Мучкаева Эльзята Владимировна
магистрант
Научный руководитель
Фастова Марина Андреевна
канд. юрид. наук, доцент

ФГБОУ ВО «Российский государственный социальный университет»
г. Москва

DOI 10.31483/r-168784

ГРАЖДАНСКО-ПРАВОВЫЕ ПОСЛЕДСТВИЯ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ: АНАЛИЗ РИСКОВ И ЗАЩИТНЫХ МЕХАНИЗМОВ

Аннотация: *статья посвящена правовым последствиям использования электронной подписи без надлежащего разрешения в условиях активного смещения гражданского оборота в цифровую среду. Электронная подпись служит надежным способом подтверждения юридически значимых действий (удалённое оформление договоров, направление заявлений, государственная регистрация прав, корпоративные процедуры). Однако с расширением технологий растёт число злоупотреблений: незаконное использование ключей, оформление сертификатов на основе похищенных персональных данных, совершение сделок без подлинной воли владельца. Автор обосновывает, что один лишь факт использования сертификата не подтверждает подлинность волеизъявления; необходима оценка совокупности обстоятельств (способ получения подписи, порядок хранения, процедуры идентификации, поведение сторон после возникновения спора). Предложены меры: ужесточение идентификации, уведомление владельца при каждом обращении, увеличение ответственности удостоверяющих центров, выработка единого судебного подхода.*

Ключевые слова: *электронная подпись, гражданское право, недействительность сделки, цифровой оборот, убытки, удостоверяющий центр, судебная защита.*

Правовое регулирование электронной подписи закреплено в Федеральном законе от 06.04.2011 №63-ФЗ «Об электронной подписи» [1]. Указанный инструмент имеет высокую значимость в обстановке, когда через информационные системы удалённо оформляется заметная доля юридически значимых действий. Для договорной, корпоративной и регистрационной сфер подобная ситуация означает необходимость надёжного механизма, позволяющего достоверно установить личность участника и подтвердить волеизъявление, исходящее от него. В подобных условиях цифровые технологии заняли прочное место в гражданском обороте на его нынешнем этапе развития.

Электронная подпись служит средством для установления лица, подписавшего электронный документ, и удостоверения того, что после её применения содержащиеся в документе сведения сохранились без изменений. В сфере гражданского оборота наибольшую правовую значимость приобретает усиленная квалифицированная электронная подпись; при прямом указании закона на соответствующий случай она обладает тем же юридическим эффектом, что и собственноручная подпись, а ещё формирует высокий уровень доверия к электронному документу [4].

Массовое внедрение электронной подписи породило новый круг юридических угроз. В практике фиксируются случаи, когда сертификаты оформляются на основе незаконно полученных персональных данных, посторонние лица получают доступ к ключам подписи, используется вредоносное программное обеспечение, а гражданам сообщают недостоверные сведения о содержании документов, предлагаемых к подписанию. Итогом подобных действий становятся сделки, по форме соответствующие установленным требованиям, однако в действительности не выражающие волеизъявление лица, указанного в качестве подписанта.

В спорах о применении электронной подписи расхождение между внешним видом действия и тем, было ли оно в действительности выражением воли соответствующего лица, приобретает особую роль. Иная картина складывается при сделках, оформленных в обычной письменной форме: подпись, сам момент подписания, поведение участников и дополнительные обстоятельства нередко поддаются прямой проверке, благодаря чему заметны признаки подделки и ситуации, в которых на сторону сделки оказывалось давление. Иначе устроена цифровая фиксация юридически значимого действия: при внешне безупречном техническом исполнении она способна не показать отсутствие согласия владельца электронной подписи. Поэтому при гражданско-правовой оценке подобных конфликтов нужно обращаться не только к формальным признакам, но и к подробному изучению фактических обстоятельств дела.

При рассмотрении подобных ситуаций одного лишь действующего сертификата ключа проверки электронной подписи недостаточно; отдельно нужно установить лицо, фактически совершившее спорное действие в информационной системе [6, с. 183]. Когда одно устройство используют несколько лиц, токен находится у родственников или работников, пароли доступны посторонним, а сведения для входа в учётную запись сохраняются автоматически, между формальным подписантом и реальным исполнителем возникает расхождение. Тогда предмет спора не сводится к вопросам техники и подлежит оценке как спор гражданско-правового характера.

