Соответствие простой электронной подписи UIDM требованиям законодательства

Оглавление

Нормативно-правовые акты
Соответствие простой электронной подписи в UIDM требованиям нормативно-правовых актов

В системах дистанционного банковского обслуживания существует необходимость юридически значимого подтверждения пользователем совершаемых операций и неотказуемость пользователя от них в дальнейшем. Такое юридически значимое подтверждение выполняется путём подписания данных об операции электронной подписью.

Для подписания пользователями выполняемых операций (в том числе по переводу денежных средств) в UIDM используется простая электронная подпись[1].

Нормативно-правовые акты

Требования действующих нормативно-правовых актов (п 5.1 Положения Банка России № 683-П[2]) устанавливают, что в целях обеспечения целостности электронных сообщений и подтверждения их составления пользователем кредитные организации должны обеспечивать использование:

- усиленной квалифицированной электронной подписи,
- усиленной неквалифицированной электронной подписи, или
- аналогов собственноручной подписи, кодов, паролей и других средств, в том числе простой электронной подписи, при условии использования средств криптографической защиты информации, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

Средства имитозащиты — аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации[3].

В соответствии с этим определением, имитозащита — защита от навязывания ложной информации, в том числе защита от модифицирования информации для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования такой информации.

Соответствие простой электронной подписи в UIDM требованиям нормативно-правовых актов

Выполняемые UIDM простые электронные подписи требованиям регулятора соответствуют.

Функция имитозащиты реализуется добавлением одноразового пароля (OTP), который пользователь вводит для подтверждения выполнения операции, в данные, используемые для расчёта цифровой подписи этих данных. Цифровая подпись представляет собой хеш-сумму (хэш-код), рассчитанную по алгоритму в соответствии с ГОСТ 34.11—2012.

Цифровую подпись можно проверить по цепочке протоколируемых событий и удостовериться, что операция подписана конкретным пользователем.

Одноразовый пароль, используемый для подтверждения выполнения операции, известен только пользователю. Одноразовый пароль перестаёт действовать после его использования либо через короткое время после его направления пользователю.

Выполняемая UIDM простая электронная подпись уникальна и однозначно связана с конкретным пользователем; в данных аудита (протоколировании события) подписания платёжного или иного документа простой электронной подписью сохраняются:

- сведения об уникальном идентификаторе пользователя в UIDM,
- контактные данные пользователя, в том числе мобильный телефон, на который был отправлен одноразовый пароль,
- использованный пользователем одноразовый пароль подтверждения выполнения операции.

---

1. Часть 2 статьи 5 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи».
2. Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».
3. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

Прочтите также

- Подписание документов простой электронной подписью
- Руководство по финансовым операциям и электронной подписи