https://doi.org/10.30764/1819-2785-2025-1-66-73

Check for updates (cc) BY

Выявление компьютерного монтажа в электронных образах документов как задача судебной экспертизы

А.Ф. Купин[1,2], **А.С. Коваленко**[2]

[1] Следственный комитет Российской Федерации, Москва 105005, Россия

[2] Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», Москва 105005, Россия

Аннотация. В статье исследован ряд теоретических и прикладных вопросов, касающихся криминалистического исследования электронных образов документов, а именно:
– проведен сравнительный анализ нормативно-правовых актов, регулирующих отдельные аспекты деятельности в части применения электронных образов документов;
– обозначены различия между электронными документами и электронными образами документов;
– сформулировано определение компьютерного монтажа электронного образа документа;
– выделены и охарактеризованы факторы, влияющие на возможность выявления компьютерного монтажа электронных образов документов как способа подделки документов;
– описаны наиболее распространенные форматы файлов, используемые для хранения, обработки и передачи электронных образов документов, и на их примере продемонстрирована эффективность применения отдельных методов и средств исследования в части выявления признаков, указывающих на действия, производимые с электронными образами документов;
– охарактеризованы принцип действия, а также особенности функционирования цветовых моделей Grayscale, RGB и Lab, применяемых при работе с электронными образами документов;
– продемонстрированы возможности каждой из них на конкретных примерах;
– определен порядок и пределы решения экспертной задачи, направленной на установление факта компьютерного монтажа в электронных образах документов, его отдельных признаков.

Ключевые слова: *компьютерный монтаж, электронный образ документа, электронный документ, цифровое изображение, формат файла, цветовая модель*

Для цитирования: Купин А.Ф., Коваленко А.С. Выявление компьютерного монтажа в электронных образах документов как задача судебной экспертизы // Теория и практика судебной экспертизы. 2025. Т. 20. № 1. С. 66–73. https://doi.org/10.30764/1819-2785-2025-1-66-73

Identification of Computer Editing in Electronic Images of Documents as a Task of Forensic Examination

Alexey F. Kupin[1,2], **Anna S. Kovalenko**[2]

[1] The Investigative Committee of the Russian Federation, Moscow 105005, Russia

[2] Bauman Moscow State Technical University (BMSTU), Moscow 105005, Russia

Abstract. The article considers a number of theoretical and applied issues related to forensic examination of electronic images of documents and in particular:
– comparative analysis of normative legal acts carried out with regard to regulation of certain aspects of the activities in terms of electronic images of documents' application;
– indication of differences between electronic documents and electronic images of documents;
– formulation of definition of the electronic image of the document computer editing;
– description of factors affecting the possibility for identification of computer editing of document electronic images as a means of document forgery;
– description of the most typical file formats used for storing, processing and transferring electronic images of documents; examination efficiency demonstration of certain methods and tools by means of the file formate examples in terms of identifying the features that indicate the actions performed on electronic images of documents;

– characteristic of the operation principle and functional specifics of Grayscale, RGB and Lab color models used when working with electronic images of documents; capabilities demonstration of each one of them with specific reference;
– determination of sequencing and limitations of solving the expert task targeted at fact finding of computer editing of document electronic images and its specific features.

Keywords: *computer editing, electronic image of the document, electronic document, digital image, file format, color model*

For citation: Kupin A.F., Kovalenko A.S. Identification of Computer Editing in Electronic Images of Documents as a Task of Forensic Examination. *Theory and Practice of Forensic Science.* 2025. Vol. 20. No. 1. P. 66–73. (In Russ.). https://doi.org/10.30764/1819-2785-2025-1-66-73

