Научная статья
УДК 34.09
https://doi.org/10.33874/2072-9936-2026-0-1-148-154

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ В СУДЕБНОМ ДЕЛОПРОИЗВОДСТВЕ

Юлия Владимировна Левина[1]

Александр Владимирович Яковлев[2]

[1,2] Ростовский государственный экономический университет (РИНХ), 344022, Россия, г. Ростов-на-Дону, ул. М. Горького, д. 166

[1] kochurau@gmail.com

[2] mfoto2@ya.ru

Аннотация

Внедрение электронного документооборота в судах судебной системы Российской Федерации позволило активизировать развитие судебного делопроизводства, ускорить получение процессуальных документов, снизить издержки посредством исключения почтовых расходов. В статье проанализированы правовые основы применения квалифицированной электронной подписи (КЭП) и даны рекомендации по ее корректному применению. Цель настоящей статьи – определить правовое значение КЭП, а также установить способы проверки подлинности КЭП с использованием криптографических методов проверки. Статья предоставляет возможность участникам процесса получить сведения о правилах работы и проверки КЭП, а также способствует развитию профессиональных навыков юристов посредством использования возможностей электронного судебного документооборота. В основе методологии исследования лежит системный метод исследования с применением общенаучных и частнонаучных методов. В результате проведенного анализа даны рекомендации участникам судебного процесса, как значительно ускорить возможность получения решений и определений суда.

Ключевые слова: квалифицированная электронная подпись; усиленная квалифицированная электронная подпись; проверка подлинности КЭП; Токен; Рутокен 3.0; программа «КриптоПро»; электронное судебное делопроизводство.

Для цитирования: *Левина Ю. В., Яковлев А. В.* Актуальные проблемы применения квалифицированной электронной подписи в судебном делопроизводстве // Вестник Российской правовой академии. 2026. № 1. С. 148–154. https://doi.org/10.33874/2072-9936-2026-0-1-148-154

Research Article

CURRENT ISSUES OF APPLICATION OF QUALIFIED ELECTRONIC SIGNATURE IN COURT PROCEEDINGS

Yulia V. Levina[1]

Alexander V. Yakovlev[2]

[1,2] Rostov State University of Economics, 166 M. Gorky St., Rostov-on-Don, 344022, Russia

[1] kochurau@gmail.com

[2] mfoto2@ya.ru

Abstract

The introduction of electronic document management in the courts of the judicial system of the Russian Federation has made it possible to intensify the development of judicial proceedings, speed up the receipt of procedural documents, and reduce costs by eliminating postal expenses. Our article analyzes the legal basis for the use of a Qualified Electronic Signature (QES) and provides recommendations for its correct use. The purpose of this article is to determine the legal significance of a QES, as well as to establish methods for verifying the authenticity of a QES using cryptographic verification methods. The article provides an opportunity for participants in the process to obtain information about the rules for working with and verifying a QES, and also contributes to the development of professional skills of lawyers through the use of the capabilities of electronic judicial document management. The research methodology is based on a systematic research method using general scientific and specific scientific research methods. As a result of the analysis, recommendations are given to participants in the trial on how to significantly speed up the possibility of obtaining court decisions and orders.

Keywords: qualified electronic signature; enhanced qualified electronic signature; verification of the authenticity of the QES; Token; Rutoken 3.0; CryptoPro Program; electronic judicial proceedings.

For citation: *Levina Yu. V., Yakovlev A. V.* Current Issues of Application of Qualified Electronic Signature in Court Proceedings. *Herald of the Russian Law Academy*, 2026, no. 1, pp. 148–154. (In Russ.) https://doi.org/10.33874/2072-9936-2026-0-1-148-154

Введение

Развитие «электронного правосудия» находится в тесной взаимосвязи с концепцией внедрения государством во все сферы общественной жизни цифровых технологий, поскольку судебная власть как разновидность государственной власти также трансформируется под влиянием информационно-коммуникационных технологий [3, с. 17].

Разделяем точку зрения В. А. Галтыхановой и В. О. Давыдовой о том, что «благодаря развитию электронного документооборота в судах в обозримом будущем появится возможность значительно ускорить процесс рассмотрения дел, отказаться от бумажных документов и обеспечить эффективное функционирование электронного правосудия на всех стадиях судебного разбирательства» [1].

Несмотря на активное внедрение цифровых технологий в судебную систему, некоторые аспекты применения КЭП остаются недостаточно изученными и находятся в зоне риска.

Основная часть

Сложности практического применения электронных документов в разных сферах общества заключаются «в основном в обеспечении их юридической силы, поэтому для защиты документов от подделки, подтверждения авторства и целостности данных, признания юридической значимости и обеспечения конфиденциальной информации была введена в эксплуатацию электронная подпись» [2].

Участники судебных процессов знакомы с письменными судебными актами (решения и определения судов), где вместо собственноручной подписи судьи стоит синий штамп, на котором указано, что документ подписан электронной подписью. Указанный штамп содержит расшифровку фамилии, имени и отчества судьи – владельца сертификата, а также указание на номер сертификата.

