Банк «Первомайский» (ПАО)
Регламент удостоверяющего центра от 01.12.2015, № 25-30113-0001

1.ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Банк – Банк «Первомайский» (ПАО).

Договор банковского обслуживания – договор, заключенный между Банком и Клиентом, на предоставление услуг и продуктов Банка посредством электронного взаимодействия между Банком и Клиентом с использованием Корпоративной информационной системы и электронной подписи.

Клиент – юридическое лицо, индивидуальный предприниматель, физическое лицо, заключивший с Банком Договор банковского обслуживания.

Корпоративная информационная система – информационная система Банка, в которой используются ключи электронной подписи и сертификаты ключей проверки электронной подписи, и посредством которой предоставляются определенные услуги Клиентам (например, ПТК «Интернет-Банк»).

Пользователь УЦ – физическое лицо, являющееся уполномоченным представителем Клиента и обладающее полномочиями по использованию ключей электронной подписи в Корпоративной информационной системе на основании учредительных документов юридического лица или доверенности, персональные данные которого указаны в Сертификате.

Рабочий день УЦ – с 9.00 до 18.00 с понедельника по пятницу кроме выходных (субботы и воскресенья) и праздничных дней.

Реестр сертификатов – информация о выданных и аннулированных (отозванных) УЦ Сертификатах.

Сертификат – электронный документ, выданный УЦ и подтверждающий принадлежность ключа проверки электронной подписи Пользователю УЦ;

Средство электронной подписи – средство криптографической защиты информации (СКЗИ), используемое для создания электронной подписи, проверка электронной подписи, ключа электронной подписи и ключа проверки электронной подписи;

Удостоверяющий центр (УЦ) – структурное подразделение Банка, осуществляющее функции по созданию и выдаче Сертификатов, а также иные функции в соответствии с настоящим Регламентом и Федеральным законом «Об электронной подписи» № 63-ФЗ от 06.04.2011 г.

2. Общие положения

2.1.Настоящий Регламент является соглашением, определяющим единые правила пользования услугами УЦ Банка, условия и порядок использования электронной подписи и средств электронной подписи, риски, связанные с использованием электронных подписей, и меры, необходимые для обеспечения безопасности электронных подписей и их проверки.

2.2.Услуги УЦ направлены на обеспечение юридически значимого электронного документооборота между участниками (Банком и его клиентами) в Корпоративных информационных системах Банка.

2.3.Настоящий Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров.

2.4.В соответствии со статьей 428 Гражданского кодекса Российской Федерации настоящий Регламент является договором присоединения. Нормы, содержащиеся в Регламенте, становятся обязательными для Клиента и Пользователя УЦ с момента заключения с Банком Договора банковского обслуживания в Корпоративной информационной системе Банка.

2.5.Факт заключения Договора банковского обслуживания является полным принятием Клиентом условий настоящего Регламента в редакции, действующей на момент заключения Договора банковского обслуживания. Клиент, присоединившийся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

2.6.Изменения и дополнения в Регламент вносятся Банком в одностороннем порядке. Все изменения и дополнения, вносимые в Регламент, полежат обязательной публикации путем размещения на официальном сайте Банка в сети Интернет https://www.1mbank.ru .

2.7.Все изменения и дополнения, вносимые Банком в настоящий Регламент по собственной инициативе не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении 10 (десяти) дней с даты размещения указанных изменений и дополнений на официальном сайте Банка в сети Интернет https://www.1mbank.ru , при изменении действующего законодательства Российской Федерации изменения и дополнения, вносимые в Регламент становятся обязательными с даты вступления в силу изменений действующего законодательства Российской Федерации.

2.8.Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае, если Клиент не согласен со внесенными изменениями и дополнениями он имеет право прекратить использование сертификата ключа проверки электронной подписи и расторгнуть Договор банковского обслуживания.

2.9.Требования настоящего Регламента применяются в течение срока действия Договора банковского обслуживания, если иное не вытекает из Регламента.

