

## ПРАКТИКА НАРУШЕНИЯ 63-ФЗ «ОБ ЭЛЕКТРОННОЙ ПОДПИСИ» В КОНТЕКСТЕ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ

*Соколов А.С., Кондакова В.Н.*

*Алтайский государственный университет, г. Барнаул*

*email: Sokolov120289@mail.ru.*

**Аннотация.** В настоящее время появляется все больше информационно-коммуникационных технологий (ИКТ), которые не остались без внимания преступных сообществ. Данная статья предполагает анализ правоприменительной практики, законодательной базы и экспертных мнений, касающихся квалификации нарушений при заключении договоров займа и кредитных договоров с использованием электронной подписи как мошенничества с использованием электронных средств платежа.

**Ключевые слова:** микрофинансовая организация (МФО), заемщик, займодавец, электронно-цифровая подпись (ЭЦП), мошенничество, электронные средства платежа.

За последнее десятилетие рынок микрофинансовых организаций в Российской Федерации вырос до рекордных объемов – 212 миллиардов рублей составил совокупный портфель микрозаймов в 2019 году. Объем выданных микрозаймов вырос на 25 %, составив 412 млрд рублей [1]. Видится вполне логичным, что такие объемы саморегулируемого рынка становятся полем для мошеннических действий, жертвами которых становятся как сами микрофинансовые организации, их клиенты, так и посторонние граждане. Суть проблемы, изучению которой посвящена данная статья, заключается в том, что многие участники рынка МФО заключают сделки с заемщиками дистанционно – без личного контакта клиента с компанией, а для подписания таких договоров клиенту направляется смс сообщение с кодом, при вводе которого в специальное поле на сайте организации договор считается подписанным.

Описанный путь заключения договоров не противоречит Федеральному Закону №353 "О потребительском кредите (займе)" от 21.12.2013 [2, с. 7], однако возникает ряд вопросов о действительности такого рода подписи, ее равнозначности подписи рукописной и о правовой оценке такого документа с точки зрения Федерального закона от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи" [3, с. 17]. Нередки случаи, когда в правоохранительные органы обращаются граждане, от имени которых были заключены договора с МФО, но средствами, поступившими на их счет по договору, они не пользовались. Граждане обращаются в правоохранительные органы и получают постановление об отказе в возбуждении уголовного дела в связи с тем, что они не понесли материального ущерба (пример – проверка №26625, зарегистрированная в КУСП отдела полиции УМВД г. Барнаула по Железнодорожному району). Однако, когда МФО подает иск в суд о возврате суммы долга, процентов, штрафа и пени по договору займа к заемщику, суды, как правило, встают на сторону истца, и рассматривают дело в рамках гражданского судопроизводства, руководствуясь при вынесении решения ФЗ № 353 «О потребительском кредите (займе)» [4]. Практика по возбуждению уголовных дел по заявлениям пострадавших от мошеннических действий лиц практически отсутствует, отсутствует также распространенная практика судебной защиты пострадавших лиц, но имеются основания полагать, что такая ситуация сложилась из-за нежелания правоохранительных органов и судов рассматривать заключение договоров описанным выше способом в контексте Федерального закона «Об электронной подписи». Микрофинансовые организации в исковых заявлениях, а

также в заявлениях в полицию зачастую употребляют формулировку «Договор займа заемщик подписал посредством электронной подписи (с использованием SMS-кода). Порядок заключения Договора займа предусмотрен «Общими условиями Договора микрозайма» и «Правилами предоставления микрозаймов ООО МФК «Честное слово»» [4], что считаем в корне неверным.

Формируя положения профильного федерального закона, законодатель, очевидно, преследовал цель формирования простых и понятных правил поведения для участников соответствующих правоотношений, однако, подошел к своей роли несколько непоследовательно, не приведя в соответствие новому нормативно-правовому акту уже изданные законы. Например, 353-ФЗ "О потребительском кредите", в котором указывается возможность подписания договора электронной подписью, но не конкретизируется сам термин ЭЦП, их разновидностей.

