ТАКТИКА ОСМОТРА ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Р.Р. Галяутдинов, *канд. юрид. наук, ассистент*
В.А. Коваленко, *студент*
Башкирский государственный университет
(Россия, г. Уфа)

DOI:10.24412/2500-1000-2022-10-3-58-62

Аннотация. *Целью настоящей статьи является определение общей тактики осмотра электронных документов. Для этого дается краткая характеристика электронных документов, а также краткое описание осмотра как следственного действия. Приводятся первоначальные шаги при осмотре электронных документов, подчеркивается значимость привлечения к осмотру специалиста. В заключительной части научной статьи предоставляется общий перечень тактических правил, которые рекомендовано соблюдать при осмотре электронных документов.*

Ключевые слова: *электронные документы, следственный осмотр, осмотр электронных документов, тактика осмотра электронных документов, виды электронных документов.*

Вот уже на продолжении длительного времени наблюдается интенсивная цифровизация общества, итогом которой, помимо прочего, становится активное внедрение электронных документов. Достоинства электронных документов в сравнении с традиционными являются неоспоримыми. Электронные документы легче хранить, передавать (поскольку они не имеют привязки к одному единственному материальному носителю), а также редактировать. Однако такие преимущества могут быть использованы не только добросовестными субъектами документооборота, но и представителями преступного сообщества. Причем преступники, которые в ходе совершения преступлений обращаются к электронным документам, зачастую обладают развитыми навыками по сокрытию преступлений, что может затруднять процесс расследования преступлений. Для того чтобы преодолеть противодействие расследованию преступлений, где фигурируют электронные документы, сотрудники должны быть хорошо осведомлены о тактике осмотра электронных документов.

Отметим, что законодатель в п. 11.1 ст. 2 Федерального закона от 27.07.2006 N149-ФЗ «Об информации, информационных технологиях и о защите информации» определил понятие электронного документа, которое звучит следующим образом: «электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах» [1].

Легальное определение электронных документов не раскрывает вопрос, заключающийся в том, что же стоит относить к электронным документам. При этом мнения исследователей на данный счет разнятся.

Например, С.А. Стяжкина полагает, что к электронным документам относятся официальные документы, т.е. те из них, которые удостоверяют юридически значимые факты [2, с. 179].

Однако нельзя не отметить, что легальное определение понятия «электронный документ» не включает в себя формулировки «официальный», «юридически значимый» и т.д. В связи с этим хотелось бы высказать точку зрения, согласно которой в рамках уголовно-процессуального права в качестве электронных документов могут выступать не только официальные документы, но и информация, не являющаяся юридически значимой, но, тем не менее,

наделенная доказательственным значением.

Так, в п. 6 ч. 2 ст. 74 УПК РФ сказано, что в качестве доказательств по уголовному делу могут выступать «иные документы» [3]. Данную формулировку можно оценить как достаточно широкую, т.е. она не ограничивается сугубо официальными документами.

Кроме того, правоприменительная практика свидетельствует о том, что переписки в сети Интернет, скриншоты социальных сетей, данные видеокамер и т.п. могут признаваться судом в качестве документов, имеющих доказательственное значение.

Так, Ленинским районным судом г. Смоленска было рассмотрено уголовное дело, возбужденное в отношении Горчакова В.М. по ч. 2 ст. 159 УК РФ. Мошеннической деятельность обвиняемый вел с использованием информационно-телекоммуникационных технологий, в связи с чем им были оставлены цифровые следы. В результате в качестве доказательств по делу проходили такие документы, как sms-переписка, а также DVD-R диск, на котором содержалась информация с детализацией телефонных соединений обвиняемого [4].

Благодаря случаю из правоприменительной практики, описанному выше, становится ясным, что в настоящее время суды расценивают разного рода информацию, представленную в электронном виде, как электронные документы, на что напрямую указывается в материалах соответствующих уголовных дел.

Отдельное внимание стоит заострить на цифровых следах, которые остаются в ходе создания и использования электронных документов. Можно сказать, что при создании разного рода данных, которые могут быть расценены судом как электронный документ, преступник одновременно способствует созданию цифровых следов. Отметим, что наиболее подходящим в уголовно-процессуальном, криминалистическом смысле представляется определение, содержащееся в научной статье Д.О. Буйнова, следуя котором под такими следами можно понимать «криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [5, с. 292].

Таким образом, ход и создания, и использования, и передачи электронных документов сопровождается формированием цифровых следов, на основании которых следственные органы могут определить дальнейшие пути расследования преступления, либо заявить о причастности лица к совершению преступления.

Таким образом, актуальность изучения тактики осмотра электронных документов можно обосновать тем, что без его грамотной организации могут быть упущены сведения, имеющие важное доказательственное значение.

Прежде чем конкретизировать тактические шаги по отношению к осмотру электронных документов хотелось бы кратко охарактеризовать осмотр как следственное действие.