2.10. УЦ осуществляет обработку (с использованием и без использования средств автоматизации) персональных данных Пользователей УЦ в целях обеспечения настоящего Регламента.

2.11. Персональные данные Пользователей УЦ хранящиеся в УЦ и не подлежащие непосредственной рассылке в качестве части сертификата ключа проверки электронной подписи относятся к конфиденциальной информации. Ключ электронной подписи, соответствующий сертификату ключа проверки электронной подписи Пользователя УЦ является конфиденциальной информацией данного пользователя УЦ.

2.12. УЦ не осуществляет хранение ключей электронной подписи пользователей.

2.13. Персональные данные, включаемые в сертификаты ключей проверки электронной подписи Пользователей УЦ и списки отозванных сертификатов, издаваемые УЦ, не являются

конфиденциальными, относятся к общедоступным персональным данным и могут быть переданы третьим лицам в целях обеспечения работоспособности и информационной целостности инфраструктуры открытых ключей.

3. Права и обязанности сторон

3.1. УЦ имеет право:

3.1.1. Отказать в аннулировании (отзыве) сертификата ключа проверки электронной подписи Пользователя УЦ в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

3.1.2. Аннулировать (отозвать) сертификат ключа проверки электронной подписи Пользователя УЦ в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного (отозванного) сертификата ключа проверки электронной подписи и указанием обоснованных причин.

3.1.3. Отказать в изготовлении сертификата ключа проверки электронной подписи Пользователя УЦ в случае, если использованное пользователем для формирования запроса на сертификат ключа проверки электронной подписи средство криптографической защиты информации не поддерживается УЦ.

3.2.Пользователь УЦ имеет право:

3.2.1. Получить список отозванных сертификатов, изготовленный УЦ.

3.2.2. Получить сертификат ключа проверки электронной подписи УЦ или сотрудника Банка.

3.2.3. Применять сертификат ключа проверки электронной подписи УЦ для проверки электронной подписи сотрудников Банка в сертификатах, изготовленных УЦ.

3.2.4. Применять сертификат ключа проверки электронной подписи пользователя УЦ для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи.

3.2.5. Применять список отозванных сертификатов, изготовленный УЦ, для проверки статуса сертификатов ключей проверки электронной подписи.

3.2.6. Воспользоваться средствами Корпоративной информационной системы, пользователем которой он является, за подтверждением подлинности электронных подписей в электронных документах.

3.2.7. Сформировать ключ электронной подписи и ключ проверки электронной подписи на своем рабочем месте с использованием средства криптографической защиты информации, предоставляемого в комплекте поставки Корпоративной информационной системы, пользователем которой он является.

3.2.8. Воспользоваться предоставляемыми Корпоративной информационной системой, пользователем которой он является, программными средствами для передачи по линиям связи в УЦ запроса на выпуск сертификата ключа проверки электронной подписи в электронном виде.

3.2.9. Воспользоваться предоставляемыми Корпоративной информационной системой, пользователем которой он является, программными средствами, чтобы получить и установить на свое рабочее место изготовленный УЦ сертификат ключа проверки электронной подписи в электронном виде.

3.2.10. Обратиться в УЦ Банка для аннулирования (отзыва) сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи.

3.3.УЦ обязан:

3.3.1. Использовать для изготовления ключа электронной подписи УЦ и формирования электронной подписи только сертифицированные ФСБ России средства криптографической защиты информации.

3.3.2. Использовать ключ электронной подписи УЦ только для подписи издаваемых им сертификатов ключей проверки электронной подписи Пользователей УЦ и списков отозванных сертификатов.

3.3.3. Принять меры по защите ключа электронной подписи УЦ от несанкционированного доступа и обеспечить его конфиденциальность.

3.3.4. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Москвы.

3.3.5. В случае изготовления УЦ ключа электронной подписи и ключа проверки электронной подписи Пользователя УЦ:

- выполнять процедуру генерации ключей и их запись на отчуждаемый носитель только с использованием сертифицированного ФСБ России средства криптографической защиты информации;

- обеспечить сохранение в тайне изготовленного ключа электронной подписи пользователя.

