DOI: http://dx.doi.org/10.21686/2411-118X-2024-1-77-82

Цифровые технологии, детерминирующие формирование специфики следов незаконного оборота поддельных денег, ценных бумаг и иных средств платежа (ст. 186, 187 Уголовного кодекса Российской Федерации)

С. Н. Ефимов
адъюнкт кафедры управления органами расследования
Академии управления МВД России.
Адрес: ФГКОУ ВО «Академия управления Министерства внутренних дел Российской Федерации»,
125993, Москва, ул. Зои и Александра Космодемьянских, д. 8.
E-mail: lehperson@yandex.ru

Digital Technologies that Determine the Formation of the Specifics of Traces of Illegal Circulation of Counterfeit Money, Securities, and Other Means of Payment (Articles 186, 187 of the Criminal Code of the Russian Federation)

S. N. Efimov
Postgraduate Student of the Department of Management of the Investigation Bodies
of the Academy of Management of the MIA of Russia.
Address: Federal State Public Educational Establishment of Higher Education
«Management Academy of the Ministry of the Interior of the Russian Federation»,
8 Zoya and Alexander Kosmodemyanskikh Str.,
Moscow, 125993, Russian Federation.
E-mail: lehperson@yandex.ru

Аннотация

В статье рассматриваются основные цифровые технологии, детерминирующие специфику образования следов незаконного изготовления хранения, перевозки или сбыта поддельных денег или ценных бумаг, а также неправомерного оборота средств и платежей. При этом обращается внимание на виды следов как специфической формы преобразования компьютерной информации, реализуемой в экономической сфере. Рассматриваются особенности таких материальных следов, которые преимущественно образуются в результате отсутствия непосредственного визуального контакта лиц, вовлеченных в противоправную деятельность. Местом нахождения виртуальных следов являются компьютерно-технические средства и телекоммуникационные сети. Указывается, что данные следы (в силу специфических свойств) достаточно длительное время могут оставаться в этих самых средствах и сетях, даже в тех случаях, когда предпринимаются активные действия, направленные на их уничтожение. При этом отмечается, что деятельность, направленная на уничтожение цифровых следов, порождает новые, аналогичные следы. В статье говорится об особенностях процессов, происходящих внутри компьютерно-технических средств и технологий, находящихся за пределами человеческого восприятия, специфике отображения указанных следов на материальных носителях, делающих следы пригодными для выявления, сбора, обработки и хранения.

Ключевые слова: цифровизация, компьютеризация, платежные карты, подделка, распоряжения о переводе денежных средств.

Abstract

The article discusses the main digital technologies that determine the specifics of the formation of traces of the illegal production, storage, transportation or sale of counterfeit money or securities, as well as the illegal circulation of funds and payments are considered. At the same time, attention is drawn to the types of traces as a specific form of transformation of computer information implemented in the economic sphere. It talks about the features of such material traces, which are mainly formed as a result of the lack of direct visual contact of persons involved in illegal activities. The location of virtual traces is computer hardware and telecommunication networks. It is indicated that these traces (due to their specific properties) can remain in these very means and networks for quite a long time, even in cases where active measures are taken to destroy them. It is noted that activities aimed

at destroying digital traces generate new, similar traces. The article talks about the features of the processes occurring inside computer hardware and technologies that are beyond the limits of human perception, the specifics of displaying these traces on material media, making the traces suitable for identification, collection, processing and storage

Keywords: digitalization, computerization; payment cards; fake; instructions for transfer of funds.

Вступительная часть

В период всеобщей компьютеризации и цифровизации[1] соответствующие этим процессам средства и технологии находят проявление во всех сферах общественной жизни, особенно в сферах и отраслях, связанных с большим объемом документооборота. К числу таковых относятся экономическая сфера и ее разновидности – финансово-экономическая и кредитно-финансовая, где цифровые технологии и компьютерные средства обеспечивают обработку огромного количества бухгалтерских операций и расчетов. Результатом их применения являются не только некоторые показатели, необходимые для принятия определенных хозяйственных, экономических решений, но и электронные, цифровые, компьютерные следы. Аналогичные последствия сопровождают применение цифровых технологий и компьютерных средств, если в рассматриваемых сферах осуществляется противоправная деятельность. Другими словами, способы совершения операций, орудия и средства, применяемые для их реализации, в полной мере детерминируют процесс образования следов преступлений в сфере кредитно-денежной системы или ценных бумаг, а также при использовании иных средств платежа.

