Дата поступления рукописи в редакцию: 16.08.2026 г.
Дата принятия рукописи в печать: 25.09.2026 г.

DOI: 10.24412/2782-3849-2026-9-156-160

ШЕЛЬСКАЯ Светлана Николаевна,
кандидат юридических наук, старший преподаватель кафедры криминалистики Московского университета МВД России имени В.Я. Кикотя, ORCID ID: 0009-0003-1965-1487, e-mail: sveta.mila2@mail.ru

ЭЛЕКТРОННЫЙ ПОДЛОГ ДОКУМЕНТОВ: ПОНЯТИЕ И ВИДЫ

Аннотация. *В связи с постепенным переходом делопроизводства на электронную форму передачи данных, участились случаи подделки электронных документов. В ходе изучения правоприменительной практики и научной литературы выявлена необходимость рассматривать электронный подлог документов отдельно от материального и интеллектуального подлогов в связи с различием в способах подделки и методах их исследования. Электронный подлог документов опрелеляется как фиктивное изготовление или внесение искаженных данных в файл электронного документа с использованием программного обеспечения. В ходе исследования и анализа подложной документации выделены следующие способы подделки электронных документов: 1) изготовление электронного документа с использованием неоригинального программного обеспечения; 2) изготовление электронного документа с поддельной электронной подписью; 3) создание электронного образа документа с изготовлением оттиска печати путем использования компьютерных программ, являющихся конструкторами печатей и штампов; 4) генерация электронного документов с помощью искусственного интеллекта; 5) внесение частичных изменений в электронный образ документа способом монтажа с использованием компьютерных программ-редакторов; 6) внесение изменений в электронный документ, подписанный простой электронной подписью. Настоящее исследование призвано систематизировать научные знания о способах подделки электронных документов и адресовано ученым-криминалистам и работникам органов расследования в целях их понимания возможностей исследования подложных файлов.*

Ключевые слова: *цифровая криминалистика; криминалистическая техника; криминалистическая документология; подлог документов; электронный документ; электронная подпись; электронный образ документа; электронный подлог; компьютерный монтаж.*

SHELSKAYA Svetlana Nikolaevna,
Candidate of Law, Senior Lecturer, Department of Criminalistics, Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot

ELECTRONIC FORGERY OF DOCUMENTS: THE CONCEPT AND TYPES

Annotation. *Due to the gradual transition of record-keeping to electronic data transmission, cases of electronic document forgery have become more frequent. A study of law enforcement practice and academic literature has revealed the need to consider electronic document forgery separately from material and intellectual forgeries, due to differences in forgery methods and investigation techniques. Electronic forgery of documents is defined as the fictitious generation or insertion of distorted data into an electronic document file using software. Through the study and analysis of counterfeit documentation, the following methods of electronic document forgery have been identified: 1) generation of an electronic document using non-genuine software; 2) generation of an electronic document with a forged electronic signature; 3) generation of an electronic image of a document with the production of a stamp impression using computer programs that function as stamp and seal designers; 4) generation of electronic documents using artificial intelligence; 5) making partial alterations to an electronic document image through editing using computer-based editing software; 6) modification of an electronic document signed with a simple electronic signature. This study aims to systematize scientific knowledge about methods of forging electronic documents and is addressed to forensic scientists and investigators in order to help them understand the possibilities of examining forged files.*

Key words: *digital forensics; forensic technology; forensic document examination; document forgery; electronic document; electronic signature; electronic document image; electronic forgery; computer-based editing.*

В традиционной Криминалистике различают материальный и интеллектуальный разновидности подлога документов. Эти способы подделки хорошо изучены и без проблем распознаются при исследовании материальных носителей информации [1]. Однако в повседневной деятельности мы все чаще имеем дело с электронной формой передачи данных. Многие организации и даже государственные учреждения переходят на электронный документооборот. Однако электронные документы и электронные образы документов часто подвергаются различного рода фальсификациям в целях совершения преступлений.

Например, злоумышленники, будучи сотрудниками организации, могут создавать электронные финансовые документы с интеллектуальным подлогом, то есть содержащие в себе заведомо ложные данные, в целях дальнейшего присвоения имущественных средств. Это особенно возможно в случаях наличия программы электронной подписи (далее ЭП) на компьютерном устройстве с широким доступом для большого круга лиц, передачи ЭП недобросовестным сотрудникам, похищения носителя ЭП или копирования закрытого ключа и др. [2]. В подобных случаях форма электронного документа является оригинальной, но в самом содержании имеется интеллектуальный подлог. Этот вид подлога может быть выявлен, в том числе, в ходе судебно-экономических исследований, в частности, бухгалтерской экспертизы, при несоответствии данных одних первичных финансовых документов другим.