3.3.6. Обеспечить изготовление сертификата ключа проверки электронной подписи пользователя в соответствии с порядком, определенным в настоящем Регламенте.

3.3.7. Обеспечить уникальность серийных номеров изготавливаемых сертификатов ключей проверки электронной подписи пользователей УЦ.

3.3.8. Обеспечить уникальность значений ключей проверки электронной подписи в изготовленных сертификатах ключей проверки электронной подписи Пользователей УЦ.

3.3.9. Аннулировать (отозвать) сертификат ключа проверки электронной подписи по заявлению на аннулирование (отзыв) сертификата ключа проверки электронной подписи и не позднее рабочего дня УЦ, следующего за рабочим днем в течение которого было подано заявление занести сведения об аннулированном (отозванном) сертификате в список отозванных сертификатов с указанием даты и времени занесения и причины отзыва.

3.3.10. Вести реестр выданных и аннулированных (отозванных) сертификатов и обеспечивать актуальность информации, содержащейся в реестре сертификатов, ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

3.3.11. Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным в настоящем Регламенте порядком доступа к реестру сертификатов информацию, содержащуюся в реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи.

3.4.Пользователь УЦ обязан:

3.4.1. Хранить в тайне личный ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

3.4.2. Не применять личный ключ электронной подписи, если пользователю стало известно, что этот ключ используется или использовался ранее другими лицами.

3.4.3. Немедленно обратиться в Банк с заявлением на аннулирование (отзыв) сертификата ключа проверки электронной подписи в случае потери, раскрытия, искажения личного ключа электронной подписи, а также в случае если пользователю стало известно, что этот ключ используется или использовался ранее другими лицами.

3.4.4. Не использовать личный ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, с момента времени подачи заявления на аннулирование (отзыв) сертификата в Банк.

3.4.5. Регулярно, не реже чем один раз в 10 дней, посещать официальный сайт Банка https://www.1mbank.ru на предмет изменения Регламента.

4. Деятельность УЦ

4.1.В соответствии с требованиями законодательства Российской Федерации и внутренними документами Банка УЦ:

1) создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты заявителям в соответствии с установленным в настоящем Регламенте порядком;

2) устанавливает сроки действия сертификатов ключей проверки электронных подписей;

3) аннулирует (отзывает) выданные УЦ сертификаты ключей проверки электронных подписей;

4) выдает по обращению заявителя средства электронной подписи;

5) ведет реестр выданных и аннулированных (отозванных) этим УЦ сертификатов ключей проверки электронных подписей в соответствии с установленным в настоящем Регламенте порядком;

6) обеспечивает доступ лиц к информации, содержащейся в реестре сертификатов, в том числе с использованием информационно-телекоммуникационной сети "Интернет";

7) создает по обращениям заявителей ключи электронных подписей и ключи проверки электронных подписей;

8) проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

9) осуществляет проверку электронных подписей по запросу;

10) осуществляет иную связанную с использованием электронной подписи деятельность.

4.2.Создание сертификата УЦ производится Администратором УЦ в порядке, предусмотренном внутренними документами Банка с учетом требований настоящего Регламента.

5. Порядок регистрации и предоставления Сертификатов

5.1.Создание сертификата ключа проверки электронной подписи и его выдача Пользователям УЦ производится только на основании заключенного Договора банковского обслуживания в следующем порядке:

- регистрация Пользователя УЦ;
- получение в УЦ средств электронной подписи;
- создание Запроса на сертификат ключа проверки электронной подписи;
- получение сертификата Пользователем УЦ.

5.2. Регистрация Пользователя УЦ проводится на основании данных, предоставляемых Пользователем УЦ при заключении Договора банковского обслуживания с Клиентом.

5.3.Предоставление УЦ средства электронной подписи производится лично Пользователю УЦ или на основании соответствующей доверенности, заверенной печатью и подписью руководителя организации.

