Указание Банка России от 11.12.2015 № 3893-У "О порядке направления запросов и получения информации из Центрального каталога кредитных историй посредством обращения в кредитную организацию"

Зарегистрировано в Минюсте России 09.02.2016 № 41021

В соответствии со статьей 13 Федерального закона от 30 декабря 2004 года № 218-ФЗ «О кредитных историях» (Собрание законодательства Российской Федерации, 2005, № 1, ст. 44; № 30, ст. 3121; 2007, № 31, ст. 4011; 2011, № 15, ст. 2038; № 27, ст. 3880; № 29, ст. 4291; № 49, ст. 7067; 2013, № 30, ст. 4084; № 51, ст. 6683; 2014, № 26, ст. 3395; 2015, № 27, ст. 3945) настоящее Указание устанавливает порядок направления субъектом кредитной истории, пользователем кредитной истории и финансовым управляющим, утвержденным в деле о несостоятельности (банкротстве) субъекта кредитной истории - физического лица (далее - финансовый управляющий), запросов в Центральный каталог кредитных историй (далее - ЦККИ) о представлении информации о бюро кредитных историй (далее - БКИ), в котором хранится кредитная история субъекта кредитной истории, и получения информации из ЦККИ посредством обращения в кредитную организацию.

[Извлечение]

7. В день обращения субъекта кредитной истории (пользователя кредитной истории, финансового управляющего) с запросом кредитная организация, осуществив идентификацию субъекта кредитной истории (пользователя кредитной истории, финансового управляющего) и проверку наличия у пользователя кредитной истории согласия субъекта кредитной истории, указанного в пункте 5 настоящего Указания, направляет запрос в ЦККИ с использованием средств телекоммуникаций через территориальное учреждение Банка России по месту нахождения кредитной организации (головного офиса, филиала, дополнительного офиса кредитной организации), которое передает запрос в ЦККИ. Кредитная организация направляет запрос в виде электронного сообщения с применением средств криптографической защиты информации, принятых к использованию в Банке России. Порядок использования средств криптографической защиты информации при обмене электронными сообщениями между Банком России и кредитными организациями в целях направления запросов и получения информации из Центрального каталога кредитных историй, а также Порядок обеспечения информационной безопасности при использовании средств криптографической защиты информации для целей передачи-приема электронных сообщений при направлении запросов и получении информации из Центрального каталога кредитных историй устанавливаются приложениями 4 и 5 к настоящему Указанию.

Запрос в ЦККИ может направляться как в виде электронного сообщения, содержащего один запрос субъекта кредитной истории (пользователя кредитной истории, финансового управляющего), так и в виде электронного сообщения, содержащего более одного запроса субъекта (субъектов) кредитной истории и (или) пользователя (пользователей) кредитной истории и (или) финансового управляющего (далее - пакетное электронное сообщение). При этом запросы субъектов кредитных историй, пользователей кредитных историй и финансовых управляющих могут формироваться в одно пакетное электронное сообщение.

[...]

Приложение 4 к Указанию Банка России от 11 декабря 2015 года № 3893-У "О порядке направления запросов и получения информации из Центрального каталога кредитных историй посредством обращения в кредитную организацию"

Порядок использования средств криптографической защиты информации при обмене электронными сообщениями между Банком России и кредитными организациями в целях направления запросов и получения информации из Центрального каталога кредитных историй

1. Обмен электронными сообщениями между Банком России и кредитными организациями осуществляется с применением средств криптографической защиты информации (далее - СКЗИ), принятых к использованию в Банке России, через территориальное учреждение Банка России по месту нахождения кредитной организации (далее - территориальное учреждение). СКЗИ используются для формирования кодов аутентификации и шифрования электронных сообщений.

2. В настоящем приложении используются следующие термины:
2.1. электронное сообщение (далее - ЭС) - совокупность данных, соответствующая установленному Банком России электронному формату, пригодная для однозначного восприятия содержания ЭС, снабженная кодом аутентификации;
2.2. код аутентификации (далее - КА) - данные, используемые для подтверждения подлинности и контроля целостности ЭС;
2.3. подтверждение подлинности и контроль целостности ЭС (далее - аутентификация ЭС) - проверка сообщения, переданного электронным способом, позволяющая получателю установить, что ЭС исходит из указанного источника и не было изменено при его передаче от источника до получателя;
2.4. ключ (идентификатор) КА (далее - ключ КА) - уникальные данные, используемые при создании и проверке КА и состоящие из: секретной части ключа (идентификатора) КА (далее - секретный ключ КА) - данных, предназначенных для создания КА

