

Крупин Владимир Александрович

студент

Научный руководитель

Фастова Марина Андреевна

канд. юрид. наук, доцент

ФГБОУ ВО «Российский государственный

социальный университет»

г. Москва

ЮРИДИЧЕСКАЯ СИЛА ВИДОВ ЭЛЕКТРОННОЙ ПОДПИСИ (ПЭП, УНЭП, УКЭП) ПРИ ЗАКЛЮЧЕНИИ ДОГОВОРОВ МЕЖДУ ЮРИДИЧЕСКИМИ ЛИЦАМИ

Аннотация: *статья посвящена комплексному анализу применения электронной подписи (ЭП) в договорной практике предпринимательского сектора Российской Федерации. Автор исходит из того, что формальная легализация ЭП (Федеральные законы №63-ФЗ и №476-ФЗ) не устранила разрыва между нормативным регулированием и реальными потребностями бизнеса. Исследуется проблема дифференцированной юридической силы простой (ПЭП), усиленной неквалифицированной (УНЭП) и усиленной квалифицированной (УКЭП) подписей применительно к договорам поставки, аренды, оказания услуг. Установлено, что подмена УКЭП на ПЭП без прямого соглашения сторон влечёт ничтожность сделки. Рассмотрены технологические и организационные риски: компрометация ключей, сбои удостоверяющих центров, реестровая уязвимость. Особое внимание уделено доказыванию факта подписания конкретным лицом. На основе анализа судебной практики и ст. 434, 160 ГК РФ предложены способы снижения рисков: аудиты безопасности, описание порядка фиксации времени, страхование ответственности удостоверяющих центров.*

Ключевые слова: *квалифицированная электронная подпись, детерминированное волеизъявление, декомпозированная аутентификация, компрометация*

ключа шифрования, реестровая транзакционная уязвимость, компрометация криптографического носителя, метаданные цифровой подписи.

Нормативный контекст и проблема экономического оборота.

Электронная подпись (ЭП) перестала быть вспомогательным инструментом. Для предпринимателей электронная подпись стала основным способом выражения воли при дистанционном заключении договоров [1, ст. 5] закрепил три вида ЭП, однако на практике смешение режимов использования порождает споры, длящиеся годами.

Российский бизнес в 2024–2026 годах столкнулся с парадоксом: чем доступнее технологии ЭП, тем труднее доказать суду, что договор подписан надлежащим лицом. Это остро проявляется при сделках между юридическими лицами, где контрагенты экономят на усиленной подписи и некорректно регламентируют (или не регламентируют) порядок использования цифровых подписей [2, с. 5].

Ниже рассматриваются две подтемы, которые структурируют ответы на эти вызовы.

Юридическая сила и соотношение видов электронной подписи: простая электронная подпись, усиленная квалифицированная электронная подпись, усиленная неквалифицированная электронная подпись при заключении договоров между юридическими лицами

Градации силы: ПЭП, УНЭП, УКЭП.

Согласно п. 2 ст. 160 ГК РФ, использование электронной подписи допускается в случаях и порядке, предусмотренных законом или соглашением сторон, а ст. 434 ГК РФ допускает заключение договора в электронной форме. Для подтверждения подлинности электронные документы подписывают электронной подписью (ЭП). Это специальный персональный цифровой код, который прикрепляют к документу. Такие подписанные электронной подписью электронные документы равнозначны бумажным документам с обычной рукописной подписью и имеют такую же юридическую силу.

Простая электронная подпись (ПЭП) и неквалифицированная электронная подпись (УНЭП), о которых пойдёт речь ниже, придают документу юридическую силу только на основании нормативных актов Правительства Российской Федерации или соглашений сторон электронного документооборота. В обоих случаях должна быть возможность проверить личность подписанта.

Электронный документ с квалифицированной электронной подписью (КЭП) обладает такой же юридической силой, что и бумажный с собственноручной подписью, без заключения каких-либо дополнительных соглашений, утверждения нормативных актов.

Если действующее законодательство не обязывает применять конкретный вид подписи для тех или иных действий, то участники электронного документооборота могут использовать любой вид подписи по договоренности между собой [3, с. 21].

Случаи, когда УКЭП не спасает: проблема фактического лица.

УКЭП технически подтверждает владельца сертификата – директора или уполномоченного сотрудника. Но что, если директор уволен, а его сертификат ещё не отозван? Или подписант временно не исполняет обязанности, а на документах появляется его электронная подпись? Суды указывают на то, что электронная подпись является аналогом собственноручной подписи, и Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи» не предусматривает возможность передачи права использования электронной подписи от её владельца иному лицу [4, с. 5].

Вывод: юридическая сила ЭП условна. Она зависит не только от вида подписи, но и от добросовестности проверяющей стороны.

Соглашение об использовании ЭП: обязательный элемент или формальность?

