Нажмите «Подписаться»

Как электронная подпись применяется сегодня кредитно-финансовыми организациями и каких изменений в регулировании этого процесса можно ожидать

Федеральный закон «Об электронной подписи» (№ 63 ФЗ) был принят более 10 лет назад, в 2011 году, и все эти годы постоянно совершенствовался. В период с 10 июля 2012 года до 28 декабря 2022-го к нему было принято 16 изменяющих документов. Их цели — минимизировать риски мошенничества с использованием ЭП и добиться однозначной идентификации субъекта, ее применившего

Текст
АЛЕКСАНДРА КРЫЛОВА,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Зачем банкам электронная подпись?
Федеральный закон № 63-ФЗ определяет электронную подпись как информацию в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным способом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

По сути, она является неотъемлемой частью, инструментом или атрибутом безбумажного документооборота, а без него, в свою очередь, невозможна цифровизация ни одной из сфер, включая область финансов.

Как следствие цифровизации банковского бизнеса происходит перетекание бóльшей части аудитории в дистанционные каналы обслуживания, что обеспечивает сокращение затрат на содержание филиальной сети. Но для оказания банковских услуг и платежных сервисов в режиме онлайн необходимо использовать электронную подпись.

По словам **Юлии Задубровской,** руководителя направления безопасности финорганизаций компании Infosecurity (входит в ГК Softline), сегодня электронные подписи применяются для открытия и закрытия банковских счетов, подписания договоров на предоставление кредитов или других банковских услуг, идентификации клиентов, подтверждения операций. «Клиенты могут использовать электронную подпись для подтверждения операций, таких как переводы денег или изменение условий договоров», — пояснила она.

Применение электронных подписей позволяет банкам перевести в электронный вид как внутренний документооборот, так и документы, которые им предоставляют клиенты, а это значительно снижает вероятность их потери или уничтожения и упрощает документооборот, считает Оксана Васильева, доцент департамента правового регулирования экономической деятельности Финансового университета при Правительстве РФ.

Для многих клиентов, особенно представителей молодого поколения, возможность подписывать документы дистанционно имеет довольно высокую ценность, благодаря ей они получают от взаимодействия с кредитно-финансовой организацией положительный опыт. «Никто не любит лишний раз тратить время на поездки в банковские отделения для подписания бумажек», — констатировал **Николай Адеев,** основатель сервиса Nopaper Office.

Для каждой из перечисленных выше задач кредитно-финансовые организации используют различные виды электронных подписей.

Виды ЭП и их применение в банках

В ФЗ № 63 от 25 марта 2011 года выделяется два вида электронных подписей: простая и усиленная. Усиленная электронная подпись, в свою очередь, может быть неквалифицированной и квалифицированной. «Выбор конкретного вида электронной подписи зависит от требований законодательства и политики конкретного банка», — пояснила Юлия Задубровская.

Чаще всего кредитно-финансовые организации применяют простую электронную подпись, которая представляет собой СМС с кодом или парой логин — пароль, поступающие на телефон клиента. При вводе кода или логина и пароля создается простая электронная подпись именно этого человека и фиксируется время ее формирования. «Простая электронная подпись позволяет клиенту заключать электронные договоры с банком (например, договор на выдачу карты или выдачу кредита), а также подтверждать перевод со счета или оплату с карты», — заключил **Сергей Казаков,** руководитель удостоверяющего центра СКБ Контур.

В силу простоты и удобства использования простая электронная подпись распространена среди российских граждан. **Антон Немкин,** член комитета Госдумы по информационной политике, информационным технологиям и связи, оценил количество обладающих ею россиян в более чем 100 млн человек.

«Особенность простой электронной подписи — в том, что она имеет юридическую силу только при заключении дополнительного соглашения между сторонами документооборота. В таком соглашении прописывается, что именно считать ключом простой электронной подписи — СМС-код или пару логин — пароль, какие документы ею подписывать», — пояснил Сергей Казаков. По его словам, обычно дополнительное соглашение банки заключают с новым клиентом или добавляют пункт об использовании простой электронной подписи в основной договор или оферту.

По сравнению с простой электронной подписью неквалифицированная электронная подпись более надежна. Она считается усиленной, поскольку для ее формирования используется криптография, а компрометировать закрытый ключ сложнее. Вместе с тем усиленная неквалифицированная электронная подпись (УНЭП) не является аналогом собственноручной подписи клиента по умолчанию. Для того чтобы признать ее таковой, банку и клиенту опять-таки требуется подписать дополнительное соглашение.

