennosti-ih-issledovaniya-ekspertom/viewer (дата обращения: 05.04.2025). Перейти к источнику Вернуться к статье

3. Россинская Е. Р., Рядовский И. А. Концепция цифровых следов в криминалистике // Аубакировские чтения : материалы Междунар. науч.-практ. конф., Алматы, 19 февр. 2019 г. Алматы, 2019. С. 6–8. Вернуться к статье

4. Цифровые следы преступлений : моногр. / А. М. Багмет [и др.]. М. : Проспект, 2021. 244 с. Вернуться к статье

5. Теория информационно-компьютерного обеспечения криминалистической деятельности : моногр. / под ред. Е. Р. Россинской. М. : Проспект, 2022. 256 с. Вернуться к статье