Введение

На сегодняшний день информационные технологии так или иначе применяются во всех сферах жизни общества, упрощая и автоматизируя решение повседневных задач. Одна из таких задач – оптимизация ведения документооборота, а именно – упрощение процедуры подачи различных документов в государственные органы, ускорение процесса обмена документами между компаниями при заключении сделок и т. д. Вместе с развитием технологий документооборот постепенно переводится в цифровой вид: многие организации и учреждения переходят с бумажного документооборота на электронный, создаются различные системы и сервисы (например, инфраструктура электронного правительства), работающие с документами в электронном формате. Это, в свою очередь, влечет за собой возникновение новых задач в судебной экспертизе, в частности, связанных с выявлением факта подделки таких документов, например, с помощью компьютерного монтажа. Этот способ недостаточно подробно описан в специальной литературе, а его выявление предполагает наличие у эксперта специальных знаний на стыке судебных экспертиз разных видов: технико-криминалистической, почерковедческой, компьютерно-технической, что на практике встречается крайне редко. Помимо этого, развитие информационных технологий, а также методов и средств обработки цифровых изображений порождает все больше возможностей не только выполнения монтажа, но и сокрытия его следов. Подобные обстоятельства свидетельствуют о необходимости изучения методов и средств выявления компьютерного монтажа в электронных образах документов. Ряд этих методов и средств, как и признаки, выявляемые с их помощью, будут подробно рассмотрены нами в рамках данной статьи.

Понятие электронного образа документа и его отличие от электронного документа

К документам в электронном формате могут быть отнесены электронные документы и электронные образы документов. Важно понимать разницу между этими понятиями.

Электронный документ создается с помощью средств вычислительной техники, изначально существует только в электронном виде и подписывается электронной подписью. В соответствии с п. 11.1 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» под электронным документом понимается «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». При этом Постановление Пленума Верховного Суда РФ от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» (далее – Постановление Пленума ВС РФ № 57) дополнительно разъясняет, что в судебной практике электронный документ – это «документ, созданный в электронной форме без предварительного документирования на бумажном носителе, подписанный электронной подписью в порядке, установленном законодательством Российской Федерации». Условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью,

закреплены в ст. 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Электронный образ документа представляет собой электронную копию документа на бумажном носителе, полученную в результате его сканирования или фотографирования. К электронным образам в некоторых случаях также может предъявляться требование о наличии цифровой подписи. Так, например, в соответствии с Постановлением Пленума ВС РФ № 57 электронный образ документа предложено рассматривать как «переведенную в электронную форму с помощью средств сканирования копию документа, изготовленного на бумажном носителе, заверенную электронной подписью в порядке, установленном законодательством Российской Федерации».

Электронный образ документа, в отличие от электронного документа, далеко не всегда предполагает обязательное наличие электронной подписи. Например, в п. 2 ст. 93 Налогового кодекса Российской Федерации (далее – НК РФ) указано, что под электронным образом документа понимается «документ на бумажном носителе, преобразованный в электронную форму путем сканирования с сохранением его реквизитов». В данном определении требование наличия электронной подписи отсутствует.

В настоящей работе мы рассматриваем понятие «электронный образ документа» применительно к документам, которые среди требований к оформлению не содержат условия обязательного нанесения электронной подписи.

Стоит отметить, что электронные образы документов распространены не менее, чем электронные документы. Так, например, в определенных ситуациях электронные образы используются для загрузки документов в систему Госуслуг, при загрузке документов по контрактам в систему Госзакупок, при ведении нотариальных дел в Единой Информационной Системе нотариата Российской Федерации, при предоставлении соответствующих документов в ходе налоговой проверки и в прочих подобных ситуациях.

Понятие и особенности выявления компьютерного монтажа в электронных образах документов

Как и в случае с обычными документами на бумажном носителе, первоначальное содержание документов в электронном формате может быть подвергнуто изменению в преступных целях. При этом для документов в электронном формате актуальным способом подделки является компьютерный монтаж. В этой связи рассмотрим его подробнее.

Возможности криминалистического исследования документов с целью выявления признаков монтажа рассматривались в работах Н.Ф. Бодрова [1–2], Т.И. Исматовой [3], А.А. Плинатуса [4], И.Н. Подволоцкого [1], М.В. Тороповой [5], Н.Н. Шведовой [6] и других ученых. Приведенные работы дают представление о монтаже как способе подделки документов, однако не содержат описания ряда важных обстоятельств, касающихся особенностей установления компьютерного монтажа документов.

На сегодняшний день в научной среде отсутствует единое понятие компьютерного монтажа. Исходя из определения понятия «монтаж», в котором оно представляется как соединенные в одно целое различные части чего-либо [7], компьютерный монтаж будет рассматриваться как процесс изменения первоначального содержания электронного образа документа путем добавления или замены изначальных реквизитов на реквизиты, полученные из других документов либо изготовленные в специализированных программах (графических редакторах, программах для создания изображений оттисков печати и др.).