5.4.Установка, настройка и дальнейшее сопровождение средства электронной подписи и программно-технических средства, на которых установлено средство электронной подписи, проводится Клиентом при участии Пользователя УЦ самостоятельно в соответствии с требованиями законодательства Российской Федерации и эксплуатационной документации к ним.

5.5.Формуляр на СКЗИ в электронном виде, находящийся в составе документации на СКЗИ, выводится Пользователем УЦ на бумажный носитель и заполняется.

5.6. УЦ ведет поэкземплярный учет выданных Пользователям УЦ экземпляров СКЗИ, эксплуатационной и технической документации к ним.

5.7.Запрещается полное или частичное воспроизведение, тиражирование и распространение переданных дистрибутивов СКЗИ без разрешения УЦ.

5.8.В случае расторжения Договора банковского обслуживания, прекращения полномочий Пользователя УЦ СКЗИ деинсталлируется с технических средств Клиента, а выданные УЦ дистрибутивы СКЗИ уничтожаются Клиентом с составлением Акта об уничтожении.

5.9.После получения средства электронной подписи Пользователь УЦ на своем рабочем месте с использованием программного обеспечения Корпоративной информационной системы осуществляет генерацию ключевой информации на ключевом носителе, формирует запрос на сертификат ключа проверки электронной подписи в виде электронного документа и отправляет его в Банк. Вместе с этим Пользователь УЦ передает в Банк собственноручно подписанный запрос на сертификат ключа проверки электронной подписи, оформленный в виде документа на бумажном носителе. Данные представленные в запросах на сертификат, оформленных в виде электронного и бумажных документов должны совпадать.

5.10. После получения от Пользователя УЦ запроса на сертификат ключа проверки электронной подписи, оформленного в виде документа на бумажном носителе, ответственный сотрудник Банка осуществляет его проверку на соответствие регистрационным документам и проверку на совпадение с запросом на сертификат, оформленного в виде электронного документа, с использованием программного обеспечения Корпоративной информационной системы. После успешной проверки ответственный сотрудник Банка отправляет запрос на сертификат ключа проверки электронной подписи в УЦ.

5.11. Изготовление сертификатов Пользователей УЦ производится УЦ на основании собственноручно подписанного запроса на сертификат, положительного результата его проверки на совпадение с запросом на сертификат, оформленного в виде электронного документа, а также при наличии в Банке документов, необходимых для идентификации и подтверждении полномочий владельца сертификата ключа проверки электронной подписи.

5.12. Изготовление сертификата ключа проверки электронной подписи Пользователя УЦ осуществляется при подключении пользователя к Корпоративной информационной системе, при плановой смене ключа Пользователя УЦ и при внеплановой смене ключа электронной подписи Пользователя УЦ.

5.13. УЦ осуществляет изготовление сертификата ключа проверки электронной подписи в виде электронного документа в соответствии с поступившим запросом.

5.14. Срок изготовления сертификата ключа проверки электронной подписи не превышает 3 рабочих дней с момента поступления запроса на сертификат в Банк.

5.15. Получение сертификата ключа проверки электронной подписи Пользователем УЦ осуществляется с использованием программного обеспечения Корпоративной информационной системы. Факт получения и признания пользователем сертификата ключа проверки электронной подписи подтверждается при помощи его первого использования на своем рабочем месте для работы с Корпоративной информационной системой по электронным каналам.

5.16. Срок действия ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя УЦ может составлять не более 1 года 3 месяцев.

6. Порядок аннулирования (отзыва) сертификата ключа проверки электронной подписи

6.1.УЦ аннулирует (отзывает) сертификат ключа проверки электронной подписи Пользователя УЦ в следующих случаях:

- по заявлению Пользователя УЦ;
- по истечении срока его действия;
- при компрометации ключа электронной подписи УЦ;
- по решению суда, вступившему в законную силу;
- при прекращении полномочий Пользователя УЦ.

- при компрометации ключа проверки электронной подписи Пользователя УЦ;

- при расторжении Договора банковского обслуживания, а также в иных случаях, предусмотренных правилами Корпоративной информационной системы.