Осмотр производится при расследовании практически всех категорий преступлений, благодаря чему следователь может получить существенный объем информации по делу. Можно сказать, что суть обозначенного следственного действия сводится к поиску улик, на основании которых возможно установить события преступления, а также лиц, причастных к нему [6, с. 286]. Примечательно, что производство осмотра, в том числе документов, допускается до момента возбуждение уголовного дела, что определяется в ч. 2 ст. 176 Уголовно-процессуального кодекса РФ [3].

Как утверждает А.А. Шурыгин, с позиций криминалистики значение имеет не только электронный документ, но и носитель информации, на котором он может быть расположен. По этой причине в криминалистической науке принято классифицировать электронные документы на различные группы [7].

В качестве примера можно привести следующую классификацию электронных документов:

1. На основании формы существования: виртуальные и материальные. В число ма-

териальных документов относят объекты, зафиксированные на электронных носителях, несущие в себе информацию, которая наделена смысловым содержанием и существует только в электронной среде. Виртуальный документ являет собой совокупность информационных объектов, образованных в итоге взаимодействия пользователя с информационной системой.

2. На основании содержания: документы, в содержании которых содержится текстовая информация, графика, видео- или фотозапись и т.п.

3. На основании степени защищенности: закрытые и открытые.

4. На основании типа материального носителя: документы, размещенные на физических носителях компьютерной информации (устройства внешней памяти, например, такие, как жесткие диски, флеш-накопители и т.п.); документы, размещенные в оперативном запоминающем устройстве (далее – ОЗУ) электронной вычислительной машины; документы, размещенные в ОЗУ периферийных устройств; документы, размещенные в ОЗУ компьютерных устройств связи и сетевых устройств [7].

Вышеизложенное позволяет сделать вывод, что тактика осмотра электронных документов характеризуется двойственным характером. С одной стороны, значение имеет форма материального носителя, на котором расположен тот или иной электронный документ. С другой стороны, важной доказательственной ролью наделяется информация, размещенная в самом электронном документе.

Подтверждение указанной позиции возможно обнаружить в научной статье А.Ю. Самойлова, который пишет, что один носитель информации, представляющий интерес для следователя, обладает двойственной криминалистической природой, первая из которых определяется наличием материальных следов, а вторая – наличием электронно-цифровых. Электронная информация в таком случае предстает электронное доказательство, имеющее под собой основу в виде электронных документов [8, с. 97].

Определяя тактику осмотра электронных документов, укажем, что на начальном этапе расследования будет неизвестно, какие именно из документов обладают доказательственным значением. В связи с этим сотрудники должны производить осмотр всего объема электронных документов, которые потенциально могут быть уликами [9, с. 81].

Г.В. Борисов считает, что в качестве особенности осмотра электронных документов можно назвать тот факт, что практически всегда при таком следственном действии обоснованным будет являться привлечение специалистов, обладающих специальными знаниями, т.е. без их содействия следователи могут оказаться в затруднительном положении при поиске, верном изъятии, а также закреплении следов преступления. Задачи, возлагаемые на специалистов, характеризуются разноплановым характером, что связана с их множеством. В связи с этим специалисты должны обладать обширным спектром знаний в сфере ценных бумаг, бухгалтерского учете, налогообложения, компьютерной техники и т.п. [9, с. 82].

С.В. Кержеманкин также пишет, что задействование специалистов по работе с электронными документами при обыске является частой мерой. Помощь специалистов позволяет правильно извлечь электронные документы, сохранить целостность содержащихся в них данных, предоставить их полное и точное описание, сформулировать вопросы для экспертов по поводу их подлинности и т.д. [10, с. 84]

Таким образом, в силу специфику электронных документов, важным тактическим мероприятием при их осмотре выступает привлечение специалиста, способного повысить эффективность следственного действия. В противном случае могут возникнуть угрозы, связанные как с безвозвратной утерей, так и с их необнаружением. Причем наличие именно таких угроз отличает осмотр электронного документа от традиционного, т.е. бумажного.

После прибытия на место предполагаемого изъятия электронных документов необходимо получить информацию об изымаемых объектах, например, такую,

как пароли, логины, структуру сетевого взаимодействия, возможность копирования информации и др. Осуществить сбор такой информации возможно при помощи обращения к владельцу электронного информационного носителя либо к штатному специалисту при изъятии соответствующего носителя у юридического лица [10, с. 118].

В ходе изъятии информации специалист должен опираться на самый эффективный способ извлечения в рамках каждого конкретного случая: изъятие вместе с электронным носителем информации (сервером) либо копирование информации. При этом можно рекомендовать производить изъятие электронной информации, расположенной на электронных носителях совместно с сервером [11, с. 118].

Отдельного внимания требует вопрос тактики осмотра тех электронных документов, которые были заверены усиленной квалифицированной электронной подписью (далее – УКЭП). В ходе осмотра таких документов следователи тщательно должны изучить вопросы наличия УКЭП. Это подразумевает, что осмотр должен быть реализован с использованием особого программного обеспечения, благодаря которому определяется достоверность УКЭП [3].