В ходе практических и теоретических исследований нами был выявлен ряд обстоятельств, влияющих на возможность установления факта компьютерного монтажа электронного образа документа:

1. Умение лица, выполнявшего монтаж, работать с современными информационными технологиями (графическими редакторами и иными специализированными программами), а также его уровень владения данными программами.

2. Знания лица, выполнявшего монтаж, о возможных признаках и следах монтажа, а также умение их скрывать.

3. Наличие у лица, выполнявшего монтаж, достаточного количества времени на подготовку поддельного документа.

4. Различие фона документа, который подвергся монтажу, и фона монтируемых реквизитов.

5. Формат файла, используемый для хранения, обработки и передачи документа.

6. Цветовая модель, используемая для работы с документом.

Первые два фактора непосредственно связаны с личностью злоумышленника, выполняющего монтаж. Очевидно, что чем выше уровень технической подготовки, и чем лучше он понимает особенности работы тех или иных технологий (например, процессов обработки изображений), тем больше следов монтажа преступник сможет скрыть, что, в свою очередь, затрудняет проведение экспертных исследований.

Однако немаловажным условием также является наличие достаточного количества времени для выполнения монтажа. Применение определенных технологий может потребовать проведения серии экспериментов, направленных на выявление возможных следов и корректировку соответствующих параметров для их сокрытия (например, работа с тональным диапазоном или подбор оптимального уровня шума). Таким образом, даже при высоком уровне технической подготовки злоумышленника, ввиду отсутствия у него достаточного количества времени, в документе могут сохраняться следы монтажа.

Что касается факторов 4–6, то они зависят от первоначальных условий, при которых производится монтаж. Так, различие фона документа, который подвергся монтажу, и фона у монтируемых реквизитов усложняет процесс монтажа, поскольку требует обработки реквизитов для устранения указанного различия. При этом даже после применения соответствующих технических методов и средств фрагменты фона могут сохраняться [8].

И, наконец, стоит подробнее рассмотреть такие важные факторы, как формат файла, который используется для хранения, обработки и передачи документа, а также применяемая цветовая модель.

Особенности форматов файлов, используемых для хранения, обработки и передачи электронных образов документов

Первостепенное значение для проведения всестороннего исследования и получения достоверных выводов относительно объектов экспертизы – электронных образов документов – имеет правильный выбор методов и средств, учитывающих особенности форматов файлов, используемых для их хранения, обработки и передачи.

Определенные методы могут быть использованы для исследования документов, представленных в различных форматах файлов Однако важно понимать, что не все методы обладают подобной универсальностью. Так, метод анализа артефактов сжатия, успешно используемый при исследовании JPEG-файлов, принципиально неприменим для работы с файлами иных форматов, так как основывается непосредственно на особенностях формата JPEG [9]. Аналогично определенные программные средства могут быть применены для широкого спектра объектов, а могут быть разработаны для анализа файлов одного конкретного формата.

Формат файла представляет собой правила размещения в теле файла пользовательской и дополнительной служебной информации (метаданных). Именно от специфики формата зависит выбор определенных методов и средств исследования. В этой связи эксперту необходимо не только понимание особенностей различных форматов файлов, но и постоянная актуализация своих знаний в этой области, так как зачастую те или иные форматы могут обновляться разработчиками.

Наиболее распространенным форматом файлов для хранения, обработки и передачи электронных образов документов является PDF (The adobe portable document format), для работы с которым предусмотрено большое количество программных средств. Стоит отметить, что в представленной работе рассматривается ситуация, в которой формат PDF используется для хранения, обработки и передачи растровых изображений документов, получаемых в результате их сканирования. Ситуация, в которой документ изначально создается в электронном формате с помощью текстового редактора и впоследствии конвертируется в формат PDF, к теме исследования не относится, поскольку в таком случае речь идет об электронном документе.

Разработчиком формата PDF является компания Adobe. Структура указанного формата включает в себя 4 раздела[1]:

1. *Header* (заголовок) – первая строка файла, содержащая информацию о номере версии спецификации PDF. Она имеет вид %PDF-1.N, где N – номер версии. На момент написания данной работы последней версией формата являлась 1.7.