6.2.При истечении срока действия сертификата ключа проверки электронной подписи Пользователя УЦ временем аннулирования сертификата Пользователя УЦ признается время, хранящееся в поле notAfter поля Validity сертификата. В данном случае информация об аннулированном сертификате Пользователя УЦ в список отозванных сертификатов не заносится.

6.3.В случае компрометации ключа электронной подписи УЦ аннулирование сертификата ключа проверки электронной подписи производится УЦ самостоятельно. При этом аннулируются все сертификаты Пользователей УЦ, выданные УЦ. Временем аннулирования сертификатов Пользователей УЦ признается время компрометации ключа электронной подписи УЦ, фиксирующееся во внутреннем документе Банка. В случае компрометации ключа электронной подписи УЦ информация о сертификатах Пользователей УЦ в список отозванных сертификатов не заносится.

6.4.***Аннулирование (отзыв) сертификата ключа проверки электронной подписи по заявлению Пользователя УЦ***.

6.4.1. При компрометации ключа проверки электронной подписи Пользователя УЦ, прекращении полномочий Пользователя УЦ, а также расторжении Договора банковского обслуживания для аннулирования (отзыва) сертификата ключа проверки электронной подписи Пользователь УЦ подает заявление на аннулирование (отзыв) сертификата в Банк в форме бумажного документа.

6.4.2. Заявление в бумажной форме содержит следующую информацию:

- идентификационные данные владельца сертификата ключа проверки электронной подписи;

- наименование Корпоративной информационной системы;

- причина отзыва сертификата;

- дата и время подачи заявления.

6.4.3. УЦ проводит действия по аннулированию (отзыву) сертификата ключа проверки электронной подписи Пользователя УЦ и вносит информацию в Реестр сертификатов в течение одного рабочего дня со дня подачи в Банк заявления на аннулирование (отзыв) Пользователем УЦ. Действие сертификата ключа проверки электронной подписи прекращается с момента внесения записи об этом в Реестр сертификатов.

6.4.4. В случае аннулирования (отзыва) сертификата по заявлению УЦ официально уведомляет Пользователя и всех лиц, зарегистрированных в УЦ, об аннулировании (отзыве) сертификата не позднее одного рабочего дня УЦ с момента подачи заявления в Банк. Официальным уведомлением о факте отзыва сертификата подписи является опубликование списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее времени наступления произошедшего случая.

6.5.По решению суда, вступившему в законную силу, УЦ аннулирует сертификат ключа проверки электронной подписи в течение не более чем одного рабочего дня.

7. Порядок ведения Реестра сертификатов ключей проверки электронной подписи и предоставления доступа к нему

7.1.Реестр сертификатов УЦ включает в себя информацию, содержащуюся в выданных УЦ сертификатах, дополнительную информацию о Пользователе УЦ, информацию о датах прекращения действия или аннулирования сертификатов, а так же об основаниях таких действий.

7.2.Ведение Реестра сертификатов включает в себя:

- создание;

- добавление новых записей;

- внесение дополнений, изменений;

- внесение сведений о прекращении действия сертификатов или об аннулировании сертификатов;

- обеспечение актуальности содержащейся информации;

- предоставление выписок из Реестра по обращению.

7.3.Реестр сертификатов, владельцами которых являются физические лица, содержит следующие поля:

- уникальный номер сертификата;

- даты начала и окончания действия сертификата;

- фамилия, имя и отчество (если имеется) владельца сертификата;

- иная информация о владельце сертификата (в зависимости от требований Корпоративной информационной системы);

- дата аннулирования (отзыва) сертификата;

- основание аннулирования (отзыва) сертификата.

7.4.Реестр сертификатов, владельцами которых являются юридические лица, индивидуальные предприниматели, содержит следующие поля:

- уникальный номер сертификата;

- даты начала и окончания действия сертификата;

- наименование и место нахождения;

- реквизиты организации;

- фамилия, имя и отчество (если имеется) физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности;

- иная информация (в зависимости от требований Корпоративной информационной системы);

- дата аннулирования (отзыва) сертификата;

- основание аннулирования (отзыва) сертификата.