Бывают ситуации, когда при осмотре электронных документов были установлены признаки изменения их персонального содержания. В таком случае следователю надлежит обратить внимание на некоторые моменты.

В случае выявления фактов подлога электронных документов следователь в ходе осмотра должен обратить внимание на следующе:

1. На время создания данного электронного документа.

2. На дату и время внесения изменений в документ, на количество изменений.

3. На содержание внесенных изменений (возможно установить путем сравнения исследуемого документа с более ранними его вариантами, методом восстановления удаленной информации и др.

4. На наличие прошлых вариантов документа, которые с некоторой вероятностью могут быть расположены в архивных папках, в «корзине» и т.д.

5. На наличие резервных копий документа.

6. Сопоставить текст электронного документа с имеющими распечатанными документами, с имеющимися образцами [7, с. 84].

В целом можно выделить следующий общий комплекс тактических особенностей осмотра электронных документов:

1. На первоначальном этапе расследования осмотру должен подлежать значительный объем электронных документов, т.к. зачастую неизвестно, в каком именно документе может содержаться информация, имеющая доказательственное значение.

2. К осмотру необходимо привлечение специалистов, способных осуществить эффективный поиск электронных документов, их изъятие, а также (в отдельных случаях) – восстановление после удаления документов преступником.

3. Осмотр должен быть произведен как в отношении самого электронного носителя документа, так и в отношении информации, содержащейся непосредственно в тексте электронного документа.

4. Электронный документ должен быть проверен на соответствие возможным признакам подлога.

В заключение можно сделать вывод, что тактика осмотра электронных документов предполагает осмотр как, собственно, материальных носителей электронных документов, таки и содержания самих документов. Безусловно, специфика осмотра электронных документов зависит от конкретного преступления, подлежащего расследованию, он первоначальной следственной ситуации. Тем не менее существуют общие тактические правила осмотра электронных документов, соблюдение которых является обязательным. Кроме того, в ходе осмотра электронных документов необходимо брат в расчет угрозы, связанные с вероятностью его утраты. В целях предотвращения таких угроз может понадобиться помощь специалиста, обладающего специальными знаниями.

Библиографический список

1. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 14.07.2022) // Российская газета. N 165. 29.07.2006.
2. Стяжкина С.А. Электронный документ как предмет уголовно-правовой охраны // Вестник удмуртского университета. – 2022. – №1. – С. 178-184.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 24.09.2022) // Российская газета. N 249. 22.12.2001.
4. Приговор № 1-360/2019 от 17 декабря 2019 г. по делу № 1-360/2019 // Судакт. – [Электронный ресурс]. – Режим доступа: //sudact.ru/regular/doc/fFHQgl7OP668/ (дата обращения 19.10.2022).
5. Буйнов Д.О. Цифровые следы при расследовании экономических преступлений // Материалы VI Всероссийской научно-практической конференции с международным участием профессорско-преподавательского состава, аспирантов и студентов. – Симферополь, 2021. – С. 291-295.
6. Туркаева Л.В. Понятие, виды и значение следственного осмотра места происшествия // Научный электронный журнал меридиан. – 2020. – №9 (43). – С. 286-288.
7. Шурыгин А.А., Катаев Д.О. Понятие электронных документов и особенности их осмотра // Молодой ученый. – 2021. – №50 (392). – С. 378-379.
8. Самойлов А.Ю. Особенности фиксации цифровых следов в ходе проведения следственного осмотра // Академическая мысль. – 2020. – №2 (11). – С. 96-98.
9. Борисов Г.В. Тактика осмотра и обыска по делам об экономических преступлениях // Энигма. – 2020. – №28-2. – С. 80-83.
10. Кержеманкин С.В. Электронный документ как предмет служебного подлога // Вестник магистратуры. – 2022. – №2-1 (125). – С. 83-85.
11. Евдокименко А.М., Янгаева М.О. Особенности изъятия электронных носителей информации // Материалы VII Международной научно-практической конференции. – Краснодар, 2019. – С. 80-83.

TACTICS OF INSPECTION OF ELECTRONIC DOCUMENTS

R.R. Galyautdinov, *Candidate of Legal Science, Assistant*
V.A. Kovalenko, *Student*
Bashkir State University
(Russia, Ufa)

Abstract. *The purpose of this article is to determine the general tactics for examining electronic documents. For this, a brief description of electronic documents is given, as well as a brief description of the inspection as an investigative action. The initial steps in the examination of electronic documents are given, the importance of involving a specialist in the examination is emphasized. The final part of the scientific article provides a general list of tactical rules that are recommended to be observed when examining electronic documents.*

Keywords: *electronic documents, investigative examination, examination of electronic documents, tactics of examination of electronic documents, types of electronic documents.*