2. *Body* (тело файла) – раздел, который состоит из последовательности объектов,

[1] Document management – Portable document format – Part 1: PDF 1.7. https://opensource.adobe.com/dc-acrobat-sdk-docs/pdfstandards/PDF32000_2008.pdf

представляющих содержимое документа. Началом объекта является номер ссылки, номер версии и ключевое слово obj, за которым следует контейнер объекта, ограниченный символами << и >>. Об окончании объекта сигнализирует ключевое слово endobj.

Формат PDF поддерживает 8 типов объектов: булевы значения (boolean objects), числа (numeric objects), строки (string objects), имена (name objects), массивы (array objects), словари (dictionary objects), потоки (stream objects) и нулевые объекты (null objects).

3. *xref Table* (таблица xref, таблица перекрестных ссылок) – таблица, содержащая перекрестные ссылки на объекты документа. Каждый объект документа представлен записью в таблице xref, которая включает в себя сведения о его смещении в теле файла и имеет фиксированную длину 20 байт.

4. *Trailer* (завершающая часть) – раздел, содержащий информацию о расположении таблицы перекрестных ссылок (значение смещения от начала файла) и некоторых специальных объектов в теле файла. Окончанием файла формата PDF является строка %%EOF.

Кроме того, важной особенностью этого формата является реализованный в нем механизм обновления документа. Суть механизма состоит в том, что при внесении каких-либо изменений в документ они добавляются в конец файла, однако сам файл при этом заново не перезаписывается[2].

Для хранения, обработки и передачи электронных образов документов также могут быть использованы файлы графических форматов, например, JPEG, TIFF, PNG, BMP и прочие. Указанные форматы применяются для работы с цифровыми изображениями и, соответственно, позволяют в полной мере задействовать весь спектр методов и программных средств, разработанных непосредственно для решения задач цифровой обработки изображений.

Под цифровым изображением понимается такая двумерная функция f (x, y), где x и y – координаты в пространстве (конкретно на плоскости) и значение f которой в любой точке, задаваемой парой координат (x, y), называется интенсивностью или уровнем серого (яркостью) изображения в этой точке, при этом величины x, y и f принимают конечное число дискретных значений [10, с. 22; 11].

Цифровое изображение состоит из конечного числа элементов, каждый из которых расположен в конкретном месте и принимает определенное значение. Эти элементы называются элементами изображения или пикселями [10, с. 22; 12, с. 41]. Цифровая обработка изображений представляет собой обработку с помощью цифровых вычислительных машин (компьютеров).

Стоит отметить, что в обработке изображений различают процессы низкого, среднего и высокого уровней. Процессы низкого уровня нацелены на уменьшение шумов, повышение контраста, изменение уровня яркости и прочие подобные операции, при которых и на входе, и на выходе присутствуют изображения. Средний уровень включает в себя такие задачи, как сегментация, классификация, описание и сжатие объектов в удобную для компьютерной обработки форму. В данном случае результат обработки представлен извлекаемыми из изображения признаками и атрибутами. Высокоуровневая обработка, в свою очередь, подразумевает «осмысление» компьютером набора распознанных объектов [13, с. 13].

Применительно к задаче выявления компьютерного монтажа в электронных образах документов для эксперта представляют интерес операции, позволяющие осуществлять цветовые преобразования и изменение тонального диапазона изображения, то есть относящиеся к низкоуровневым процессам обработки. В этой связи обработка цифровых изображений в рамках данной работы рассматривалась нами с точки зрения низкоуровневых процессов.

В качестве примера графического формата разберем более подробно формат JPEG. Он был создан в результате работы объединенной группы экспертов в области фотографии JPEG (Joint Photographic Experts Group) и задумывался как новый международный стандарт сжатия цветных изображений [13, с. 58; 14].

Одно из существенных преимуществ этого формата заключается в возможности максимального сохранения визуального качества изображения при наименьшем размере файла, что может быть существенно для систем, в которых ежедневно обрабатывается большой объем документов. Указанное преимущество обусловлено алгоритмом сжатия JPEG, состоящим из трех

[2] Там же. https://opensource.adobe.com/dc-acrobat-sdk-docs/pdfstandards/PDF32000_2008.pdf

последовательно применяемых технологий [13, с. 59; 15]:

1. Цветовая субдискретизация.

2. Дискретное косинусное преобразование и дискретизация.

3. Кодирование длин серий, дельта-кодирование и метод Хаффмана.