После этого у клиента появляется возможность использовать усиленную неквалифицированную электронную подпись при дистанционном банковском обслуживании. «А внутри кредитной организации УНЭП становится инструментом корпоративного документооборота. Сотрудники банка соглашаются на использование неквалифицированной электронной подписи и могут подписывать ей кадровые документы или обмениваться служебными документами во внутренней системе», — рассказал Сергей Казаков.

Аналогом собственноручной подписи выступает усиленная квалифицированная электронная подпись (УКЭП). В соответствии с требованиями ФЗ «Об электронной подписи» средства криптографической защиты, которые применяются для ее формирования, должны быть сертифицированы ФСБ РФ, а ее подлинность подтверждает квалифицированный сертификат ключа проверки электронной подписи, выданный одним из аккредитованных удостоверяющих центров.

Для применения УКЭП банку не требуется заключать дополнительные соглашения с клиентами, потому применение этого вида электронной подписи в кредитно-финансовых организациях намного шире.

«С помощью УКЭП клиенты-юрлица могут через банк открыть ООО или обмениваться с банком электронными документами, например отправлять отчеты по кредитам. Сотрудники кредитных организаций также используют квалифицированную электронную подпись для взаимодействия с другими ведомствами. При этом в рамках "пилота" они прикладывают к квалифицированной электронной подписи машиночитаемую доверенность — аналог бумажной доверенности на подписание документов. Таким образом, квалифицированная электронная подпись позволяет сотрудникам быть законными представителями своей кредитной организации. Также УКЭП применяется банками при работе в личном кабинете Центробанка РФ или на внешнем портале Единой платформы внешнего взаимодействия. Например, просматривать запросы и предписания Центробанка и отвечать на них», — добавил Сергей Казаков.

В некоторых случаях квалифицированная электронная подпись используется и в отношениях банка с физлицами. Наиболее частый сценарий — оформление ипотеки. Если сделка проводится в электронном виде, то все документы по ипотеке физлицо подписывает с помощью усиленной квалифицированной электронной подписи. При этом часто УКЭП выдается конкретно под этот случай и сразу в отделении банка — квалифицированный сертификат выпускает удостоверяющий центр банка или УЦ-партнер.

Кстати, как отмечает **Андрей Игнатов,** менеджер продуктов Рутокен компании «Актив», большинство изменений, внесенных в 63-ФЗ за последние 4-5 лет, касались именно выдачи усиленной квалифицированной электронной подписи юридическим и физическим лицам.

Риски, реальные и потенциальные

Простая электронная подпись наименее защищена. «СМС-код знают многие: банк, оператор сотовой связи, СМС-агрегаторы — и только потом клиент, на чье устройство он в конце концов поступает», — прокомментировал Николай Адеев. По словам эксперта, код может быть перехвачен на любом из этапов пути к клиенту и даже на его собственном телефоне.

Самый простой способ перехвата — звонок мошенников. В подтверждение этого тезиса эксперт привел данные Центробанка. Согласно им, во втором квартале 2022 года 54% всех мошеннических схем в финансовой сфере — социальная инженерия, цель которой — узнать именно код из СМС.

А в начале этого года и вовсе возник прецедент, встревоживший многие банки, занимающиеся онлайн-кредитованием. «17 января Верховный Суд признал недействительным кредит, оформленный мошенниками. Клиент банка назвал злоумышленникам код из СМС и, сам того не зная, подписал кредитный договор на 200 тыс. рублей под 19% годовых. Суд встал на сторону клиента, напоминает Николай Адеев.

Любое лицо, получившее доступ к телефону с СМС-кодом для формирования простой электронной подписи, может переводить деньги или подписывать договоры с банком от имени клиента. «Кто несет ответственность в таком случае, банку стоит прописать в соглашении об использовании простой электронной подписи. Например, указать в нем, что клиент обязан предпринять меры для предотвращения компрометации ключа простой электронной подписи или возложить ответственность за негативные последствия компрометации простой электронной подписи на клиента, пояснил Сергей Кузнецов.

В компании «Актив» отмечают, что использование простой электронной подписи несет в себе риски и для самих кредитно-финансовых организаций. Так, лицо, на которого указывает ПЭП под документом, может заявить, что подпись фальсифицирована и ему не принадлежит, или что документ после подписания был изменен без его ведома. Еще одна группа рисков связана с юридической значимостью ПЭП в случае судебного разбирательства. «Простая электронная подпись не обеспечивает контроль целостности и подтверждения подлинности при подписании электронных сообщений», — заключил Андрей Игнатов. Подтверждением тому и служит решение Верховного Суда от 17 января этого года.

