

**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)**

« » 2016 г.

№

г. Москва

П О Л О Ж Е Н И Е

**О порядке сообщения банком (иной кредитной организацией) об
открытии или о закрытии счета, об изменении реквизитов счета в
электронной форме в территориальный орган страховщика**

На основании статьи 22² Федерального закона от 24 июля 1998 года № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний» (Собрание законодательства Российской Федерации, 1998, № 31 ст. 3803; 2001, № 44, ст. 4152; 2002, № 1, ст. 2, ст. 3; № 48, ст. 4737; 2003, № 17, ст. 1554; № 28, ст. 2887; № 43, ст. 4108; № 52 ст. 5037; 2004, № 35, ст. 3607; № 49, ст. 4851; 2007, № 1, ст. 22; № 30, ст. 3806; 2008, № 30, ст. 3616; 2009, № 30, ст. 3739; № 48, ст. 5745; 2010, № 21, ст. 2528; № 31, ст. 4195; № 49, ст. 6409; № 50, ст. 6606, ст. 6608; 2011, № 45, ст. 6330; № 49, ст. 7061; 2012, № 10, ст. 1164; 2013, № 14, ст. 1644; № 27, ст. 3477; № 49, ст. 6332; № 51, ст. 6678; № 52, ст. 6986; 2014, № 14, ст. 1551; № 19, ст. 2321; № 26, ст. 3394; № 30, ст. 4217; № 49, ст. 6915; 2016, № 1, ст. 14; № 27, ст. 4183), Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации

(Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699; № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317; № 27, ст. 3634; № 30, ст. 4219; № 40, ст. 5318, № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, ст. 37; № 27, ст. 3958, ст. 4001; № 29, ст. 4348, ст. 4357; № 41, ст. 5639; № 48, ст. 6699; 2016, № 1, ст. 23, ст. 46, ст. 50; № 26, ст. 3891; № 27, ст. 4225, ст. 4273, ст. 4295) настоящее Положение устанавливает порядок сообщения банком (иной кредитной организацией) (далее - банк) об открытии или о закрытии счета, об изменении реквизитов счета юридического лица, индивидуального предпринимателя (далее – клиенты) в электронной форме в территориальный орган Фонда социального страхования Российской Федерации по месту своего нахождения (далее – территориальный орган страховщика).

Глава 1. Порядок формирования и направления банком сообщения об открытии или о закрытии счета, об изменении реквизитов счета клиента

1.1. Электронное сообщение, сформированное в соответствии с пунктом 1.1 Положения Банка России от 7 сентября 2007 года № 311-П «О порядке сообщения банком в электронном виде налоговому органу об открытии или о закрытии счета, вклада (депозита), об изменении реквизитов счета, вклада (депозита)», зарегистрированного Министерством юстиции Российской Федерации 8 октября 2007 года № 10265, 7 июля 2010 года № 17755, 14 декабря 2010 года № 19176, 20 мая 2014 года № 32352 («Вестник

Банка России» от 17 октября 2007 года № 58, от 21 июля 2010 года № 42, от 17 декабря 2010 года № 69, от 28 мая 2014 года № 46) (далее - Положение Банка России № 311-П), одновременно является сообщением, направляемым территориальному органу страховщика.

Датой сообщения банком территориальному органу страховщика об открытии или о закрытии счета, об изменении реквизитов счета признается дата формирования территориальным учреждением Банка России в соответствии с Положением Банка России № 311-П перечня наименований электронных сообщений сводного архивного файла первого типа, в котором содержалось полученное территориальным органом страховщика электронное сообщение. Дата сообщения указывается в квитанции о получении территориальным органом страховщика электронного сообщения.

1.2. Доставка электронного сообщения банка, сформированного в соответствии с пунктом 1.1 настоящего Положения, осуществляется в порядке, установленном Положением Банка России № 311-П, с учетом особенностей, установленных настоящим Положением, через территориальное учреждение Банка России, на поднадзорной территории которого расположен банк (далее - территориальное учреждение), и через Департамент информационных технологий Банка России (далее – ДИТ) в уполномоченное подразделение Фонда социального страхования Российской Федерации (далее – уполномоченное подразделение страховщика) для последующей доставки электронного сообщения в территориальный орган страховщика.

1.3. Сводные архивные файлы территориальных учреждений первого типа ДИТ направляет в уполномоченное подразделение страховщика с одновременным направлением указанных архивных файлов в уполномоченный налоговый орган в соответствии с Положением Банка России № 311-П.