7.5.Предоставление УЦ информации связанной с сертификатами ключа проверки электронной подписи и содержащейся в Реестре сертификатов, в том числе информации об аннулировании сертификата, осуществляется по письменному обращению заинтересованного в получении вышеуказанной информации лица. Обращение принимается в любом офисе Банка и оформляется в простой письменной форме с обязательным указанием следующей информации:

- фамилия, имя и отчество (если имеется), обратившегося за получением информации лица, его дата рождения, адрес регистрации по месту жительства и почтовый адрес фактического местонахождения, адрес электронной почты (если имеется);

- сведения о сертификате в составе: уникальный номер сертификата, фамилия, имя и отчество (если имеется) Пользователя УЦ;

- предпочитаемый способ получения выписки из Реестра сертификатов УЦ (почтовым отправлением, лично в офисе Банка или направлением электронным документом с использованием информационно-телекоммуникационной сети Интернет на адрес электронной почты, указанный в обращении).

7.6.Информация оформляется и представляется УЦ в форме выписки из Реестра сертификатов, подписанной собственноручной подписью и заверенная печатью УЦ или электронной подписью уполномоченного представителя УЦ в срок с момента поступления и официальной регистрации обращения, не превышающий:

- семи дней для направления информации почтовым отправлением;

- одного рабочего дня для направления выписки посредством информационно телекоммуникационных сетей или для предоставления на бумажном носителе лично обратившемуся лицу (при этом выдача выписок из Реестра сертификатов осуществляется по адресу головного офиса Банка – г. Краснодар, ул. Красная, 139);

7.7.Корневой сертификат УЦ и список отозванных сертификатов опубликованы на официальном сайте Банка https://www.1mbank.ru и доступ к ним не ограничен. Публикация списка отозванных сертификатов УЦ осуществляется регулярно в течение следующего рабочего дня с момента отзыва последнего сертификата. Дополнительно корневой сертификат УЦ и список отозванных сертификатов могут распространяться средствами Корпоративной информационной системы.

7.8. Для обеспечения защиты Реестра сертификатов от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в Банке реализуется комплекс организационно-технических мероприятий включающих в себя:

- применение сертифицированных программных и программно-аппаратных средств защиты информации;
- защиту внешних сетевых соединений;
- антивирусную защиту;
- контроль целостности программного обеспечения;
- дополнительные организационные меры по защите информации;
- применение систем обеспечения противопожарной безопасности;
- применения систем охранной сигнализации;
- физическую защиту и охрану помещения и оборудования УЦ.

Программные и программно-аппаратные средства защиты информации, применяемые в УЦ, включают в себя:

- средства криптографической защиты информации;
- программно-аппаратные комплексы защиты от несанкционированного доступа;
- средства мониторинга событий;
- системы резервного копирования и восстановления данных.

8. Проверка подлинности электронной подписи в электронных документах

8.1.В общем случае подтверждение электронной подписи в электронных документах осуществляется автоматически средствами электронной подписи в составе Корпоративной информационной системы. Однако Клиент имеет право обратиться в Банк для проведения отдельной процедуры подтверждения подлинности электронной подписи в электронных документах, циркулирующих в Корпоративной информационной системе. Для этого Клиент подает в Банк заявление на проверку подлинности электронной подписи в электронном документе в Корпоративной информационной системе.

8.2.Подтверждение подлинности электронной подписи электронного документа осуществляет УЦ на основании заявления в бумажной форме и содержащего следующую информацию:

- дата и время подачи заявления;
- наименование Корпоративной информационной системы;
- идентификационные данные субъекта, электронную подпись которого требуется проверить в электронном документе;
- уникальный номер сертификата ключа проверки электронной подписи, на котором требуется проверить электронную подпись электронного документа;
- дата и время формирования электронной подписи в электронном документе, а также другие реквизиты электронного документа (наименование, номер, содержание).