Однако электронные документы могут содержать не только интеллектуальный подлог, но и сами их форма, отдельные элементы и даже электронная подпись могут быть поддельными. Подобный подлог нельзя рассматривать в качестве материального, поскольку материальные изменения документа на его носителе являются предметом исследования технико-криминалистических экспертиз [3]. Документы, содержащиеся на электронных носителях, исследуются в рамках компьютерных экспертиз [4]. Полагаем, что подобный вид подлога документов более уместно называть электронным. В связи с вышеизложенным, фиктивное изготовление или внесение искаженных данных в файл электронного документа с использованием программного обеспечения следует признавать электронным подлогом.

Для электронного подлога документов, как и для материального подлога, характерны способы полной и частичной подделки документов. Рассмотрим более подробно полные способы подделки, при которых электронные документы или электронные образы документов изготавливаются полностью.

В организациях или учреждениях для создания электронных документов может использоваться специфическое, специально разработанное или даже секретное (государственная, коммерческая и иные виды тайн) программное обеспечение. Разумеется, далеко не у всех злоумышленников будет иметься доступ к подобным компьютерным программам, поэтому в случаях подделки электронных документов от имени таких организаций или учреждений, формат поддельных документов будет существенно отличаться от оригинальных. В ходе судебной компьютерной экспертизы может быть установлено, какое именно программное обеспечение использовалось при изготовлении электронного документа и имеет ли оно отличие от оригинального, используемого в конкретной организации. Даже факт использования злоумышленником такой же программы, что и в учреждении, но другой модификации, может иметь существенное значение по уголовному делу.

В целях совершения преступлений также могут применяться различные способы подлога электронной подписи: создание поддельного цифрового сертификата посредством специализированных программ; создание графических изображений электронной подписи с применением технологий искусственного интеллекта [5]. В подобных случаях электронные документы должны направляться для исследования в рамках компьютерно-технической экспертизы.

Распространенным способом электронного подлога является изготовление документа путем монтажа с использованием программного обеспечения. Например, мошенники, выдавая себя за представителей коммерческой фирмы, могут заключать фиктивные сделки с потерпевшими.

Так, на некоторых коммерческих торговых сайтах участники не проходят надежной аутентификации и не применяется принцип безопасности заключаемой сделки, например, портал оптовых закупок на сайте https://yopt.org. Также злоумышленники могут создать фишинговый сайт реально существующей организации и якобы от ее имени осуществлять поставку товаров, предоставлять услуги.

Используя подобные сайты, мошенники при переписке с потерпевшими отправляют им поддельные электронные договоры и иные документы в целях совершения хищений. Как правило,

подобные документы существуют только в электронном виде, создаются способом монтажа путем вставки в документ с расширением doc/docx изображения рукописной подписи руководителя организации и оттиска печати этого предприятия с последующим сохранением в файле с расширением pdf [6]. В подобных случаях электронные документы отправляются на исследование судебной компьютерно-технической экспертизы.

В целях предупреждения совершения мошенничества путем электронного подлога документов в торговых интернет-площадках должны быть предусмотрены меры по установлению личности клиента, представителя организации, а также подтверждения подлинности передаваемой информации электронной подписью либо должен соблюдаться принцип безопасности сделки.

При совершении мошенничества с использованием поддельных электронных образов документов, бланки которых не имеют степеней защиты, как правило, электронные документы изготавливаются полностью. При этом оттиски печатей могут быть изготовлены с использованием различных компьютерных программ, являющихся конструкторами печатей и штампов. В этих случаях поддельные электронные документы также являются объектами исследования компьютерно-технической экспертизы.

Если созданные в ходе электронного подлога рукописные подписи и оттиски печати переносятся с помощью печатающего устройства, например, цветного принтера, на бумажный носитель, который в дальнейшем выдается за оригинальный документ, то подлежат исследованию признаки материального подлога. Документы на материальных носителях отправляются на технико-криминалистическую экспертизу.