Сводные архивные файлы территориальных учреждений второго типа, принятые ДИТ в соответствии с Положением Банка России № 311-П, в уполномоченное подразделение страховщика не направляются.

1.4. ДИТ обеспечивает направление сводных архивных файлов, включающих транспортные файлы уполномоченного налогового органа первого типа, полученных в соответствии с Положением Банка России № 311-П и содержащих квитанции о принятии (непринятии) уполномоченным налоговым органом электронного сообщения, а также извещения об ошибках, в уполномоченное подразделение страховщика в день их получения от уполномоченного налогового органа. Квитанции о принятии (непринятии) уполномоченным налоговым органом электронного сообщения, а также извещения об ошибках, содержащиеся в транспортных файлах уполномоченного налогового органа первого типа, проходят процедуру аутентификации в уполномоченном подразделении страховщика.

Сводные архивные файлы, включающие транспортные файлы уполномоченного налогового органа второго типа, принятые ДИТ в соответствии с Положением Банка России № 311-П, в уполномоченное подразделение страховщика не направляются.

Глава 2. Работа банков с квитанциями и извещениями, поступающими от уполномоченного подразделения страховщика

2.1. Банк получает квитанции, содержащие подтверждения о получении электронного сообщения, сформированные уполномоченным подразделением страховщика в электронном виде и снабженные кодом аутентификации (далее - КА) указанного подразделения после получения им электронного сообщения и квитанции о принятии уполномоченным налоговым органом этого электронного сообщения (далее - квитанция о получении электронного сообщения).

Электронное сообщение банка, в отношении которого уполномоченным подразделением страховщика получена квитанция о его непринятии уполномоченным налоговым органом, исключается из дальнейшей обработки. В этом случае квитанция о получении этого электронного сообщения уполномоченным подразделением страховщика не формируется и банку не направляется.

2.2. В случаях выявления несоответствия сведений, указанных в ранее полученном электронном сообщении, учетным данным, имеющимся у страховщика, уполномоченным подразделением страховщика может формироваться извещение о необходимости корректировки ранее полученного электронного сообщения, снабженное соответственно КА указанного подразделения и направляемое в электронном виде в ДИТ для его последующей доставки в банк через территориальное учреждение (далее - извещение о корректировке).

2.3. Адресованные одному и тому же банку квитанции о получении электронного сообщения, а также извещения о корректировке поступают в банк от территориального учреждения в составе транспортных файлов уполномоченного подразделения страховщика, сформированных с помощью программы архиватора.

2.4. В случае неполучения банком квитанции о получении электронного сообщения по истечении десяти рабочих дней после дня его направления в порядке, установленном Положением Банка России № 311-П, при условии получения этим банком квитанции о принятии уполномоченным налоговым органом данного электронного сообщения, банк может направить письменный запрос в произвольной форме в уполномоченное подразделение страховщика для выяснения причин недоставки соответствующей квитанции о получении электронного сообщения с приложением к запросу предусмотренных Положением Банка России № 311-П копии уведомления о принятии территориальным учреждением транспортного файла банка, содержащего соответствующее электронное сообщение, и копии квитанции о принятии уполномоченным налоговым органом электронного сообщения.

2.5. В случае получения извещения о корректировке банк формирует электронное сообщение с учетом исправленных данных и направляет его соответственно в уполномоченное подразделение страховщика в порядке, установленном настоящим Положением, не позднее пяти рабочих дней, следующих за датой получения банком извещения о корректировке.

Указанный срок продлевается до пятнадцати рабочих дней в случае, если формирование и направление банком электронного сообщения связано с получением от клиента дополнительных документов и сведений, необходимых для исправления соответствующих данных.

В случае если у банка, исходя из имеющихся сведений и представленных клиентом документов, отсутствуют основания для корректировки ранее полученного уполномоченным подразделением страховщика электронного сообщения, по которому банком получено извещение о корректировке, информация об этом доводится банком до территориального органа страховщика в произвольной письменной форме с соблюдением срока, установленного абзацем вторым настоящего пункта.

2.6. Из электронных сообщений, сформированных в течение рабочего дня в соответствии с пунктом 2.5 настоящего Положения, банк формирует в порядке, установленном Положением Банка России № 311-П, транспортные файлы, предназначенные для отправки в уполномоченное подразделение страховщика (далее - транспортные файлы банка четвертого типа).

Транспортные файлы банка четвертого типа снабжаются КА банка и направляются в тот же рабочий день, в который они были сформированы, до 16 часов 00 минут по местному времени по каналам связи или на магнитном носителе в территориальное учреждение для последующей доставки включенных в них электронных сообщений через ДИТ в уполномоченное подразделение страховщика.