Представляется, что данная визуализация электронной подписи не в полной мере позволяет удостовериться в подлинности документа.

Для начала необходимо определить, что представляет собой квалифицированная электронная подпись с точки зрения действующего законодательства.

Основным нормативным правовым актом, регулирующим порядок использования КЭП, является Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – Закон об электронной подписи), в котором закреплено, что КЭП приравнивается к собственноручной подписи и обладает юридической силой [4, ст. 2].

Для ее создания используются сертифицированные ФСБ России криптографические алгоритмы.

Выдавать КЭП могут только аккредитованные удостоверяющие центры.

В силу положений ст. 160 и 434 Гражданского кодекса РФ электронные документы с использованием КЭП признаются письменной формой сделки [7, ст. 160, 434].

Арбитражный процессуальный кодекс РФ и Гражданский процессуальный кодекс РФ позволяют подачу документов в суд в электронном виде с использованием КЭП [8, ст. 41.1, 125, 126; 9, ст. 35, 131, 132].

Конкретизирует порядок подачи в федеральные суды общей юрисдикции и проверки электронных документов Приказ Судебного департамента при Верховном Суде РФ [6].

Таким образом, усиленная квалифицированная электронная подпись (КЭП) обладает высшей степенью защиты, соответствующей требованиям Закона об электронной подписи, что делает ее незаменимым инструментом обеспечения аутентичности и целостности электронных документов в судебном делопроизводстве.

В соответствии с указанными нормативными правовыми актами существуют три вида электронной подписи: простая электронная подпись, усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись. Простая электронная подпись – это чаще всего цифровой код, который приходит на телефон в виде сообщения.

Усиленная неквалифицированная электронная подпись – это подпись, защищенная механизмом шифрования; она используется компаниями для подписания внутренних документов, на практике применяется редко.

Усиленная квалифицированная электронная подпись – это подпись, защищенная механизмом шифрования; сам математический механизм шифрования проходит аккредитацию в ФСБ России. Такая подпись выдается специальными аккредитованными центрами. Подделать такую подпись нельзя. Она выдается на специальном носителе – токене и выглядит, как обычная флешка.

Усиленная квалифицированная электронная подпись выполняет функции собственноручной подписи в цифровом мире. Токен – носитель подписи также шифруется в целях предотвращения его использования без владельца подписи.

В дальнейшем в статье речь пойдет именно об усиленной квалифицированной подписи, для удобства обозначения которой будет использоваться аббревиатура «КЭП».

При анализе системы подписания документа КЭП с использованием механизма шифрования было установлено следующее.

Для подписания электронного документа необходимо его создать в формате PDF и загрузить в специальную программу шифрования, например КриптоПро CSP, математический алгоритм которой рассчитывает, сколько в документе гласных, согласных и их последовательность, количество знаков, интервалов, запятых, устанавливает другую индивидуальную информацию.

Иными словами, специальная программа определенным секретным способом шифрует конкретный документ, после чего добавляет к нему цифровую подпись владельца сертификата.

В итоге получается два документа, один это которых – это первоначальный документ в формате PDF, а второй – новый зашифрованный файл в формате .sig (файл с подписью владельца сертификата).

Проверка подлинности КЭП заинтересованным лицом должна осуществляться через электронный сервис «e-trust.gosuslugi.ru», основанный на криптографичес-

ких алгоритмах, сертифицированных ФСБ России, что гарантирует высокий уровень доверия к результатам верификации.

Для проверки подлинности электронной подписи необходимо загрузить на сайт конкретный подписанный документ в формате PDF и прилагаемый к нему файл с электронной подписью в формате .sig.

После нажатия кнопки «проверка» появится результат верификации. Если в будущем будет внесено какое-либо изменение в первоначальный файл PDF, например, появится дополнительная информация, и файл будет подвергнут повторной проверке посредством сервиса «e-trust.gosuslugi.ru», то система ответит, что электронная подпись неверна.

Указанное исключает возможность незаметного внесения изменений в первоначальный документ после его подписания.

Таким образом, документ, подписанный КЭП, должен содержать два файла: исходный файл в формате PDF и файл с электронной подписью в формате .sig.

Вместе с тем на практике к документам, подписанным КЭП, не всегда прилагается файл с электронной подписью в формате sig.

Результаты

Несмотря на четкие требования законодательства, на практике судебные акты, подписанные квалифицированной электронной подписью, публикуются на официальных сайтах судов или размещаются в ГАС «Правосудие» или КАД «МойАрбитр» зачастую только в формате PDF (с визуализацией подписи в виде штампа) без прилагаемого файла в формате .sig (или аналогичного), содержащего криптографическую подпись.

Указанное обстоятельство исключает возможность для лиц, участвующих в деле, проверить подлинность подписи.

Вместе с тем согласно Закону об электронной подписи юридическая сила КЭП обеспечивается криптографической защитой и возможностью проверить ее подлинность.

А как было указано ранее, в отсутствие файла .sig или встроенной электронной подписи проверить, что документ не был изменен после подписания, невозможно, что снижает доверие к электронному документообороту.