На практике именно те правовые связи, возникающие при оформлении кредитных договоров, совершении регистрационных действий, принятии корпоративных решений, распоряжении недвижимым имуществом, участии в торгах и заключении договоров поставки, нередко служат источником споров. В перечисленных сферах электронная подпись служит средством, позволяющим быстрее совершать юридически значимые действия, но ускорение цифрового документооборота неизбежно уменьшает срок, необходимый для проверки подлинности намерений сторон. Так, по мере того как возрастает имущественный эффект сделки, для всех её участников должен повышаться уровень осмотрительности.

При рассмотрении документа, удостоверенного электронной подписью, на первый план выходит поведение стороны, принимающей его. Когда участнику были известны сомнительный характер операции, расхождение действий с обычной деловой практикой, явная экономическая невыгодность согласованных условий либо признаки постороннего вмешательства, на безусловную защиту закона он рассчитывать не вправе. Из требований гражданского законодательства проистекает обязанность действовать добросовестно, а потому одна лишь внешняя корректность подписи не способна легализовать поведение, заведомо противоречащее такому стандарту [7, с. 251].

Вопрос о том, каким образом очертить допустимое поведение держателя сертификата ЭП, не имеет простого решения. Полное возложение на него последствий за каждый поступок, совершённый при использовании сертификата, исключается. Одновременно игнорирование базовых требований защиты в цифровой среде не может оставаться без правовой оценки. В случае передачи носителя ключа посторонним, размещения PIN-кодов рядом с устройством, использования заведомо ненадёжных программ либо отсутствия реакции владельца на сигналы о возможной компрометации такое поведение подлежит оценке как грубая неосторожность. При подобных обстоятельствах при распределении убытков необходимо принимать во внимание собственную степень вины владельца подписи.

Правовое положение удостоверяющего центра заслуживает отдельного рассмотрения. Для удостоверяющих центров характерна деятельность, не сводящаяся к обычной коммерческой посреднической модели, поскольку государство наделило такие организации функцией официально удостоверять соответствие выданного сертификата конкретному лицу [8, с. 7]. При ошибках при установлении личности, оформлении сертификата на основании подложных документов, ненадлежащем сохранении сведений либо игнорировании обязательных правил информационной безопасности возникает комплекс неблагоприятных последствий. По данной причине усиленный стандарт требований к удостоверяющим центрам выглядит оправданным как для частноправовой сферы, так и для публичных интересов.

При цифровых отношениях на первый план выходит надлежащее документирование электронных следов. Для действенного восстановления и охраны правового статуса лица, чьи интересы затронуты, требуется сохранять сведения о моменте входа в систему, о последовательности действий пользователя, об использованном IP-адресе, о модели устройства, о способе прохождения идентификации, о направлениях отправки уведомлений и об истории изменения сведений учётной записи. При утрате таких сведений либо неполном отражении выяснение фактических обстоятельств во время разбирательства заметно усложняется. По этой причине обязанность сохранять служебные записи системы о значимых операциях и событиях на разумный срок должна пониматься как значимый компонент правового механизма защиты участников цифрового оборота.

В сфере использования электронной подписи у граждан особенно заметен дефицит правового понимания. Для многих пользователей подобный механизм служит лишь средством технической авторизации в цифровых сервисах, а его правовой эффект нередко остаётся вне поля внимания. Подтверждение документа в электронной форме способно породить кредитные обязательства, выразить согласие на отчуждение имущества, повлечь изменение корпоративных прав и создать иные имущественные обязанности. При непонимании правового смысла совершаемого волеизъявления риск недобросовестных действий возрастает заметно.

Для предотвращения нарушений полезно развивать механизм обязательных уведомлений для пользователей. Пользователю направляют ясные, без задержки поступающие сообщения, где отражены не только само применение подписи, но и правовая природа совершаемой операции: речь идёт о заключении договора займа, направлении заявления о регистрации, изменении корпоративных сведений, представлении налоговой отчётности и иных действиях, имеющих юридическое значение [9, с. 31]. При более высокой точности таких уведомлений владелец быстрее обнаружит подозрительную активность и уменьшит возможный ущерб.