В основе структуры файлов формата JPEG лежит разделение на секции, перед каждой из которых располагается специальный маркер, начинающийся со значения FF и имеющий длину 2 байта. Стартовым маркером для файлов формата JPEG является последовательность FF D8, концевым маркером – FF D9. В качестве наиболее значимых для исследования файлов JPEG можно выделить следующие маркеры[3]:

1. FF FE – начало секции с комментарием.

2. FF DB – таблица квантования.

3. FF C4 – таблица Хаффмана.

4. FF E0 – зарезервированная область для сегментов приложений.

5. FF DA – начало секции с закодированными данными изображения. Именно после этого маркера и до концевого маркера FF D9 следует непосредственно само изображение.

Подробная информация о всех маркерах JPEG содержится в документации к указанному формату[4].

Стоит отметить, что именно официальная документация от разработчиков является основным источником, позволяющим эксперту получить необходимую для выбора методов и средств исследования информацию о структуре и особенностях того или иного формата.

Основные цветовые модели, используемые для работы с электронными образами документов

При проведении исследования эксперту также необходимо учитывать, что любое цифровое изображение кодируется в соответствии с определенной цветовой моделью (цветовым пространством), которая, как и формат файла, может оказывать влияние на выбор методов и средств исследования. Так, например, для одних и тех же программных инструментов, реализованных в Adobe Photoshop, в зависимости от цветовой модели исследуемого изображения могут различаться настраиваемые параметры. Под цветовой моделью понимается модель представления цвета, в соответствии с которой цвет кодируется в формате точки с конкретными координатами. На сегодняшний день существует большое количество цветовых моделей: RGB, Lab, CMYK, Grayscale (градации серого, оттенки серого), YCbCr, HSB, HSL и другие. На наш взгляд, наиболее распространенными цветовыми моделями, применяемыми в работе с электронными образами документов, являются Grayscale, RGB и Lab.

Grayscale – это ахроматическая модель, используемая для черно-белых изображений. Каждый пиксель 8-битного изображения в указанной цветовой модели содержит значение яркости в диапазоне от 0 (черный) до 255 (белый). В 16- и 32-битных изображениях количество градаций серого больше. Значения градаций серого также могут быть выражены в процентах суммарного покрытия черной краской (значение 0 % эквивалентно белому, а 100 % – черному цвету). Указанная модель наиболее часто используется для хранения изображений, полученных в результате сканирования.

Цветовая модель RGB представляет собой адаптивное цветовое пространство, которое описывает способ кодирования цветов за счет комбинации трех основных из них – красного (Red), зеленого (Green) и синего (Blue).

Lab – аппаратно-независимая трехканальная цветовая модель, обладающая широким цветовым охватом и применяемая в качестве промышленного стандарта передачи цветов[5]. Любой цвет в этой модели определяется яркостью (L) и двумя компонентами a и b. Значение первого компонента (a) задает положение цвета в диапазоне от пурпурного до зеленого, второго (b) – от желтого до синего.

Заключение

Приведенные особенности технологий, задействованных в процессе создания документов в электронной форме, следует учитывать при решении задач по выявлению компьютерного монтажа в электронных образах документов. При этом необходимо помнить и о других факторах, к которым, например, относятся навык лица, выпол-

[3] Information technology – Digital compression and coding of continuous-tone still images: Extensions. https://www.itu.int/rec/T-REC-T.84-199607-I/en

[4] Там же.

[5] Четверкин П.А. Методы цифровой обработки слабовидимых изображений при технико-криминалистическом исследовании: дис. … канд. юрид. наук. Москва, 2009. 259 с. (С. 48).

нившего монтаж, работать с современными информационными технологиями, наличие у него знаний о возможных следах монтажа и способах их сокрытия, а также достаточного количества времени. Стоит также обращать внимание на характеристики документа, подделка которого может осуществляться указанным способом (формат файла, фон документа и монтируемых реквизитов, используемая цветовая модель). Помимо этого, при выборе определенных методов и программных средств для исследования эксперту нужно принимать в расчет особенности некоторых форматов файлов и цветовых моделей, используемых для хранения, обработки и передачи электронных документов. Таким образом, внимание к вышеперечисленным обстоятельствам позволит снизить вероятность выбора неэффективных методов и средств и, как следствие, избежать получения недостоверных результатов и ошибочных выводов.