Для того чтобы избежать проблем в договорных отношениях, юридическим лицам желательно заранее письменно согласовать в договоре порядок электронного документооборота. Это критически важно, когда стороны пользуются не усиленной квалифицированной (УКЭП), а иными видами подписей.

Порядок электронного документооборота сторон как минимум должен содержать следующую информацию: конкретный вид ЭП для каждого типа документа (например, счёт – ПЭП, договор – УКЭП), порядок фиксации точного времени подписания (например, через штамп времени удостоверяющего центра), порядок действий при компрометации ключа (например, в течение 6 часов уведомить контрагента).

Без такого соглашения даже УКЭП превращается в дорогой, но бесполезный инструмент.

Например, по одному из арбитражных дел суд удовлетворил иск о взыскании задолженности, приняв в качестве доказательства электронную накладную. При этом суд пояснил, что простой или неквалифицированной электронной подписью можно подтвердить документ только при наличии особого письменного соглашения сторон (в соответствии с законом №63-ФЗ). Данная позиция отражена в постановлении 13-го арбитражного апелляционного суда от 1 октября 2020 года [5, с. 5].

Проблема легитимности клона документа.

Стороны не могут подписывать один и тот же документ дважды: и по ЭДО (ЭЦП), и на бумаге (собственноручно). В силу закона №63-ФЗ допустим только один из этих двух вариантов. В противном случае произойдёт необоснованное задвоение документа путём создания его нелегитимного оригинала.

Суды указывают, что направление претензии по юридическому адресу не имеет правового значения, если документ получен по ЭДО [6, с. 9].

Технологические и организационные риски использования ЭП в договорной работе: защита от компрометации, подтверждение воли стороны и другое.

Использование электронной подписи ускоряет документооборот, но создаёт ряд технологических уязвимостей. Главные риски: компрометация ключа (несанкционированный доступ к носителю или облаку), сбои в работе криптопровайдеров и устаревание алгоритмов шифрования, отсутствие декомпозированной аутентификации. Отдельная проблема – зависимость от аккредитованных удостоверяющих центров: их аннулирование или технический коллапс

(например, отключение электричества) может парализовать подписание контрактов. Кроме того, при использовании простой ЭП (логин/пароль через почту) высок риск подделки воли стороны из-за взлома учётной записи.

Компрометация криптографического носителя (токена).

Ключевым технологическим риском остаётся физическая или сетевая компрометация носителя ключа ЭП. Не исключена возможность того, что ЭП на том или ином документе была проставлена после кражи токена, но до момента отзыва сертификата. Банки и контрагенты не могут отличить легитимную подпись от несанкционированной.

Существует страхование ответственности удостоверяющих центров, которое предусматривает компенсацию расходов на возмещение убытков третьим лицам, если они пострадали из-за некорректной информации в сертификате ключа проверки электронной подписи или реестре сертификатов. Однако в таких договорах обычно есть исключения из покрытия, которые подробно описаны в правилах страхования, например: утрата токена владельцем подписи.

В договоре следует прописывать, что сторона, не отзывавшая сертификат в течение 1 рабочего дня с момента обнаружения пропажи, несёт все риски как свои.

Доказывание: презумпция авторства подписи.

Судебная практика постепенно отходит от презумпции «есть подпись – значит, подписал владелец». Суды требуют дополнительные доказательства детерминированного волеизъявления: логи доступа к рабочему месту, видеозапись из офиса, данные геолокации. Для предпринимателя это означает, что одного файла с УКЭП недостаточно. Нужно вести журнал сессий подписания и фиксировать, какой сотрудник в какое время открывал КриптоПро.

В деле №2–1113/2014 суд сделал вывод о фактическом выполнении бухгалтером трудовых обязанностей «на основании данных, содержащихся в файлах регистрации работы в СЭД» [7, с. 2].

Если сторона дела сомневается в подлинности электронного документа или переписки, суд может назначить судебную компьютерно-техническую экспертизу.

Экспертиза ЭП становится рутинной: проверяется не только криптоматематика, но и метаданные (атрибуты файла, время, устройство).

Реестровая транзакционная уязвимость и проблема отзыва сертификата.

В случае отзыва сертификата в реестре ФНС это происходит не мгновенно. Всегда имеют место человеческий фактор (время на формирование обращения) и технические особенности процесса отзыва. По данным портала государственных услуг, процесс может занимать до нескольких часов. Это «окно уязвимости». Злоумышленник может за эти часы подписать договор, который нанесёт ущерб сторонам.

Решением служит техническое условие в договоре: «Подпись не считается действительной, если сертификат был отозван ранее времени подписания, даже если факт отзыва ещё не отражён в локальном менеджере сертификатов контрагента». Такая оговорка перекладывает проверку на сторону, принимающую подпись.

Способы снижения рисков: от теории к формулировкам в договоре.

На основе анализа двух подтем предлагаются конкретные редакции договорных условий для предпринимателей.