Когда цифровой контроль выстроен по риск-ориентированному принципу, проверочные действия соотносят с характером операции. При необычном действии программа вправе без участия человека запросить ещё одно удостоверение личности, временно заблокировать использование подписи либо инициировать повторную идентификацию. Усиленная верификация уместна там, где затрагивается недвижимое имущество, происходит смена руководителя юридического лица, оформляется крупный кредит или передаются корпоративные права. Такой набор инструментов отвечает задаче сдерживания возможных злоупотреблений на разумной и юридически корректной основе.

В судебном разбирательстве приоритет должен принадлежать не внешней безупречности, а содержательной проверке обстоятельств. Когда спор пытаются свести лишь к вопросу о технической правильности подписи, а фактические условия дела остаются вне рассмотрения, возникает риск, что противоправное поведение получит вид правомерного. По этой причине суду надлежит исследовать не отдельный признак, а всю совокупность значимых данных: каким способом был получен сертификат, какой режим доступа существовал к устройству, как действовали стороны до спорной сделки и после неё, имелась ли у операции хозяйственная логика, насколько быстро она была совершена и каким образом владелец отреагировал после выявления нарушения [10, с. 194].

Для споров, в которых фигурируют электронный документооборот и электронная подпись, оправдано продолжение выработки адресных разъяснений со стороны высших судебных инстанций. При закреплении единых ориентиров по доказыванию, распределению бремени ответственности, проверке добросовестности сторон и правовой оценке последствий несанкционированного применения подписи правоприменение приобретёт большую предсказуемость, а число противоречивых судебных решений уменьшится.

Результативность использования электронной подписи опирается на два основания: надёжность криптографических механизмов и чёткость системы юридических правил, задающих порядок её использования. Когда правовой режим не закрепляет, кто и в каком объёме несёт неблагоприятные последствия спорной

ситуации, не предусмотрено быстрое прекращение действия сертификата, не действуют реальные процедуры возмещения потерь, а судебные органы не придерживаются согласованного подхода к сходным делам, участники электронного обмена начинают воспринимать его как менее надежный. Иная картина возникает там, где прочность технологической инфраструктуры сочетается с детально выстроенными нормами частноправового характера; при такой конфигурации возникают условия для стабильного роста электронных сделок и удалённого взаимодействия субъектов рынка.

Для гражданско-правовой сферы первоочередная задача – установить, сохраняют ли подобные сделки юридическую силу. Когда установлено отсутствие у участника самостоятельного намерения либо искажение его воли обманом, заблуждением или недобросовестным использованием доверия, правовая система получает основание признать сделку недействительной. Наличие актуального сертификата само по себе не служит безусловным подтверждением надлежащего совершения волеизъявления.

При разрешении споров данной категории суд не ограничивается одним лишь фактом технического удостоверения подписи. Он сопоставляет, каким образом был выдан сертификат, соблюдалась ли процедура идентификации личности, имел ли соответствующий участник реальную возможность пользоваться носителем сведений о ключе, как стороны вели себя после заключения сделки и отвечала ли сама операция критерию экономической оправданности. При опоре лишь на техническое подтверждение подписания необходимый баланс между участниками гражданского оборота не достигается.

Вопрос о том, на кого должны лечь неблагоприятные последствия, подлежит самостоятельной правовой оценке. При явной недобросовестности контрагента либо при его молчании при признаках сомнительной сделки соответствующие потери допустимо отнести на его счет. Когда удостоверяющий центр допускает ненадлежащую идентификацию заявителя или не исполняет обязательные требования безопасности, основание для возложения последствий возникает уже в

отношении центра. Иной вариант касается владельца подписи: при грубом несоблюдении правил хранения данных ключа риск неблагоприятного исхода допустимо переложить на него.

Для работы подобных центров оправдана повышенная требовательность к внимательности и проверке сведений. Подобный подход объясняется тем, что они выполняют обязанность с общественной значимостью, удостоверяют, насколько верны данные о лице, которому принадлежит сертификат. При неверном установлении личности либо нарушении порядка выдачи сертификатов возникает риск серьёзного имущественного ущерба для граждан и организаций [11, с. 117]. По указанной причине в работе указанных субъектов нужен усиленный уровень заботливости и осмотрительности.