Официальная статистика свидетельствует о том, что в 2022 г. в России было совершено 111 429 преступлений экономической направленности. Каждое четвертое из них – в финансовой сфере, размер материального ущерба (по оконченным и приостановленным уголовным делам) составил 339,1 млрд руб.[2] Риски криминализации финансового рынка, по мнению Генерального прокурора Российской Федерации И. В. Краснова, «…продолжают возрастать в связи с активным применением информационно-телекоммуникационных технологий, трансформацией экономики…», «…проблему представляет противоправная деятельность руководителей и работников кредитных организаций, в том числе микрофинансовых…»[3].

Исследовательская часть

Акцентируя внимание на специфике обозначенной противоправной деятельности, ее результатах, особенностях используемых средств и технологий, образующихся при этом следах, считаем целесообразным первоначально классифицировать следы на идеальные и материальные, так как это традиционно принято в криминалистике и в полной мере имеет отношение к преступлениям, предусмотренным статьями 186, 187 Уголовного Кодекса Российской Федерации.

Специфика рассматриваемых видов противоправной деятельности позволяет говорить о том, что лица, вовлеченные в преступную деятельность, могут не контактировать между собой, а в случаях совершения преступлений при использовании иных средств платежа такие контакты вообще не требуются. Это исключает образование идеальных следов. Основную массу следов по таким видам преступлений будут составлять материальные следы. По нашему мнению, следует рассмотреть указанные виды следов, учитывая их количественную и качественную составляющие. Наиболее распространенными по делам данной категории являются материальные следы, при этом следует указать на один из сравнительно «новых» их видов (который можно вообще выделить в отдельную группу) – компьютерные следы. По части их определения продолжают дискутировать ученые и специалисты-практики.

Анализ судебно-следственной практики позволяет говорить о том, что наибольшее количество следов по преступлениям в сфере кредитно-денежной системы, ценных бумаг и иных средств платежа находится в компьютерно-технических средствах и телекоммуникационных сетях.

[1] О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации»: Постановление Правительства Российской Федерации от 2 марта 2019 г. № 234. – URL: https://base.garant.ru/72190034/

[2] Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития. Аналитический обзор. – М., 2023.

[3] Генпрокурор РФ назвал причины низкой раскрываемости преступлений на финрынке. – URL: https://www.interfax.ru/business/884429

Отсюда вывод – основным видом следов будут являться компьютерно-технические (виртуальные) следы. Обусловлено это еще и тем, что указанные следы имеют свойство достаточно длительное время оставаться в этих самых средствах и сетях даже в тех случаях, когда предпринимаются активные действия, направленные на их уничтожение. Парадоксальность ситуации заключается в том, что деятельность, направленная на уничтожение цифровых следов, порождает новые, аналогичные следы, и так до бесконечности. Но есть проблема: их сложно отыскать и надлежащим образом изъять для того, чтобы в последующем использовать для исследования и изобличения преступников.

Классификация и дифференциация следов в криминалистике эволюционируют и в зависимости от этапов развития научно-технического прогресса. Это закономерное явление. В полной мере по такому пути идет процесс эволюции компьютерных следов. Чем больше у специалистов следственных и правоохранительных органов появляется возможностей поиска, выявления, обнаружения и изъятия компьютерных следов, тем больший их объем фигурирует в качестве доказательств. Закономерно, что по мере развития самих информационных технологий их присутствие в уголовном судопроизводстве будет возрастать. Это не значит, что ранее таких следов в компьютерном (виртуальном) пространстве не существовало. Скорее, не было технических возможностей, рекомендаций работы с ними. Можно предполагать, что и в дальнейшем, в ходе научно-технического прогресса и в процессе расширения использования компьютерных средств и технологий, объем работы с цифровыми следами будет увеличиваться, равно как и классификационная составляющая (научная мысль не будет стоять на месте).