Визуальный штамп («подписано КЭП») не имеет криптографической защиты и может быть легко сфальсифицирован. В данном случае не исключаются риски фальсификации и (или) оспаривания документов.

Опубликование судебного акта без файла подписи лишает участников процесса возможности удостовериться, что текст решения (определения) суда не был изменен после подписания судьей.

Использование в судебной системе упрощенного подхода при размещении документов, подписанных КЭП, в открытых источниках создает правовую неопределенность и может стать основанием для оспаривания подлинности судебного акта.

В этой связи рекомендуется разработать единые стандарты публикации судебных актов в электронном виде судов общей юрисдикции и арбитражных судов, со-

ответствующие требованиям Закона об электронной подписи, предусматривающие обязанность публиковать одновременно с документом в формате PDF файл в формате .sig (или использовать встроенную ЭП в PDF, если она соответствует положениям ГОСТ 34.10-2018 [5]).

Таким образом, целесообразно дополнить личный кабинет участников процесса на сайте ГАС «Правосудие» и КАД «МойАрбитр» разделом, в котором выкладывать не только решение суда, подписанное КЭП, но и отдельный файл электронной подписи.

Кроме того, полагаем, необходимо предусмотреть автоматизированную проверку подписи на порталах ГАС «Правосудие» и КАД «МойАрбитр» по аналогии с сервисом «e-trust.gosuslugi.ru».

Выводы

Текущая практика публикации судебных документов без файла электронной подписи снижает уровень доверия к электронному правосудию и создает риски фальсификации судебных актов. Для исправления ситуации необходимо повысить стандарты размещения документов с КЭП в открытом доступе и обеспечить их строгое соответствие закону.

Реализация предложенных мероприятий в полной мере соответствует современным тенденциям развития электронного правосудия.

Пристатейный библиографический список

1. *Галтыханова В. А., Давыдова В. О.* Развитие систем электронного документооборота в судах общей юрисдикции // Вопросы российской юстиции. 2023. № 25.

2. *Новицкая Е. А., Перова М. В.* Применение электронной подписи в системах электронного документооборота // Перспективы развития информационных технологий. 2015. № 26.

3. *Федоренко Н. В., Левина Ю. В.* Электронное правосудие : учебное пособие. Ростов-на-Дону : Издательско-полиграфический комплекс РГЭУ (РИНХ), 2023.

4. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» // СПС «КонсультантПлюс».

5. ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи : межгосударственный стандарт. Введ. 2018-12-04. М. : Стандартинформ, 2018.

6. Приказ Судебного департамента при Верховном Суде РФ от 27 декабря 2016 г. № 251 «Об утверждении Порядка подачи в федеральные суды общей юрисдикции документов в электронном виде, в том числе в форме электронного документа» // СПС «Гарант».

7. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ // СПС «КонсультантПлюс».

8. Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ // СПС «КонсультантПлюс».

9. Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ // СПС «КонсультантПлюс».

References

1. *Galtykhanova V. A., Davydova V. O.* Development of Electronic Document Management Systems in Courts of General Jurisdiction. *Issues of Russian Justice*, 2023, no. 25. (In Russ.)

2. *Novitskaia E. A., Perova M. V.* Application of Electronic Signature in Electronic Document Management Systems. *Prospects for the Development of Information Technologies*, 2015, no. 26. (In Russ.)

3. *Fedorenko N. V., Levina Iu. V.* Electronic Justice: Textbook. Rostov-on-Don: Publishing and Printing Complex of the Russian State University of Economics, 2023. (In Russ.)

4. Federal Law of April 6, 2011 No. 63-FZ "On Electronic Signature" (SPS "ConsultantPlus"). (In Russ.)

5. GOST 34.10-2018. Information Technology. Cryptographic Protection of Information. Processes for the Formation and Verification of Electronic Digital Signatures: Interstate Standard. Introduced on December 4, 2018. Moscow: Standartinform, 2018. (In Russ.)

6. Order of the Judicial Department under the Supreme Court of the Russian Federation of December 27, 2016 No. 251 "On Approval of the Procedure for Submitting Documents to Federal Courts of General Jurisdiction in Electronic Form, Including in the Form of an Electronic Document" (SPS "Garant"). (In Russ.)

7. Civil Code of the Russian Federation (Part One) of November 30, 1994 No. 51-FZ (SPS "ConsultantPlus"). (In Russ.)

8. Arbitration Procedure Code of the Russian Federation of July 24, 2002 No. 95-FZ (SPS "ConsultantPlus"). (In Russ.)

9. Civil Procedure Code of the Russian Federation of November 14, 2002 No. 138-FZ (SPS "ConsultantPlus"). (In Russ.)

Сведения об авторах:
Ю. В. Левина – кандидат экономических наук.
А. В. Яковлев – студент магистратуры.

Information about the authors:
Yu. V. Levina – Candidate of Economic Sciences.
A. V. Yakovlev – Master's Student.

Статья поступила в редакцию 05.05.2025; одобрена после рецензирования 28.08.2025; принята к публикации 19.01.2026.

The article was submitted to the editorial office 05.05.2025; approved after reviewing 28.08.2025; accepted for publication 19.01.2026.