отправителем;
публичной части ключа (идентификатора) КА (далее - открытый ключ КА) - данных, предназначенных для аутентификации ЭС получателем;
2.5. ключ шифрования - уникальные данные, используемые при шифровании и расшифровании ЭС и состоящие из:
секретной части ключа шифрования (далее - секретный ключ шифрования);
публичной части ключа шифрования (далее - открытый ключ шифрования);
2.6. владелец ключа КА или ключа шифрования - кредитная организация или территориальное учреждение, ключ КА или ключ шифрования которого зарегистрирован в регистрационном центре, функционирующем в территориальном учреждении;
2.7. средства аутентификации - аппаратные и (или) программные средства, обеспечивающие создание и проверку КА;
2.8. средства шифрования - аппаратные, программные, программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче и получении по каналам связи;
2.9. компрометация ключа КА или ключа шифрования - событие, определенное владельцем ключа КА или ключа шифрования как ознакомление неуполномоченным лицом (лицами) с его секретным ключом КА или секретным ключом шифрования;
2.10. пользователь ключа КА или ключа шифрования - лицо, назначенное владельцем ключа КА или ключа шифрования и уполномоченное им использовать ключ КА или ключ шифрования от имени владельца ключа КА или ключа шифрования;
2.11. регистрационный центр - структурное подразделение территориального учреждения, выполняющее функции регистрации ключей КА и (или) ключей шифрования и управления ключами КА и (или) ключами шифрования владельцев ключей КА или ключей шифрования;
2.12. регистрационная карточка ключа КА и (или) ключа шифрования - документ, содержащий распечатку открытого ключа КА и (или) ключа шифрования в шестнадцатеричной системе счисления, наименование владельца ключа КА или ключа шифрования и иные идентифицирующие владельца ключа КА или ключа шифрования реквизиты, подписанный руководителем (или замещающим его лицом) кредитной организации или территориального учреждения и заверенный оттиском печати (далее - регистрационная карточка).

3. Территориальное учреждение и кредитная организация обеспечивают сохранность своих секретных ключей КА и ключей шифрования.

Ответственность за содержание данных, включаемых в ЭС, несет владелец ключа КА, которым снабжено ЭС.

4. Ключи КА изготавливаются владельцем ключа самостоятельно. Ключи КА подлежат регистрации в регистрационном центре. Для этого изготавливается регистрационная карточка ключа КА в двух экземплярах в соответствии с порядком, определяемым регистрационным центром.

Регистрационная карточка ключа КА содержит:
наименование владельца ключа КА;
наименование применяемого СКЗИ;
информацию, идентифицирующую ключ КА (идентификатор и (или) номер ключа КА, идентификатор и (или) номер серии ключа КА);
распечатку открытого ключа КА в шестнадцатеричной системе счисления;
дату изготовления ключа КА;
даты начала и окончания действия ключа КА;
подпись руководителя (или замещающего его лица) владельца ключа КА, заверенную оттиском печати владельца ключа КА;
подпись администратора регистрационного центра;
иные реквизиты.

Форма регистрационной карточки ключа КА разрабатывается регистрационным центром в зависимости от функциональных возможностей конкретного СКЗИ.

Регистрационная карточка ключа КА может распечатываться на одном листе или нескольких страницах. При распечатке регистрационной карточки ключа КА на нескольких страницах каждая страница должна содержать подпись руководителя (или замещающего его лица) владельца ключа КА, заверенную оттиском печати владельца ключа КА.

Один экземпляр оформленной регистрационной карточки ключа КА хранится в регистрационном центре, другой - у владельца ключа КА. Ключ КА считается зарегистрированным со дня передачи владельцу ключа КА его экземпляра оформленной регистрационной карточки ключа КА.

5. Ключи шифрования, используемые для обеспечения защиты информации при передаче и получении ЭС по каналам связи, предоставляются регистрационным центром с оформлением акта их передачи-приема по форме, определяемой регистрационным центром, либо изготавливаются владельцем ключа шифрования самостоятельно и регистрируются регистрационным центром. Процедура регистрации ключей шифрования аналогична процедуре регистрации ключей КА, предусмотренной в пункте 4 настоящего приложения.

6. Порядок обращения с секретными ключами КА и ключами шифрования, обеспечивающий их конфиденциальность, и допуск к ним конкретных пользователей устанавливаются внутренними документами владельца ключа КА или ключа шифрования и Порядком обеспечения информационной безопасности при использовании средств криптографической защиты информации для целей передачи-приема электронных сообщений при направлении запросов и получении информации из Центрального каталога кредитных историй в соответствии с приложением 5 к настоящему Указанию.

7. Управление ключами КА и ключами шифрования осуществляется и регламентируется регистрационным центром в порядке, разрабатываемом на основании приложения 5 к настоящему Указанию и эксплуатационно-технической документации на используемые СКЗИ.

8. Плановый срок действия ключей КА и ключей шифрования определяется регистрационным центром.