Применительно к настоящему времени дискуссия относительно самостоятельности компьютерных (виртуальных, бинарных, компьютерно-технических, электронных, электронно-цифровых) следов в криминалистике и следственной практике периодически активизируется. Безусловно, существование таких следов не подлежит сомнению, однако не ослабевает спор об их отнесении к указанным ранее видам следов, об их формировании в самостоятельную группу [1. – С. 40–46; 3; 4. – С. 49–55; 9]. Причина дискуссии обусловлена спецификой самого процесса следообразования, системой средств и методов их поиска, выявления, изъятия, обработки и сохранения. Специфические особенности образования следов позволяют ученым и специалистам по-разному определять обозначенное явление, начиная с отрицания материальной среды как таковой. Так, высказывается комбинированная точка зрения, которая заключается в том, что отличительной особенностью механизма виртуального следообразования является не материальная, а искусственно созданная среда (виртуальное пространство). Доступ в это пространство возможен «…лишь при наличии технических устройств и специальных познаний, где также возможно свое деление по отраслям, видам и подвидам» [2. – С. 128–133]. Представляется, что данная позиция вряд ли бесспорна.

Чтобы получить ответы на поставленные вопросы и прояснить затронутые проблемы, следует обратиться к основополагающим дефинициям. В. Б. Вехов, рассматривая компьютерную информацию, определяет ее как «…сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов» [2. – С. 71]. При этом ученый отмечает, что «…такие следы являются материальными невидимыми следами. В основе механизма их образования лежат электромагнитные взаимодействия двух и более материальных объектов – объективных форм существования компьютерной информации. При этом между объектами следообразования отсутствует непосредственный механический контакт, поскольку изменение их внутренних свойств осуществляется с помощью электромагнитных сигналов и полей, имеющих конкретные материальные признаки: частоту, напряженность, направленность, время существования» [2. – С. 84].

В. А. Мещеряков считает указанные следы «виртуальными, […] под которыми понимаются любые изменения состояния автоматизированной информационной системы (образованного ею “кибернетического пространства”), связанные с событием преступления и зафиксированные в виде компьютерной информации (информации, пригодной для машинной обработки) на материальном носителе, в т. ч. на электронно-магнитном поле». По его мнению, «виртуальные следы» занимают промежуточное положение между идеальными и материальными следами [9. – С. 102–104]. При-

мерно аналогичной позиции придерживается Е. С. Лапин, говорящий о «…сложной, идеально-материальной природе цифровых следов»[1].

По мнению В. О. Давыдова и А. Ю. Головина, виртуальные следы представляют собой зафиксированное в виде цифрового образа формальной модели изменение состояния информации в памяти абонентских электронных устройств (терминалов, биллинговых систем), вызванное алгоритмом установленного программного обеспечения и связанное с событием преступления (имеющее уголовно-релевантное значение). А механизму подобного следообразования, по мнению этих же авторов, присущи следующие стадии: физическое проявление свойств следообразующих объектов (изображение, цифровой набор данных, температура, отсчеты времени, звук); преобразование исходной физической формы проявления следообразующего объекта в цифровую форму (аналогово-цифровое преобразование); предварительная обработка, передача и хранение полученной цифровой информации [6. – С. 254–259].

Вероятно, целесообразнее всего говорить о процессах, происходящих внутри компьютерно-технических средств и технологий, находящихся за пределами человеческого восприятия (хотя сам процесс известен), обусловливающих особенности отображения указанных следов на материальных носителях и делающих следы пригодными для выявления, сбора, обработки и хранения. Определяющее значение, по нашему мнению, играют механизм отображения рассматриваемых следов и их процессуальное изъятие для последующего использования в уголовном судопроизводстве.

Наличие различных подходов к определению цифровых, компьютерных следов обусловлено характером функционирования компьютерно-технических средств и технологий, что послужило поводом для формирования оснований классификации указанных следов. Так, А. Г. Волеводз предложил классифицировать виртуальные следы по виду материального носителя информации, на основании которого выделить:

– следы на жестком диске (винчестере), магнитной ленте (стримере), оптическом диске (CD, DVD), на дискете (флоппи-диске);

– следы в оперативных запоминающих устройствах (ОЗУ) ЭВМ;

– следы в оперативных запоминающих устройствах периферийного оборудования (принтеры, сканеры и т. д.);

– следы в оперативных запоминающих устройствах компьютерного оборудования связи и сетевого оборудования;

– следы в проводных, радиооптических и других электромагнитных системах и сетях связи [3. – С. 159–160].

Работники-практики правоохранительных органов предлагают несколько иные основания для выделения видов виртуальных следов. По мнению М. М. Льянова, наиболее значимым является их деление в зависимости от:

– электронного носителя информации, на котором содержится виртуальный след;

– местонахождения электронного носителя информации с содержащимися на нем виртуальными следами;

– структуры и содержания информации, которая хранится в виртуальном следе [7. – С. 97–106].