Часто при подделке государственных документов на материальных носителях для имитации подписей и записей используются планшетные плоттеры и иные графопостроители. В таких случаях при изображении графических объектов пишущий узел перемещается по неподвижному материальному носителю. Однако воспроизведение таких важных признаков, как направление движений и дифференциация нажима, вряд ли возможно [7]. Соответственно подобные графические элементы являются предметами исследования судебной почерковедческой экспертизы. Материалы документа и способ его изготовления могут быть исследованы в ходе судебной технико-криминалистической экспертизы документов. А сами графопостроители могут быть объектами исследования компьютерно-аппаратной экспертизы.

В настоящее время набирает обороты новый способ изготовления подложных файлов – генерация электронных документов с помощью искусственного интеллекта. Например, бухгалтерские, финансовые и даже юридические документы генерируются с использованием программных средств ИИ в целях сокрытия истинного их экономического смысла, ухода от налогов или для иного противоправного обоснования вычетов и расходов. Преступники с помощью нейросетей, языковых моделей и пр. могут сконструировать фиктивные документы в условиях отсутствия реальной хозяйственной активности и взаимодействия с контрагентами. Также с помощью ИИ может быть осуществлена подмена уже существующих документов, включая тонкое копирование стиля, подписи, печати, формулировок и реквизитов. Но также с помощью искусственного интеллекта можно выявить признаки сгенерированности электронного документа в ходе анализа: данных о времени отправки/получения документа, IP-адреса, структуры xml. Подделанные ИИ документы по сравнению с однотипными документами в хозяйствующем субъекте часто имеют несоответствующий шрифт, иное расположение реквизитов, однотипность лексики, особенности стилистики, шаблонность фраз, скопированных с документов других организаций. ИИ может также выявлять связи между организациями: перекрёстные сделки, совпадение контактных лиц, адресов, IP, нерегулярные расчетные счета и другие признаки серых схем [8].

Что касается частичного электронного подлога документов, то одним из распространенных способов является внесение в электронный образ документа частичных изменений с использованием различного программного обеспечения. Например, Единый портал государственных услуг стал излюбленной площадкой для совершения мошенничества при получении выплат. Поскольку сотрудники МФЦ практически больше не привлекаются для проверки подлинности документов, предъявляемых заявителями. Преступники в своем аккаунте указанного портала загружают поддельные отсканированные образы документов, которые якобы подтверждают их право получать социальные выплаты. Фальсификация отсканированных документов осуществляется посредством различных компьютерных программ, в том числе, графических и PDF-редакторов. При этом за основу, как правило, берутся отсканированные образы подлинных документов, в которые вносятся частичные изменения путем компьютерного монтажа. Например, может быть осуществлена замена фотографии с использованием фоторедактора. В этих случаях поддельные электронные образы документов являются объектами исследования компьютерно-технической экспертизы.

Возможны случаи внесения частичных изменений и в электронный документ. Если такой

документ заверен электронной подписью, то он перестает быть действительным. При создании ключа электронной подписи и ключа проверки электронной подписи используются средства, которые устанавливают факт изменения содержания электронного документа после момента его подписания. Однако простая электронная подпись не гарантирует, что в файл не были внесены изменения. Поэтому простая электронная подпись не используется для заверения юридически значимых документов.

Для создания усиленной неквалифицированной подписи используют криптографические алгоритмы, которые создают индивидуальный цифровой отпечаток документа, поэтому часто используется для подписания документа от имени, например, коммерческой организации. А для усиленной квалифицированной подписи применяют надежные сертифицированные криптографические алгоритмы, поэтому она приравнивается к собственноручной подписи [9]. Однако информационные технологии развиваются стремительно, поэтому можем предположить, что существуют попытки разработать компьютерные, скорее всего, вредоносные программы, позволяющие обойти электронную подпись, при внесении частичных изменений в подлинный документ.

Таким образом, приходим к выводу, что электронный подлог документа – это фиктивное изготовление или внесение искаженных данных в файл электронного документа с использованием программного обеспечения. Способы полной подделки электронных документов: изготовление электронного документа с использованием неоригинального программного обеспечения; изготовление электронного документа с поддельной электронной подписью; создание электронного образа документа с изготовлением оттиска печати путем использования компьютерных программ, являющихся конструкторами печатей и штампов; генерация электронного документа с помощью искусственного интеллекта. Способы частичной подделки электронных документов: внесение частичных изменений в электронный образ документа способом монтажа с использованием компьютерных программ-редакторов; внесение изменений в электронный документ, подписанный электронной подписью.