Территориальное учреждение обеспечивает прием направленных по каналам связи или на магнитном носителе транспортных файлов банка четвертого типа по рабочим дням до 16 часов 00 минут по местному времени.

2.7. Транспортные файлы банков четвертого типа, принятые в течение рабочего дня территориальным учреждением и прошедшие проверку в соответствии с главой 2 Положения Банка России № 311-П, распаковываются территориальным учреждением с помощью программы архиватора.

Из всех электронных сообщений, полученных в результате распаковывания транспортных файлов банка четвертого типа,

территориальное учреждение формирует и направляет в ДИТ в порядке, установленном Положением Банка России № 311-П, с учетом особенностей, установленных настоящим Положением, сводный архивный файл четвертого типа.

ДИТ направляет полученные от территориального учреждения сводные архивные файлы четвертого типа в уполномоченное подразделение страховщика не позднее 18 часов 00 минут по московскому времени рабочего дня, следующего за днем их получения от территориального учреждения.

2.8. ДИТ обеспечивает направление сводных архивных файлов, включающих транспортные файлы уполномоченного подразделения страховщика в день их получения от указанного подразделения в территориальное учреждение для последующей доставки в банк с использованием каналов связи, применяемых в Банке России для передачи статистической информации.

2.9. Территориальное учреждение по получении от ДИТ сводных архивных файлов уполномоченного подразделения страховщика осуществляет их разархивацию с помощью программы архиватора. Полученные в результате разархивации транспортные файлы уполномоченного подразделения страховщика направляются территориальным учреждением в банк по каналам связи или на магнитном носителе не позднее 18 часов 00 минут по местному времени рабочего дня, следующего за днем их получения от ДИТ.

Банк обеспечивает прием транспортных файлов уполномоченного подразделения страховщика от территориального учреждения по каналам связи или на магнитном носителе и проводит процедуру аутентификации содержащихся в них квитанций о получении электронного сообщения, а также извещений о корректировке.

2.10. При отрицательном результате процедуры аутентификации квитанции о получении электронного сообщения и (или) извещения о корректировке банк информирует об этом должностное лицо уполномоченного подразделения страховщика, указанное в служебной части

квитанции о получении электронного сообщения и (или) извещения о корректировке. В этом случае уполномоченное подразделение страховщика повторно направляет в банк указанные документы в порядке, установленном настоящим Положением и Положением Банка России № 311-П.

2.11. В банковских правилах, определяемых банком, должен быть установлен порядок доведения до филиала банка, не наделенного правом самостоятельного направления электронных сообщений, получаемых банком (филиалом банка, имеющим банковский идентификационный код) квитанций о получении электронного сообщения, а также извещений о корректировке.

Глава 3. Требования по обеспечению информационной безопасности и хранения банками квитанций о получении электронного сообщения, а также извещений о корректировке

3.1. Информационное взаимодействие банков с уполномоченным подразделением страховщика, а также с территориальным учреждением, предусмотренное настоящим Положением, осуществляется с применением средств криптографической защиты информации (далее - СКЗИ), определяемых Банком России по согласованию со страховщиком. Обеспечение информационной безопасности при использовании СКЗИ осуществляется в порядке, установленном приложением к настоящему Положению.

3.2. При передаче электронных сообщений, указанных в пункте 1.1 настоящего Положения, транспортных файлов от уполномоченного подразделения страховщика в банки территориальные учреждения и ДИТ обеспечивают неизменность всех данных, содержащихся в них, а также защиту от несанкционированного доступа к ним третьих лиц.

3.3. Электронное сообщение, указанное в пункте 1.1 настоящего Положения, а также полученные банком квитанции о получении электронного сообщения и извещения о корректировке хранятся банком в электронном виде в течение срока, который не может быть меньше установленного законодательством Российской Федерации срока хранения

соответствующего юридического дела клиента, которое формируется банком в порядке, установленном Инструкцией Банка России от 30 мая 2014 года № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов», зарегистрированной Министерством юстиции Российской Федерации 19 июня 2014 года № 32813 («Вестник Банка России» от 26 июня 2014 года № 60).

Транспортные файлы банка, направленные в территориальное учреждение, а также полученные уведомления о принятии (непринятии) территориальным учреждением транспортного файла банка хранятся банком в электронном виде до получения в отношении каждого электронного сообщения, содержащегося в соответствующем транспортном файле банка, квитанции о получении электронного сообщения.

Глава 4. Заключительные положения

4.1. Настоящее Положение вступает в силу по истечении 10 дней после дня его официального опубликования.