В принципе, соглашаясь с наличием и выделением отдельной группы следов, называемых виртуальными, А. О. Насимова и А. А. Рыхлов указывают на необходимость уточнения признаков, с помощью которых можно определить сущность этого явления. По мнению ученых, эти следы можно отнести к таковым, если они:

– скопированы на другие устройства без потери свойств (копирование файла на флэш-карту, онлайн-диск);

– не имеют материального воплощения следообразующего объекта, но являются материальными, поскольку имеют особую форму отображения в виде цифрового образа, содержащегося на материальном носителе или в киберпространстве;

– формируются в результате преобразования компьютерной информации;

– не могут формироваться без электронного носителя [10. – С. 124–128].

Виртуальные следы как специфическая форма преобразования компьютерной информации должны обладать комплексом признаков. При их наличии, как считают Ю. В. Гаврилин и В. В. Шипилов, они:

1) отражают событие преступления в информационном поле;

[1] Лапин Е. С. Философия криминалистики: учеб. пособие для вузов. – 2-е изд., испр. и доп. – М. : Юрайт, 2016. – С. 88–89.

2) являются материальными по своей природе, но не отражают пространственную форму следообразующего объекта;

3) выступают результатом преобразования компьютерной информации;

4) служат носителями свойств, присущих компьютерной информации;

5) обладают способностью к дублированию, т. е. к копированию на другие электронные носители без изменения их характеристик [5. – С. 2–6].

Наиболее упрощенно процесс функционирования операционной системы компьютерно-технических средств, технологий и сетей можно представить в общем виде, где следы деятельности отображаются в свойствах самого файла или различных журналах, которые располагаются в памяти постоянных запоминающих устройств (ПЗУ). Такое устройство находится, как правило, на системной плате и является неотъемлемой частью компьютерно-технического средства. Кроме этого, там же находится оперативное-запоминающее устройство (ОЗУ), встроенное в системную плату. Данные устройства являются стационарными для компьютера и отвечают за все процессы, происходящие в компьютере, однако при этом являются всего лишь техническими устройствами («железом»).

Для возможности функционирования указанных устройств и поддержания их работоспособности необходима установка операционной системы и программного обеспечения. Сегодня наиболее распространенными операционными системами являются Windows, Android, iOS, Ubuntu, macOS, Fedora, Solaris, Free BSD, Chrome OS и др.

По мнению специалистов, существует три вида программного обеспечения: Linux, Microsoft Windows и Apple Mac OS. Справедливости ради укажем, что все перечисленные операционные системы и программное обеспечение являются зарубежными продуктами, и, исходя из сложившейся обстановки, предложения по их совершенствованию вряд ли появятся. Поэтому в условиях современных реалий жестких санкций прогнозируем появление новых продуктов, которые будут предложены отечественными производителями.

Кроме этого, существенную роль в процессе функционирования компьютерно-технических систем и технологий играют внешние запоминающие устройства (ВЗУ), не входящие в стационарную систему компьютера, однако обладающие техническими свойствами, направленными на сохранение информации путем копирования. Это различные флеш-накопители (флешки), жесткие диски.

Необходимо также сказать, что для функционирования телекоммуникационных сетей существуют свои операционные системы, разработанные непосредственно для обеспечения работоспособности серверных сетей и коммуникаций. Они предназначены для работы и обслуживания неограниченного количества пользователей в целях раздела между ними программных и аппаратных ресурсов (Unix, Linux, Windows XP Professional, Windows 2000). Именно на основе указанных операционных систем функционируют интернет-провайдеры, предоставляющие доступ к сети. Весь механизм следообразования определяется функциональными разрешениями и способностями указанных технических устройств и телекоммуникационных сетей. Любое действие на компьютере осуществляется посредством проведения операции, которая перерабатывает определенный вид и объем информации (в том числе включение или выключение компьютера, создание или уничтожение файла.). Все типы и виды операций находят отражение в памяти компьютера посредством записи их в различных журналах (журнал безопасности, журнал администрирования). Действия с системными файлами находят отражение в реестре компьютера в reg-файлах. Аналогичным образом все действия и операции в сети Интернет, а также иных сетях сосредотачиваются, отражаются и аккумулируются в log-файлах.