Для снижения рисков по первому блоку (юридическая сила):

- прямо перечислить все виды ЭП, допустимые для каждого документа;
- установить, что споры о подлинности подписи решаются экспертизой, но бремя предоставления журналов подписания лежит на стороне, возражающей против подписи.

Для снижения технологических рисков:

- необходимы регулярные аудиты безопасности, двухфакторная аутентификация и строгое разграничение доступа к ключам;
- обязать каждую сторону страховать риск компрометации ключей;

– включить условие о форс-мажоре при технических сбоях.

Применение электронной подписи в коммерческих договорах не следует рассматривать ни как абсолютный гарант юридической безопасности, ни как безусловный фактор уязвимости сделок. Это инструмент, безопасность и юридическая сила которого прямо пропорциональны уровню проработки договорных условий и технической составляющей. Первая подтема показала, что разграничение ПЭП, УНЭП и УКЭП без прямого соглашения сторон – путь к ничтожности. Вторая подтема обнаружила глубинные технологические бреши: зависимость от инфраструктуры, окна уязвимости реестров, компрометацию токенов.

Предпринимателям сегодня недостаточно купить УКЭП в аккредитованном центре. Необходимо пересмотреть тексты договоров, внедрить внутренние регламенты фиксации сессий и страхование. ЭДО требует не только техники, но и новой договорной культуры.

Список литературы

1. Федеральный закон «Об электронной подписи» №63-ФЗ от 06.04.2011 (ред. от 31.07.2025).
2. Постановление Арбитражного суда Северо-Западного округа от 02.12.2025 №Ф07–13006/2025 по делу №А21–16552/2024.
3. Методические рекомендации по внедрению электронного документооборота в целях обеспечения популяризации использования электронного документооборота среди граждан и организаций Российской Федерации: утв. ФНС России.
4. Постановление Арбитражного суда Поволжского округа от 15.03.2021 №Ф06–42411/2018 по делу №А12–35538/2017; Постановление Девятого арбитражного апелляционного суда от 05.08.2019 №09АП-31911/2019 по делу №А40–42134/2019.
5. Постановление 13-го Арбитражного апелляционного суда от 01.10.2020 №13АП-17288/2020 по делу №А56–3662/2020.

6. Постановление 11-го Арбитражного апелляционного суда от 04.04.2025 по делу №А72–2927/2024.

7. Решение Вязниковского городского суда (Владимирская область) от 01.07.2014 по делу №2–1113/2014.

8. Достовалов П.В. Правомерность использования электронно-цифровой подписи при заключении гражданско-правовых договоров / П.В. Достовалов, О.В. Плетнева // Новое в бухгалтерском учете и отчетности. – 2012.

9. Соловяненко Н.И. Юридическая роль электронной подписи в электронной коммерции / Н.И. Соловяненко // Предпринимательское право в XXI веке: преемственность и развитие. – М.: МЗ Пресс, 2012.

10. Помогаева М.А. Электронное учебное пособие «Электронно-цифровая подпись»: выпускная квалификационная работа / М.А. Помогаева; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. – Екатеринбург, 2019.

11. Крамаров С.О. Криптографическая защита информации: учеб. пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов, Е.Н. Тищенко, П.С. Шевчук. – М.: РИОР: Инфра-М, 2018. EDN YUWDVN

12. Бачило И.Л. Информационное право: учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб., 2015.

13. Правовое обеспечение профессиональной деятельности для специальности «Информационные системы и программирование»: учебник / А.И. Землин, Д.Ю. Левшиц, Е.С. Митякина, М.В. Мамонова. – М.: КноРус, 2024. – 128 с. EDN DLIPYY

14. Бондаренко Н.Л. Правовая и организационная природа процессов цифровизации и регуляторная функция государства в данной сфере / Н.Л. Бондаренко, Ю.Г. Конаневич // Ex Jure. – 2021. – №1. – С. 56–67. DOI 10.17072/2619-0648-2021-1-56-67. EDN OZFAFE

15. Землин А.И. Проблемные вопросы правового регулирования отношений, связанных с использованием высокоавтоматизированных транспортных

средств / А.И. Землин // Журнал российского права. – 2022. – Т. 26. №12. – С. 58–69. DOI 10.12737/jrl.2022.128. EDN BSMKWA

16. Основы права (с практикумом): учебник / А.И. Землин, И.В. Мишуткин, А.А. Агешин [и др.]; под общ. ред. А.И. Землина. – М.: КноРус, 2024. – 373 с. – URL: <https://book.ru/book/955241> (дата обращения: 05.08.2026).

17. Коршунов Н.М. Право интеллектуальной собственности: учебное пособие / Н.М. Коршунов, Н.Д. Эриашвили, В.И. Липунов. – М.: Юнити-Дана, 2011. – 327 с. EDN RAZFHZ