СПИСОК ЛИТЕРАТУРЫ

1. Подволоцкий И.Н., Бодров Н.Ф. К вопросу о традиционных и современных способах технической подделки подписей и рукописных записей // Законы России: опыт, анализ, практика. 2011. № 12. С. 84–89.
2. Россинская Е.Р., Бодров Н.Ф. Современное состояние и перспективы исследования образов цифровых следов в судебной почерковедческой экспертизе // Криминалистика: вчера, сегодня, завтра. 2022. Т. 21. № 1. С. 121–135. https://doi.org/10.55001/2587-9820.2022.44.98.011
3. Исматова Т.И. Особенности диагностического исследования копий рукописных текстов, изготовленных способом цифрового монтажа // Судебная экспертиза. 2013. № 4 (36). С. 90–99.
4. Плинатус А.А. Современные возможности технико-криминалистического исследования копий документов, изготовленных посредством монтажа // Криминалистические средства и методы в раскрытии и расследовании преступлений. М.: ЭКЦ МВД России, 2006. С. 139–146.
5. Торопова М.В. Содержание понятия монтажа в судебно-технической экспертизе документов и его криминалистическая оценка // Теория и практика судебной экспертизы в современных условиях: Материалы 4-й Международной научно-практической конференции (Москва, 30–31 января 2013 г.). М.: Проспект, 2013. С. 306–308.
6. Шведова Н.Н. Методические и организационные проблемы комплексных исследований поддельных документов, изготовленных способом компьютерного монтажа // Теория и практика судебной экспертизы в современных условиях: Материалы 3-й Международной научно-практической конференции (Москва, 25–26 января 2011 г.). М.: Проспект, 2011. С. 577–579.
7. Ожегов С.И. Толковый словарь русского языка. М.: Азбуковник, 2003. 943 с.
8. Купин А.Ф., Коваленко А.С., Сорокина Е.К. Установление факта компьютерного монтажа документа методами судебной экспертизы // Дискуссионные вопросы теории и

REFERENCES

1. Podvolotsky I.N., Bodrov N.F. About Investigations of Established and Modern Methods of Forged Signatures and Notes. *Laws of Russia: Experience, Analysis and Practice.* 2011. No. 12. P. 84–89. (In Russ.).
2. Rossinskaya E.R., Bodrov N.F. The Current State and Prospects for the Study of Digital Trace Images in Forensic Handwriting Expertise. *Forensics: Yesterday, Today, Tomorrow*. 2022. Vol. 21. No. 1. P. 121–135. (In Russ.). https://doi.org/10.55001/2587-9820.2022.44.98.011
3. Ismatova T.I. Peculiarities of Diagnostic Examination of Copies of Handwritten Texts Made by Means of Digital Editing. *Forensic Expertise*. 2013. No. 4 (36). P. 90–99. (In Russ.).
4. Plinatus A.A. Modern Capabilities of Forensic Technical Examination of Document Copies Made by means of Montage. *Forensic Tools and Methods in the Detection and Investigation of Crimes.* Moscow: EKTs MVD Rossii, 2006. P. 139–146. (In Russ.).
5. Toropova M.V. The Content of the Term 'Mounting' in Forensic Technical Examination of Documents and its Forensic Assessment. *Theory and Practice of Forensic Examination in Present-Day Conditions: Materials of the 4th International Science and Research Conference (Moscow, January 30–31, 2013).* Moscow: Prospekt, 2013. P. 306–308. (In Russ.).
6. Shvedova N.N. Methodological and Organizational Issues of Complex Examination of Forged Documents Made by means of Computer Editing. *Theory and Practice of Forensic Examination in Present-Day Conditions: Materials of the 3rd International Science and Research Conference (Moscow, January 25–26, 2011).* Moscow: Prospekt, 2011. P. 577–579. (In Russ.).
7. Ozhegov S.I. *Explanatory Dictionary of the Russian Language.* Moscow: Azbukovnik, 2003. 943 p. (In Russ.).
8. Kupin A.F., Kovalenko A.S., Sorokina E.K. Fact-Finding of Document Computer Editing by Means of Forensic Methods. *Discussion Issues of Theory and Practice of Forensic Examination:*