Обязанность направлять владельцу уведомление при каждом использовании электронной подписи служит действенным средством предупреждения нарушений. При поступлении сообщения без задержки через государственные сервисы, мобильную связь либо электронную почту владелец получает возможность быстро распознать несанкционированное применение. Затем допускается незамедлительно поставить вопрос о приостановлении сертификата, не дожидаясь серьёзных последствий.

Одним из перспективных векторов нормативного развития выступает дальнейшее укрепление механизмов дистанционной идентификации. Вероятность оформления подписи на иное, подменяющее лицо заметно снижается при сочетании многофакторной проверки личности, сверки данных по государственным информационным массивам, биометрических методов и видеофиксации процедуры.

Для данной категории споров единообразие правоприменения имеет первостепенное значение. При поступлении дел на рассмотрение суд не может ограничиваться автоматическим признанием любой электронной подписи безусловно надёжным доказательством; напротив, ему требуется проверить весь комплекс

обстоятельств, относящихся к делу. Лишь при подобной оценке сохраняются добросовестное поведение, справедливое разрешение и устойчивость гражданско-правового оборота.

Для цифровой экономики и гражданского оборота электронная подпись выступает не факультативным дополнением, а базовым условием работы. Её юридическая сила существует лишь при доверительной среде: участники надлежаще идентифицированы, риски распределены разумным образом, а судебная защита выстроена надлежащим образом. При последовательном обновлении законодательства на удостоверяющие центры ложится более высокая ответственность, а практические механизмы защиты пользователей получают развитие; число конфликтов сокращается, устойчивость электронного документооборота возрастает.

Список литературы

1. Федеральный закон «Об электронной подписи» №63-ФЗ от 06.04.2011 // Собрание законодательства РФ. – 2011. – №15. – Ст. 2036.

2. Федеральный закон «О персональных данных» №152-ФЗ от 27.07.2006 // Собрание законодательства РФ. – 2006. – №31 (ч. I). – Ст. 3451.

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» №149-ФЗ от 27.07.2006 // Собрание законодательства РФ. – 2006. – №31 (ч. I). – Ст. 3448.

4. Федеральный закон «Гражданский кодекс Российской Федерации (часть первая)» №51-ФЗ от 30.11.1994 // Собрание законодательства РФ. – 1994. – №32. – Ст. 3301.

5. Федеральный закон «Гражданский кодекс Российской Федерации (часть вторая)» №14-ФЗ от 26.01.1996 // Собрание законодательства РФ. – 1996. – №5. – Ст. 410.

6. Бачило И.Л. Информационное право: учебник для магистров / И.Л. Бачило. – 3-е изд., перераб. и доп. – М.: Юрайт, 2013. – 564 с.

7. Копылов В.А. Информационное право: учебник / В.А. Копылов. – 2-е изд., перераб. и доп. – М.: Юристъ, 2003. – 512 с.

8. Хабриева Т.Я. Право в условиях цифровой реальности / Т.Я. Хабриева, Н.Н. Черногор // Журнал российского права. – 2018. – №1(253). – URL: https://cyberleninka.ru/article/n/pravo-v-usloviyah-tsifrovoy-realnosti (дата обращения: 30.07.2026).

9. Талапина Э.В. Алгоритмы и искусственный интеллект сквозь призму прав человека / Э.В. Талапина // Журнал российского права. – 2020. – №10. – С. 25–39. DOI 10.12737/jrl.2020.118. EDN DLFNEL

10. Гусаим И.В. Мошенничество при сделках по распоряжению недвижимым имуществом с использованием электронно-цифровой подписи / И.В. Гусаим // Пробелы в российском законодательстве. – 2023. – №2. – С. 193–197.

11. Минбалеев А.В. Перспективные направления правового регулирования персональных данных / А.В. Минбалеев // Юридический вестник Дагестанского государственного университета. – 2024. – Т. 52. №4. – С. 115–121. DOI 10.21779/2224-0241-2024-52-4-152-156. EDN BJNVQZ