Рассмотрим положения ФЗ №63, а именно к статьям 5 и 6. В статье 6 Закон разъясняет, что существует несколько видов электронно-цифровой подписи, в том числе простая (неквалифицированная) и усиленная. Различают также подвиды: усиленная квалифицированная электронная подпись и усиленная неквалифицированная. Квалифицированная электронная подпись – это такая электронная подпись, ключ проверки которой указан в квалифицированном сертификате [3, с. 5]. Соответственно, согласно ст. 6 Закона об электронной подписи документом, равнозначным документу на бумажном носителе, признается электронный документ, подписанный электронной подписью.

Сложившаяся практика не возбуждения уголовных дел по ст. 159.3 несет в себе огромный преступный потенциал – на сегодняшний день вышеописанным образом происходит заключение договоров не только МФО, но и рядом банков, специализирующихся на потребительском кредитовании, таких как «Тинькофф-банк», «Хоум Кредит энд Финанс Банк». Между тем, нежелание правоохранительных органов открывать практику расследования подобных дел по многочисленным заявлениям может способствовать (и способствует) безнаказанным и неконтролируемым действиям преступников. Злоумышленники могут:

- лишать собственника принадлежащего ему имущества;
- получать денежные средства от имени других лиц в кредитных и микрофинансовых организациях;
- незаконным путем производить смену собственника юридического лица;
- лишать участника гражданско-правовых правоотношений возможности подачи заявок на конкурсные процедуры в сфере закупок для государственных и муниципальных нужд при хищении подписи.

Осуществляя анализ способов совершения мошенничеств с использованием электронной подписи, стоит указать на две группы таких способов: технические (технологические) и социального взаимодействия. Среди способов технического характера выделим создание на физическом носителе из ненадежного источника электронной подписи программы-шпиона, которая может получить доступ к коду подписи и коду ее проверки. Другим средством противоправного получения сведений о ключе подписи и ее проверки является внедрение в компьютер пользователя подписи вредоносных программ с последующим получением данных о ключе подписи и ключе проверки, и это только в том случае, если мы говорим о том виде электронной подписи, который позволяет равносильно собственноручной подтвердить личность подписанта. Способы мошенничества на основе социального взаимодействия более распространены и разнообразны, начиная от тайного хищения носителя подписи (а в случае подписания простой неквалифицированной подписью – устройства, с помощью которого был направлен код для подписания) до введения в заблуждение сотрудников удостоверяющего центра или их незаконные действия по выдаче электронной подписи не уполномоченному лицу. Здесь можно указать и

на получение подписи по поддельным документам, в том числе, заверенным нотариусом доверенностям [6, с. 2-3].

Специфику расследования такого вида преступлений составляет установление и процессуальное закрепление следов совершенного преступления, а они остаются в силу закономерностей правового и технического режима использования подписи. Типичными следами по делам этого вида выступают:

- устройства-электронные накопители информации с файлами, имеющими формат электронной подписи;
- сертификаты ключей проверки электронной подписи на электронном и (или) бумажном носителях;
- договоры и бухгалтерские документы с удостоверяющим центром о создании и выдаче электронной подписи;
- компьютерные файлы в виде электронных документов, подписанные электронной подписью;
- программное обеспечение для проверки подлинности сертификатов ключей электронной подписи, а также смартфоны с хранящейся в них информацией.

С сожалением отмечаем, что по приведённой нами в пример проверке № 26625 отделом полиции не был изучен ни один из вышеперечисленных следов, не был запрошен или истребован ни один документ, позволивший бы установить факт мошенничества.

Обстоятельствами, подлежащими установлению при расследовании мошенничеств этого вида, которые детализируют предмет доказывания, выступают:

- наличие законного режима обладания имуществом потерпевшим до совершения преступления;
- выдача уполномоченным центром электронной подписи на имя потерпевшего при отсутствии его надлежащего уведомления;
- использование персональных данных потерпевшего для совершения подлога при выдаче электронной подписи на его имя;
- факт использования электронной подписи при заключении договора по отчуждению имущества, принадлежащего потерпевшему;
- переход права собственности от потерпевшего к другому лицу для реализации имущества или совершения других незаконных сделок с ним [8, с. 50].