практики судебной экспертизы: Материалы IV Международной научно-практической конференции (Москва, 25–26 марта 2021 г.). М.: РГУП, 2021. С. 354–360.
9. Rakovi D.N. Error Level Analysis (ELA) // Tehnika. 2023. Vol. 78. No. 4. P. 445–451. https://doi.org/10.5937/tehnika2304445R
10. Гонсалес Р., Вудс Р. Цифровая обработка изображений. Издание 3-е, исправленное и дополненное. М.: Техносфера, 2012. 1104 с.
11. Gonzalez R.C., Woods R.E., Eddins S.L. Digital Image Processing Using MATLAB. 3rd ed. Gatesmark Publishing, 2020. 616 p.
12. Яне Б. Цифровая обработка изображений. М.: Техносфера, 2007. 584 с.
13. Визильтер Ю.В., Желтов С.Ю., Бондаренко А.В., Ососков М.В., Моржин А.В. Обработка и анализ изображений в задачах машинного зрения: Курс лекций и практических занятий. М.: Физматкнига, 2010. 672 с.
14. Sebestyen I. JPEG: Still Image Data Compression Standard // Computer Standards & Interfaces. 1993. Vol. 15. No. 4. P. 365–366. https://doi.org/10.1016/0920-5489(93)90038-s
15. Hudson G., Léger A., Niss B., Sebestyén I. JPEG at 25: Still Going Strong // IEEE MultiMedia. 2017. Vol. 24. No. 2. P. 96–103. https://doi.org/10.1109/mmul.2017.38

Materials of the IV International Science and Research Conference (Moscow, March 25–26, 2021). Moscow: RGUP, 2021. P. 354–360. (In Russ.).
9. Rakovi D.N. Error Level Analysis (ELA). *Tehnika*. 2023. Vol. 78. No. 4. P. 445–451. https://doi.org/10.5937/tehnika2304445R
10. Gonzalez R., Woods R. *Digital Image Processing*. 3rd ed., revised and expanded. Moscow: Tekhnosfera, 2012. 1104 p. (In Russ.).
11. Gonzalez R.C., Woods R.E., Eddins S.L. *Digital Image Processing Using MATLAB.* 3rd ed. Gatesmark Publishing, 2020. 616 p.
12. Yane B. *Digital Image Processing*. Moscow: Tekhnosfera, 2007. 584 p. (In Russ.).
13. Vizilter Yu.V., Zheltov S.Yu., Bondarenko A.V., Ososkov M.V., Morzhin A.V. *Machine Vision Issues in Image Processing and Analysis: Lectures and Practical Training Course.* Moscow: Fizmatkniga, 2010. 672 p. (In Russ.).
14. Sebestyen I. JPEG: Still Image Data Compression Standard. *Computer Standards & Interfaces.* 1993. Vol. 15. No. 4. P. 365–366. https://doi.org/10.1016/0920-5489(93)90038-s
15. Hudson G., Léger A., Niss B., Sebestyén I. JPEG at 25: Still Going Strong. *IEEE MultiMedia.* 2017. Vol. 24. No. 2. P. 96–103. https://doi.org/10.1109/mmul.2017.38

ИНФОРМАЦИЯ ОБ АВТОРАХ

Купин Алексей Фёдорович – к. юр. н., старший инспектор управления научно-исследовательской деятельности (научно-исследовательского института криминалистики) Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации; доцент кафедры «Безопасность в цифровом мире» Московского государственного технического университета имени Н.Э. Баумана;
e-mail: alexcrim@rambler.ru

Коваленко Анна Сергеевна – ассистент кафедры «Безопасность в цифровом мире» Московского государственного технического университета имени Н.Э. Баумана;
e-mail: annekovalenko@mail.ru

Статья поступила: 15.11.2024
После доработки: 20.12.2024
Принята к печати: 24.01.2025

ABOUT THE AUTHORS

Kupin Alexey Fedorovich – Candidate of Law, Senior Inspector of the Research Directorate (Research Institute of Criminalistics) of the Chief Criminalistic Directorate (Criminalistic Center) of the Investigative Committee of the Russian Federation; Associate Professor of "Security in the Digital World" Department, Bauman Moscow State Technical University; e-mail: alexcrim@rambler.ru

Kovalenko Anna Sergeevna – Assistant Professor of "Security in the Digital World" Department, Bauman Moscow State Technical University;
e-mail: annekovalenko@mail.ru

Received: November 15, 2024
Revised: December 20, 2024
Accepted: January 24 2025