«Кредитные договоры являются одними из самых высокорисковых как для банка, так и для клиента, поэтому их нельзя подписывать кодом из СМС, — убеждена **Дарья Верестникова,** эксперт по безопасности SafeTech и сооснователь сервиса Noparer. — У СМС-кода есть преимущество — ничего не нужно скачивать, чтобы подписать документ, и для некоторых низкорисковых операций она подходит. Поэтому в нашем сервисе мы реализовали усиленную СМС-подпись. В отличие от обычного кода из СМС она имеет более высокую доказательную базу: СМС — дополнительное разрешение на подписание документа, а при подписании собирается хэш документа».

Что касается усиленных электронных подписей, то подделать их намного сложнее. Так что, как отмечает, **Евгения Боднар,** юрист и эксперт по банкротству компании «Финансово-правовой альянс», риски их мошеннического использования заключаются в классических методах работы преступников. Это похищение электронного носителя подписи (USB-ключа), оформление электронной подписи по подложным документам или незаконно полученным личным документам реальных лиц (паспорт, ИНН, СНИЛС и т.д.). Как правило, с помощью таких криминальных манипуляций мошенникам удается осуществлять транзакции с расчетных счетов организаций или физических лиц для хищения денежных средств, оформления кредитов и микрозаймов и т.д.

Немалый ущерб от неправомерного использования усиленных электронных подписей могут понести юридические лица. «Получив доступ к учетной записи и электронной подписи, с использованием которых осуществляется взаимодействие в системах интернет-банкинга, злоумышленник может направить поручение о переводе денежных средств со счета организации в банке. Как вариант у него есть возможность, используя УКЭП организации, изменить информацию о ее руководителе, а затем уже на вполне законных с виду основаниях осуществлять управление денежными средствами организации от своего имени», — рассказала Юлия Задубровская. Кроме того, и в самих банках неправомерное использование электронной подписи работника может привести к краже денежных средств как банка, так и его клиентов, напомнила она.

По мнению эксперта, помимо внешних причин (подделки электронной подписи, утечки данных из удостоверяющего центра, нарушения клиентами требований к защите информации, дей-

ствий хакеров) учащению случаев неправомерного использования способствуют и внутренние причины. Это отсутствие должного внимания при проверке новых клиентов банка или при контроле платежей, недостаточная техническая обеспеченность информационной безопасности, нарушение работниками банка требований по защите информации.

«Желание заполучить нового клиента, спешка, недостаточная информационная подготовка работника могут привести к небрежной проверке документов. Отсутствие контроля за типом и способам направляемых запросов на предоставление финансовых услуг могут позволить мошеннику украсть деньги клиента», — заключила Юлия Задубровская.

Куда двигаться дальше?

Благодаря совершенствованию нормативной базы за время, минувшее с 2019 года, когда достоянием общественности стали первые серьезные случаи мошенничества с электронной подписью, рост случаев неправомерного использования разных видов электронной подписи удалось стабилизировать.

По мнению Оксаны Васильевой, динамика нарушений использования электронной подписи замедлилась. «В 2018-2019 годах была решена одна из главных проблем в этой области — получить электронную подпись на другого гражданина стало сложнее. Так что при оформлении кредита или ипотеки онлайн-банки сегодня рискуют меньше», — констатировала эксперт.

Вместе с тем в сфере применения электронной подписи она и в 2023 году видит несколько проблем, ожидающих своего решения. Так, электронная подпись до сих пор не позволяет со стопроцентной гарантией идентифицировать субъекта, подписавшего документ онлайн. При предоставлении в суд документа, подписанного электронной подписью, скорее всего, придется его заверять у нотариуса, а это дополнительная трата времени и средств. Кроме того, обычному пользователю активировать электронную подпись порой весьма непросто, поэтому часто приходится обращаться к услугам специалистов. И утверждать, что риск мошенничества с электронной подписью полностью исключен, до сих пор нельзя.

С Оксаной Васильевой согласна и Евгения Боднар, считающая, что устранить риск похищения денежных средств или причинения ущерба иным способом на сегодняшний день не удается. «Особенно актуальна проблема защиты от незаконного использования ЭЦП в банкротных процедурах, когда утвержденный судом арбитражный управляющий распоряжается денежными средствами несостоятельного должника в кредитно-финансовых учреждениях и при реализации имущества на торговых площадках», — отметила она и добавила, что при банкротстве крупных предприятий кредиторы заинтересованы в справедливом распоряжении конкурсной массой, поэтому незаконное вмешательство третьих лиц в деятельность арбитражного управляющего может причинить существенный вред интересам многих субъектов.

Как будут решаться эти проблемы? Путем запретов или поиска прогрессивных технологических сервисов, уже умеющих их указанные трудности? Время покажет. Б.О