В заключение отметим, что выявленная проблема в квалификации многочисленных инцидентов с неправомерным использованием ЭЦП как преступлений, подпадающих под действие ст. 159.3 Особенной части Уголовного кодекса Российской Федерации влечет за собой укоренение порочной практики игнорирования развивающегося рынка электронного документооборота, что в определенном смысле является высоким риском для государства, вкладывающего немалые средства в развитие информационных технологий [10]. Использование ЭЦП, несмотря на появление и регулярное обновление соответствующего Федерального закона, остается белым пятном на поле правоприменительной практики. Почему складывается такая практика – большой вопрос, рассматривать который необходимо как на политическом, так и на научно-техническом и юридическом уровнях, кроме того, в контексте развития информационных технологий, следует уделить особое внимание развитию соответствующих компетенций сотрудников полиции, отвечающих за экономическую безопасность, так как именно они проводят первоначальные проверки по заявлениям о мошенничестве в описанных выше ситуациях, и проверки эти в большинстве случаев заканчиваются ничем.

В рамках же гражданско-правовых отношений с 2017 по 2019 годы нами было найдено только одно судебное решение, признающее договор, подписанный простой неквалифицированной электронной подписью, незаключенным на основании

несоответствия подписания договора ФЗ №63, и данный факт требует обратить на себя внимание – решение Железнодорожного районного суда г. Улан-Удэ вступило в законную силу, но этого мало для создания устойчивой практики [9].

В связи с отсутствием правоприменительной практики квалификации нарушений 63-ФЗ "Об электронной подписи" по ст. 159 Уголовного кодекса РФ, мы делаем вывод о необходимости проведения масштабной разъяснительной работы с правоохранительными органами и органами прокуратуры с целью уточнения общественно опасных последствий неправомерного использования электронно-цифровой подписи.

#### **Библиографический список**

1. Алексеев И., Уклеин И., Сараев А. Итоги 2019 года для рынка МФО и прогноз на 2020-й: период трансформации [Электронный ресурс]. - Режим доступа: <https://www.raexpert.ru/researches/mfo/2019> (дата обращения 05.10.2020).
2. Федеральный закон №353 "О потребительском кредите (займе)" от 21.12.2013 // Российская газета, 23 декабря 2013 г. № 6265.
3. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи" // Российская газета, 8 апреля 2011 г. № 5451.
4. Решение № 2-2912/2018 2-2912/2018~М-1281/2018 М-1281/2018 от 21 мая 2018 г. по делу № 2-2912/2018. [Электронный ресурс]. - Режим доступа: <https://sudact.ru/regular/doc/УКijWzz0CGr8/> (дата обращения 05.10.2020).
5. Решение Железнодорожного районного суда г. Барнаула № 2-1542/2019 от 6.05.2019 г.
6. Бондаренко Ю. А. Особенности расследования мошенничества, совершенного с использованием электронной подписи // Гуманитарные, социально-экономические и общественные науки. 2020. - №3 – С.1–7.
7. Бахимова Л.А., Латышова Л.А., Мифтахова Л.Х. Методы защиты от фальсификации электронной подписи // Вестник Казанского технологического университета. - 2016. - №14. - С. 123 - 125
8. Бессонов А.А. О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник Университета имени О.Е. Кутафина. - 2019. - №3 (55). – С. 46-52.
9. Решение № 2-2395/2017 от 5 июня 2017 г. по делу № 2-2395/2017. [Электронный ресурс]. - Режим доступа: <https://sudact.ru/regular/doc/ЗЕО022QkqUNO/> (дата обращения: 10.10.2020).
10. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 27.10.2020).

#### **PRACTICE OF VIOLATION OF 63-FZ "ON ELECTRONIC SIGNATURE" IN THE CONTEXT OF FRAUD ACTIONS**

*Sokolov A.S., Kondakova V.N.  
Altai State University, Barnaul  
email: Sokolov120289@mail.ru*

**Abstract.** Today there are a lot of information and communication technologies (ICT) appear, which haven't gone unnoticed by criminal communities. This article assumes an analysis of law enforcement practice, legislative framework and expert opinions regarding the qualification of violations when concluding loan agreements and credit agreements using digital signatures as fraud with modern ways of payment.

**Keywords:** microfinance organization, borrower, lender, digital signature (EDS), fraud, digital means of payment.