конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто’2023»

О нормативных изменениях для финансовой отрасли, касающиеся применения СКЗИ и средств ЭП

Информационное письмо Банка России от 16.03.2023 № ИН-017-56/22

Борис Зинюк

Банк России

(Федеральный закон от 10.07.2002 N 86-ФЗ)

Статья 57.4. Банк России по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, … , устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента…
(**Положение Банка России от 17 апреля 2019 года № 683-П**)

Статья 76.4-1. Банк России по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, … , устанавливает обязательные для некредитных финансовых организаций требования к обеспечению защиты информации…
(**Положение Банка России от 20.04.2021 N 757-П**)

Статья 76.9-6. Банк России по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, … , устанавливает обязательные для лиц, оказывающих профессиональные услуги на финансовом рынке, требования к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций…
(**Положение Банка России от 17.10.2022 N 808-П**)

Положение Банка России от 17 апреля 2019 года № 683-П

(в ред. Указания Банка России от 18.02.2022 N 6071-У)

Подпункт 5.1 Кредитные организации должны обеспечить целостность электронных сообщений и подтвердить их составление уполномоченным на это лицом.

В целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом кредитные организации должны обеспечивать реализацию мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

....

... вступили в силу с 1 октября 2022 года (Указания Банка России от 18.02.2022 N 6071-У).

Положение Банка России от 20.04.2021 N 757-П

(в ред. Указания Банка России от 18.02.2022 N 6071-У)

Глава 1
Пункт 1.9. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить целостность электронных сообщений и подтвердить их составление уполномоченным на это лицом.

В целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать реализацию мер по использованию **усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи** или иных **СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения**.

До **31.03.2023** включительно не применяются меры воздействия в отношении участников финансового рынка за нарушение требований гл. 1 (Информационное письмо Банка России от 30.12.2022 N ИН-018-38/157).

Положение Банка России от 17.10.2022 N 808-П

1.3. Лица, оказывающие профессиональные услуги на финансовом рынке, должны осуществлять свою деятельность в рамках процессов (направлений) защиты информации, указанных в пункте 1.1 настоящего Положения, с помощью средств криптографической защиты информации (далее - СКЗИ) в соответствии с технической документацией на СКЗИ, а также в соответствии с … ПКЗ-2005.

1.5. …

При применении усиленной квалифицированной электронной подписи лица, осуществляющие актуарную деятельность, должны выполнять требования эксплуатационной документации к средствам электронной подписи.

Начало действия положений документа - 01.04.2023 .

Исключения!

- ✓ абзацем третьим подпункта 5.1 пункта 5 Положения № 683-П
- ✓ абзацем третьим пункта 1.9 главы 1 Положения № 757-П

Требования по реализации мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, Реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения, не применяются в случае, если в целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом при передаче электронных сообщений **используются выделенные контролируемые сегменты вычислительных сетей**, доступ к которым нарушителем невозможен, и угрозы нарушения целостности электронных сообщений определены кредитными организациями как неактуальные, что **обосновано в модели угроз и нарушителей безопасности информации**.

- ✓ Легально ввезённые на территорию Российской Федерации СКЗИ

Простая электронная подпись!

Возможность одновременного обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом только простой электронной подписью (далее – ПЭП)
Положением № 683-П и Положением №757-П не предусмотрена.

Таким образом использование простой электронной подписи возможно только совместно с СКЗИ, реализующими функцию имитозащиты информации с аутентификацией отправителя сообщения

Что такое СКЗИ, реализующими функцию имитозащиты?

Под СКЗИ, реализующим функцию имитозащиты информации с аутентификацией отправителя сообщения, подразумевается средство, обеспечивающее целостность и аутентификацию отправителя электронных сообщений за счет вычисления кода аутентификации сообщений (имитозащиты),

- произведенное на территории Российской Федерации
- или ввезённое на территорию Российской Федерации установленным порядком

Что такое СКЗИ, реализующими функцию имитозащиты?

СКЗИ, реализующее согласно документации функцию имитозащиты, определенную подпунктом б) пункта 2 Положения ПКЗ-2005:

средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

и пунктом 3. 11 рекомендации по стандартизации Р 1323565.1.012-2017 «Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации»:

имитозащита: Защита обрабатываемой информации с использованием криптографических механизмов от навязывания ложной информации

Что такое СКЗИ, реализующими функцию имитозащиты?

Таким образом в документации на СКЗИ должно быть написано,
что оно реализует функцию имитозащиты информации

В эксплуатационной документации ввозимого на территорию Российской Федерации СКЗИ обычно
такой фразы нет!

Разработка криптографических средств

В соответствии с Положением ПКЗ-2005 разработка СКЗИ
(а также производство, монтаж, обслуживание и ремонт, распространение, предоставление услуг и т.п.)
на территории Российской Федерации – лицензируемый вид деятельности!

(за исключением случаев, указанных в пункте 3 ПП от 16 апреля 2012 года № 313)

В случае применения СКЗИ российского производства, СКЗИ должны пройти оценку
соответствия требованиям по информационной безопасности ФСБ России.

Случаи признания ПЭП и УНЭП

(Федерального закона от 6 июня 2011 года № 63-ФЗ «Об электронной подписи»)

ПЭП	УНЭП
электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом.	1)получена в результате криптографического преобразования информации с использованием ключа электронной подписи; 2)позволяет определить лицо, подписавшее электронный документ; 3)позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; 4)создается с использованием средств электронной подписи.

Нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, … , должны предусматривать, в частности:
1) правила определения лица, подписывающего электронный документ, по его простой электронной подписи;
2) обязанность лица, создающего и (или) использующего ключ простой электронной подписи, соблюдать его конфиденциальность.

Случаи признания ПЭП и УНЭП

(Федерального закона от 6 июня 2011 года № 63-ФЗ «Об электронной подписи»)

С учетом изложенного, в случае если при электронном взаимодействии используется

- усиленная неквалифицированная электронная подпись или
- простая электронная подпись финансовым организациям необходимо отражать в договорах с клиентами:

- ❑ случаи (закрытый список) признания электронных документов, подписанных УНЭП (ПЭП),
- ❑ порядок проверки УНЭП (ПЭП),
- ❑ условия обеспечения информационной безопасности.

А также выполнить условия отнесения подписи к УНЭП (ПЭП).

Положение Банка России от 25.07.2022 N 802-П (ред. от 25.07.2022) "О требованиях к защите информации в платежной системе Банка России"

Хранение и использование криптографических ключей участника СБП, предназначенных для подписания исходящих электронных сообщений и (или) расшифрования на прикладном уровне входящих электронных сообщений, должны осуществляться в **аппаратных модулях безопасности** информационной инфраструктуры оператор услуг информационного обмена СБП, **имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности** …

Доступ к криптографическим ключам участника СБП должен быть обеспечен только для участника СБП как владельца сертификата ключа проверки электронной подписи.

Вопросы

???