4.2. Центральный банк Российской Федерации в срок не позднее 30 дней после дня вступления в силу настоящего Положения обеспечивает разработку и размещение на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» согласованных со страховщиком:

форматов и структуры квитанции о получении электронного сообщения, извещения о корректировке, а также справочника кодов ошибок, включаемых в извещение о корректировке;

структуры наименований транспортных файлов банка четвертого типа, сводных архивных файлов территориального учреждения четвертого типа, транспортных файлов уполномоченного подразделения страховщика, сводных архивных файлов уполномоченного подразделения страховщика;

информации о допустимых объемах транспортных файлов банка четвертого типа, сводных архивных файлов территориального учреждения четвертого типа, транспортных файлов уполномоченного подразделения

страховщика, сводных архивных файлов уполномоченного подразделения страховщика.

4.3. Согласованные со страховщиком изменения в форматы, структуру и наименования файлов, указанных в пункте 4.2 настоящего Положения, а также информацию о допустимых объемах транспортных и архивных файлов, указанных в пункте 4.2 настоящего Положения, размещаются на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» и применяются по истечении 30 дней после дня их размещения, если информация о более поздних сроках их применения не размещена на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Председатель
Центрального банка
Российской Федерации

Э.С. Набиуллина

Согласовано

Председатель Фонда
социального страхования
Российской Федерации

А.С. Кигим

Приложение
к Положению Банка России
от _____ 2016 г. № _____
«О порядке сообщения банком
(иной кредитной организацией)
об открытии или о закрытии
счета, об изменении реквизитов
счета в электронной форме в
территориальный орган
страховщика»

Порядок обеспечения информационной безопасности при использовании СКЗИ

1. В настоящем Приложении используются следующие термины:

подтверждение подлинности и контроль целостности электронного сообщения - проверка сообщения, переданного электронным способом, позволяющая получателю установить, что данное сообщение исходит из указанного источника и не было изменено при его передаче от источника до получателя;

ключ КА - уникальные данные, используемые при создании и проверке КА и состоящие из секретной части ключа КА (далее - секретный ключ КА), предназначенной для создания КА сообщения, и публичной части ключа КА (далее - открытый ключ КА), предназначенной для аутентификации электронного сообщения получателем;

ключ шифрования - уникальные данные, используемые при зашифровывании и расшифровывании электронного сообщения;

владелец ключа КА или ключа шифрования (далее - владелец ключей) - уполномоченное подразделение страховщика, банк, территориальное учреждение, чей ключ КА или ключ шифрования зарегистрирован в регистрационном центре, функционирующем в Банке России;

СКЗИ - аппаратные и (или) программные средства, обеспечивающие создание и проверку КА, а также реализующие алгоритмы

криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи;

компрометация ключа КА или ключа шифрования - событие, определенное владельцем ключей как ознакомление неуполномоченным лицом (неуполномоченными лицами) с секретным ключом КА или секретным ключом шифрования владельца ключей;

пользователь ключа КА или ключа шифрования - лицо, назначенное владельцем ключей и уполномоченное им использовать ключ КА или ключ шифрования от имени владельца ключей;

регистрационная карточка ключа КА - документ, подписанный руководителем владельца ключа КА (или замещающим его лицом), заверенный оттиском печати владельца ключа КА, содержащий распечатку открытого ключа КА в шестнадцатеричной системе счисления, наименование владельца ключа КА и иные идентифицирующие владельца ключа КА данные (далее - регистрационная карточка).

2. Обмен электронными сообщениями между уполномоченным подразделением страховщика и банком осуществляется с применением СКЗИ, принятых к использованию в Банке России. СКЗИ используются для формирования КА и шифрования электронных сообщений.

3. Владельцы ключей могут иметь резервные ключи КА и ключи шифрования.

4. В Банке России и его территориальных учреждениях организуются регистрационные центры, выполняющие функции регистрации ключей КА и (или) ключей шифрования и управления ключами КА и (или) ключами шифрования, предусмотренными настоящим Положением.

5. Владелец ключей изготавливает ключ КА самостоятельно. Ключ шифрования, предназначенный для обеспечения защиты информации при ее передаче по каналам связи, предоставляется ему регистрационным центром. Получение ключа шифрования оформляется актом. Форма акта определяется регистрационным центром.

6. Ключ КА подлежит регистрации в регистрационном центре. Для этого изготавливается регистрационная карточка в 2 экземплярах в соответствии с порядком, определяемым регистрационным центром.