Список литературы:

[1] Поборцев Е.И. Материальный и интеллектуальный подлог в документах и способы их обнаружения. // Тенденции развития науки и образования. 2024. № 108-6. С. 89-92.

[2] Нуриманова Э.Р., Печерица Е.В. Способы подлогов электронных финансовых документов и методы их выявления. // Здоровье - основа человеческого потенциала: проблемы и пути их решения. 2020. Т. 15. № 3. С. 1422-1427.

[3] Бочарова О.С. Персонализация идентификационных документов: анализ технологий и методы выявления материального и интеллектуального подлога. // Вопросы криминологии, криминалистики и судебной экспертизы. 2022. № 2 (52). С. 87-93.

[4] Арутюнов А.С., Фаниев П.А. Классификация файлов и метаданных как объектов компьютерной экспертизы. // Общество и право. 2022. № 4 (82). С. 79-82.

[5] Когут В.А. Цифровой анализ при производстве экспертизы электронных документов по экономическим преступлениям. В сборнике: Санкт-Петербургский международный криминалистический форум. Материалы международной научно-практической конференции. Санкт-Петербург, 2024. С. 867-875.

[6] Изюмов Р.Н., Диянова А.А. Особенности фиксации и исследования документов в делах, связанных с подлогом документов в электронном формате на сайтах по поиску и предоставлению услуг в сети Интернет. В сборнике: Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации. Сборник научных статей по материалам международной научно-практической конференции. Москва, 2021. С. 158-164.

[7] Серго С.В., Снежкова Ж.Ю. К вопросу об имитации подписей и записей с помощью цветных печатающих устройств при расследовании преступлений в сфере оборота поддельных документов, государственных наград, штампов, печатей или бланков. // Юристъ-Правоведъ. 2023. № 1 (104). С. 111-117.

[8] Васенкова Е. Как налоговая выявляет поддельные ИИ-документы, зачем это главбухам и какие риски. // Аутсорсинг учетных функций. – URL: https://bridge-group.ru/articles/nalogi/kak-nalogovaya-vyyavlyaet-poddelnye-ii-dokumenty-zachem-eto-glavbukham-i-kakie-riski/.

[9] Сапаров Д.К. Правовое регулирование электронного документооборота и цифровых подписей. // Холодная наука. 2025. № 14. С. 86-107.

References:

[1] Exodus E.I. Material and intellectual forgery in documents and methods of their detection . // Trends in the development of science and education. 2024. № 108-6. S. 89-92.

[2] Nurimanova E.R., Pecheritsa E.V. Methods of forgery of electronic financial documents and methods of their identification . // Health is the basis of human potential: problems and ways to solve them. 2020. VOL. 15. № 3. S. 1422-1427.

[3] O.S. Bocharova. Personalization of identification documents: analysis of technologies and methods for identifying material and intellectual forgery . // Issues of criminology, forensic science and forensic expertise. 2022. № 2 (52). S. 87-93.

[4] Arutyunov A.S., Faniev P.A. Classification of files and metadata as objects of computer expertise . // Society and law. 2022. № 4 (82). S. 79-82.

[5] Kogut V.A. Digital analysis in the examination of electronic documents on economic crimes. In the collection: St. Petersburg International Forensic Forum. Materials of the international scientific-practical conference. St. Petersburg, 2024. S. 867-875.

[6] Izyumov R.N., Diyanova A.A. Features of fixation and research of documents in cases related to forgery of documents in electronic format on sites for search and provision of services on the Internet. In the collection: Development of the doctrine of countering the investigation of crimes and measures to overcome it in the context of digital transformation. Collection of scientific articles based on the materials of the international scientific-practical conference. Moscow, 2021. S. 158-164.

[7] Sergo S.V., Snezhkova J.Yu. On the issue of imitation of signatures and records using color printing devices when investigating crimes in the field of circulation of fake documents, state awards, stamps, seals or forms . // Lawyer-Pravoveda. 2023. № 1 (104). S. 111-117.

[8] Vasenkova E. How the tax authorities identify fake AI documents, why do the chief accountants need it and what risks . // Outsourcing of accounting functions. – URL: https://bridge-group.ru/articles/nalogi/kak-nalogovaya-vyyavlyaet-poddelnye-ii-dokumenty-zachem-eto-glavbukham-i-kakie-riski/.

[9] Saparov D.K. Legal regulation of electronic document management and digital signatures . // Cold science. 2025. № 14. S. 86-107.