9. Плановая смена ключей КА и ключей шифрования организуется регистрационным центром с соответствующим уведомлением всех владельцев ключей КА или ключей шифрования.

10. Внеплановая смена ключей КА и (или) ключей шифрования может осуществляться как по инициативе регистрационного центра, так и владельца ключа КА или ключа шифрования в случае компрометации или утраты секретного ключа КА и (или) ключа шифрования.

11. При смене ключей КА или ключей шифрования оформляется новая регистрационная карточка в соответствии с пунктом 4 настоящего приложения.

12. После ввода в действие новых ключей КА или ключей шифрования прежде действовавшие секретные ключи КА или ключи шифрования уничтожаются, а открытые ключи КА хранятся территориальным учреждением и кредитной организацией в течение всего срока хранения ЭС, для подтверждения подлинности и контроля целостности которых они могут быть использованы.

13. Уничтожение открытых ключей КА после истечения срока их хранения осуществляется территориальным учреждением и кредитной организацией самостоятельно.

14. Программные средства, предназначенные для создания и проверки КА, а также документация на эти средства хранятся территориальным учреждением и кредитной организацией в течение всего срока хранения ЭС, для подписания и подтверждения подлинности и контроля целостности которых использовались (могут использоваться) указанные средства.

15. Сведения о ключах КА и ключах шифрования не подлежат передаче третьим лицам, за исключением случаев, установленных законодательством Российской Федерации.

Приложение 5 к Указанию Банка России от 11 декабря 2015 года № 3893-У "О порядке направления запросов и получения информации из Центрального каталога кредитных историй посредством обращения в кредитную организацию"

Порядок обеспечения информационной безопасности при использовании средств криптографической защиты информации для целей передачи-приема электронных сообщений при направлении запросов и получении информации из Центрального каталога кредитных историй

1. Установка и настройка СКЗИ на автоматизированных рабочих местах (далее - АРМ) пользователей выполняются в присутствии Администратора информационной безопасности, назначаемого владельцем ключа КА или ключа шифрования. При каждом запуске АРМ должен быть обеспечен контроль целостности установленного программного обеспечения СКЗИ.

2. Территориальным учреждением Банка России по месту нахождения кредитной организации (далее - территориальным учреждением) и кредитной организацией организуется работа по учету, хранению и использованию носителей ключевой информации (ключевых дискет, ключевых идентификаторов Touch Memory, ключевых Smart-карточек и иных аналогичных носителей ключевой информации) с секретными ключами КА и ключами шифрования. Возможность несанкционированного доступа к носителям ключевой информации должна быть исключена.

3. Руководством владельца ключа КА или ключа шифрования определяется список лиц, имеющих доступ к секретным ключам КА и ключам шифрования (с указанием конкретной информации для каждого лица). Доступ неуполномоченных лиц к носителям ключевой информации исключается.

4. Для хранения носителей ключевой информации с секретными ключами КА и ключами шифрования должны использоваться надежные металлические хранилища. Хранение носителей ключевой информации с секретными ключами КА и ключами шифрования допускается в одном хранилище с другими документами в отдельном контейнере, опечатываемом пользователем ключа КА и (или) ключа шифрования.

5. В течение рабочего дня вне времени составления и передачи-приема электронного сообщения (далее - ЭС), а также по окончании рабочего дня носители ключевой информации с секретными ключами КА и (или) ключами шифрования помещаются в хранилище.

6. Не допускается:
снимать несанкционированные копии с носителей ключевой информации;
знакомить с содержанием носителей ключевой информации или передавать носители ключевой информации лицам, к ним не допущенным;
выводить секретные ключи КА или ключи шифрования на дисплей (монитор) электронно-вычислительной машины (далее - ЭВМ) или принтер;
устанавливать носитель секретных ключей КА или ключей шифрования в считывающее устройство (дисковод) ЭВМ, на которой программные средства передачи-приема ЭС функционируют в непредусмотренных (нештатных) режимах, а также на другие ЭВМ;

записывать на носители ключевой информации постороннюю информацию.

7. При компрометации секретного ключа КА или ключа шифрования владелец ключа КА или ключа шифрования, допустивший компрометацию, обязан предпринять все меры для прекращения любых операций с ЭС с использованием этого ключа и немедленно проинформировать о факте компрометации регистрационный центр, который организует внеплановую замену ключей КА или ключей шифрования.

8. Владелец ключа КА или ключа шифрования, допустивший компрометацию, представляет в регистрационный центр документ, содержащий информацию о компрометации ключа КА или ключа шифрования.

9. В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей работника территориального учреждения или кредитной организации, имевшего доступ к секретным ключам КА или ключам шифрования, должна быть проведена замена ключей, к которым указанный работник имел доступ.

тайна кредитных историй, средства защиты информации, техническая защита информации