Регистрационная карточка содержит:

наименование владельца ключа КА;

наименование применяемого средства аутентификации и (или) шифрования;

информацию, идентифицирующую ключ КА (идентификатор и (или) номер ключа КА, идентификатор и (или) номер серии);

назначение ключа КА (область применения);

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;

подпись администратора регистрационного центра;

иные реквизиты.

Форма регистрационной карточки разрабатывается регистрационным центром в зависимости от функциональных возможностей конкретного СКЗИ. Регистрационная карточка может распечатываться на одной или нескольких страницах. При распечатке регистрационной карточки на нескольких страницах каждая страница должна содержать подпись руководителя (или замещающего его лица) владельца ключей, заверенную оттиском печати владельца ключей.

Один экземпляр оформленной регистрационной карточки остается в регистрационном центре, другой передается владельцу ключа КА. Ключ КА считается зарегистрированным со дня передачи владельцу ключа КА его экземпляра оформленной регистрационной карточки.

7. Владельцы ключей обеспечивают сохранность своих секретных ключей КА и ключей шифрования.

8. Управление ключами КА и ключами шифрования осуществляется регистрационным центром и регламентируется в порядке, предусмотренном Банком России.

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

10. Плановая смена ключей КА и (или) ключей шифрования организуется регистрационным центром при соответствующем уведомлении всех владельцев ключей КА и (или) ключей шифрования.

11. Внеплановая смена ключей КА и (или) ключей шифрования может производиться по инициативе регистрационного центра либо владельца ключей в случае компрометации или утраты секретного ключа КА и (или) ключа шифрования.

12. При смене ключей КА и (или) ключей шифрования выполняются работы в соответствии с пунктами 5 и 6 настоящего Порядка.

13. После ввода в действие новых ключей КА и (или) ключей шифрования прежде действовавшие секретные ключи КА и (или) ключи шифрования уничтожаются, а открытые ключи КА хранятся владельцем ключей в течение всего срока хранения электронных сообщений, для подтверждения подлинности и контроля целостности которых они могут быть использованы.

14. Уничтожение открытых ключей КА после истечения срока их хранения осуществляется владельцем ключей самостоятельно.

15. Программные средства, предназначенные для создания и проверки КА, а также документация на эти средства хранятся владельцем ключей в течение всего срока хранения электронных сообщений, для подписания и подтверждения подлинности и контроля целостности которых использовались (могут быть использованы) указанные средства.

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

17. Установка и настройка СКЗИ на автоматизированных рабочих местах (далее - АРМ) пользователей выполняются с учетом требований, изложенных в эксплуатационной документации на СКЗИ, в присутствии администратора информационной безопасности, назначаемого владельцем ключей. При каждом запуске АРМ должен быть обеспечен контроль целостности установленного программного обеспечения СКЗИ.

18. Владельцем ключей определяются и утверждаются порядок учета, хранения и использования носителей ключевой информации (ключевых дискет, ключевых идентификаторов touch memo, ключевых смарт-карточек) с секретными ключами КА и ключами шифрования, который должен полностью исключать возможность несанкционированного доступа к ним.

19. Банк, отправивший электронное сообщение, снабженное КА банка, отвечает за информацию, содержащуюся в электронном сообщении.

20. Руководитель структурного подразделения владельца ключей утверждает 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 должен быть исключен.

21. Для хранения носителей ключевой информации с секретными ключами КА и (или) ключами шифрования должны использоваться надежные металлические хранилища. Допускается хранение носителей ключевой информации с секретными ключами КА и (или) ключами шифрования в одном хранилище с другими документами, но при этом отдельно от них, в отдельном контейнере, опечатываемом пользователем ключа КА и (или) ключа шифрования.

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

23. 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 и (или) ключи шифрования на дисплей (монитор) электронно-вычислительной машины (ЭВМ) или принтер;

устанавливать носитель секретных ключей КА и (или) ключей шифрования в считывающее устройство АРМ, программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие ЭВМ;

записывать на носители ключевой информации постороннюю информацию.

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

25. По факту компрометации ключа КА и (или) ключа шифрования владелец ключей, допустивший компрометацию, должен организовать служебное расследование, документально оформленные результаты которого представляются в регистрационный центр.

26. В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей работника, имевшего доступ к секретным ключам КА и (или) ключам шифрования,

должна быть проведена замена ключей, к которым указанный работник имел доступ.

27. СКЗИ и открытые ключи КА, необходимые для аутентификации хранящихся в банке электронных сообщений, квитанций о получении электронного сообщения и извещений об ошибках, подлежат хранению банком в течение срока, указанного в пункте 3.3 настоящего Положения.