Указанные следы, исходя из информационной процедуры, отражаются в рабочих записях, протоколах антивирусных программ, самом программном обеспечении и различных каталогах. Схематично эта процедура, по мнению С. В. Чубейко, включает «…временные файлы операционной системы Windows, располагающиеся в следующем каталоге: %SystemRoot%\Temp. В Unix-подобных операционных системах, временные файлы могут находиться в специальной папке /tmp, которая располагается в корневом каталоге. Сотрудникам полиции необходимо обращать внимание на хранение данных в программе Microsoft Word, являющейся наиболее распространенной программой для создания текстовых документов. Данная программа имеет папку для автосохранения «C:\Users\User\ AppData\Roaming\Microsoft\Word\» и папку для

расположения локальных файлов по умолчанию «C:\Users\User\Documents\» [12. – С. 117–122].

Заключительная часть

По нашему мнению, сам процесс взаимодействия двоичного кода в системе его преобразования посредством технических средств и технологий не представляет интереса для процесса ретроспективного познания субъектом расследования объективной действительности, связанной с познаваемым событием. Ключевое значение в этом играет объективная картина, выразившаяся в наличии пригодных для восприятия материальных объектов, которые имеют доказательственное значение и возможность их физического восприятия и обработки.

Отметим, что применение специальных знаний невозможно без понимания сведущим лицом всего процесса, протекающего внутри компьютерно-технической системы или технологии. Но это уже специфическое знание, которое в полном объеме вряд ли доступно для усвоения следователем. Именно в этом аспекте, как представляется, обусловлены различные взгляды на систему и классификацию компьютерно-технических следов. Бесспорно, указанные следы на современном этапе играют огромную, если не основную, роль в расследовании любого преступления. Особенно тех, где активно применяются компьютерно-технические средства и технологии. В полной мере, как позывает практика, это относится к преступлениям, предусмотренным статьями 186, 187 Уголовного кодекса Российской Федерации. При их совершении незаконно применяются различные средства платежа, изготавливаются поддельные денежные купюры, ценные бумаги и иные материальные объекты кредитно-финансовой системы. Учитывая характер указанной преступной деятельности, можно констатировать, что использующиеся при ее осуществлении компьютерно-технические средства и технологии следует рассматривать и как орудия и средства совершения преступления, и как источники следов данной преступной деятельности.

Список литературы

1. *Вехов В. Б.* «Электронная криминалистика»: понятие и система // Криминалистика: актуальные вопросы теории и практики : материалы междунар. науч.-практ. конф. – Ростов н/Д, 2017. – С. 40–46.

2. *Вехов В. Б.* Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки : монография. – Волгоград: ВА МВД России, 2008.

3. *Волеводз А. Г.* Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М. : Юрлитинформ, 2002.

4. *Гаврилин Ю. В., Лыткин Н. Н.* Понятие, свойства и криминалистическое значение компьютерно-технических следов преступления // Вестник криминалистики / отв. ред. А. Г. Филиппов. – Вып. 4 (16). – М. : Спарк, 2005. – С. 49–55.

5. *Гаврилин Ю. В., Шипилов В. В.* Особенности следообразования при совершении мошенничеств в сфере компьютерной информации // Российский следователь. – 2013. – № 23. – С. 2–6.

6. *Давыдов В. О., Головин А. Ю.* Значение виртуальных следов в расследовании преступлений экстремистского характера // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3-2. – С. 254–259.

7. *Льянов М. М.* Процесс обнаружения виртуальных следов при расследовании преступлений // Юридическая наука и правоохранительная практика. – 2021. – № 4 (58). – С. 97–106.

8. *Мещеряков В. А.* Основы методики расследования преступлений в сфере компьютерной информации : автореф. дисс. … д-ра юрид. наук. – Воронеж, 2001.

9. *Мещеряков В. А.* Основы методики расследования преступлений в сфере компьютерной информации : дисс. … д-ра юрид. наук. – Воронеж, 2001.

10. *Насимова А. О., Рыхлов А. А.* Виртуальные следы в криминалистике // Сфера знаний: научное взаимодействие в рамках образовательного процесса: сб. науч. трудов. – Казань: ООО «СитИвент», 2018. – С. 124–128.

11. *Переверзева Е. С., Комов А. В.* Механизм следообразования виртуальных следов // Вестник Санкт-Петербургского университета МВД России. – 2022. – № 1 (93). – С. 128–133.

12. Чубейко С. В., Черкасов Р. И., Дьяченко П. Е. Противодействие сокрытию информационных следов при совершении преступлений // Философия права. – 2020. – № 3 (94). – С. 117–122.