8.3. По факту получения заявления уполномоченным сотрудником Банка осуществляется поиск и выгрузка электронного документа, подписанного электронной подписью, из Корпоративной информационной системы и передача его для проверки в УЦ.

8.4.Электронная подпись в предоставленном электронном документе будет считаться равнозначной собственноручной подписи при выполнении следующих условий:

- сертификат ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности электронной подписи, не утратил силу (действует) на момент формирования электронной подписи в электронном документе - дата и время формирования электронной подписи в электронном документе, указанная в заявлении на подтверждение подлинности электронной подписи;

- электронная подпись, проверенная на сертификате ключа проверки электронной подписи с серийным номером, указанным в заявлении на подтверждение подлинности электронной подписи, верна;

- формирование электронной подписи осуществлено без нарушений условий настоящего Регламента.

8.5.По окончанию работ по проверке подлинности электронной подписи оформляется протокол проверки, который передается Клиенту.

8.6.Срок проведения работ по подтверждению подлинности электронной подписи в электронном документе и предоставлению заключения о произведенной проверке составляет 5 (пять) рабочих дней с момента его поступления в УЦ.

9. Смена ключа электронной подписи и сертификата

9.1.Плановая смена ключей электронной подписи УЦ

9.1.1. Плановая смена ключа электронной подписи УЦ и выпуск соответствующего ему корневого сертификата выполняется Администратором УЦ.

9.1.2. Максимальный срок действия ключа электронной подписи УЦ составляет 7 лет, максимальный срок действия сертификата ключа проверки электронной подписи УЦ – 30 лет.

9.1.3. Процедура плановой смены ключа электронной подписи УЦ осуществляется в следующем порядке:

- Администратор УЦ формирует новый ключ электронной подписи и соответствующий ему корневой сертификат УЦ;

- Администратор УЦ осуществляет ввод в действие нового корневого сертификата УЦ.

9.1.4. Ключ электронной подписи и корневой сертификат УЦ, замененные в ходе плановой смены, из обращения не изымаются до тех пор, пока не истекут сроки действия всех сертификатов ключей проверки электронной подписи, выданных с их использованием, а также используются для выпуска списка отозванных сертификатов.

9.1.5. По окончании процедуры плановой смены ключа электронной подписи и корневого сертификата УЦ в Реестр сертификатов вносится соответствующая запись о плановой смене ключа электронной подписи и корневого сертификата УЦ.

9.1.6. Уведомление Пользователей УЦ и Клиентов о проведении плановой смены ключа электронной подписи и коневого сертификата УЦ, осуществляется посредством размещения соответствующей информации и файла корневого сертификата, на официальном сайте Банка https://www.1mbank.ru.

9.1.7. С момента официальной публикации объявления о проведении плановой смены ключа электронной подписи и корневого сертификата УЦ все поступившие запросы на выпуск сертификата ключа проверки электронной подписи обрабатываются УЦ с использованием новых ключей электронной подписи.

9.2*.*Плановая смена ключа электронной подписи Пользователя УЦ

9.2.1. Плановая смена ключей электронной подписи и сертификатов Пользователей УЦ осуществляется с учетом особенностей Корпоративной информационной системы по окончанию срока действия текущего ключа электронной подписи и сертификата.

9.2.2. Процедура плановой смены сертификатов аналогична процедуре первичного получения сертификата и производится в порядке, предусмотренном пунктами 5.9-5.16 настоящего Регламента.

9.3*.*Внеплановая смена ключа электронной подписи УЦ

9.3.1. Внеплановая смена ключа электронной подписи УЦ осуществляется в случае:

- компрометации ключа электронной подписи УЦ;
- выхода из строя ключевого носителя содержащего ключ электронной подписи УЦ;
- в иных предусмотренных законодательством Российской Федерации случаях.

9.3.2. Процедура внеплановой смены ключа электронной подписи УЦ выполняется в порядке, определенном процедурой плановой смены ключа электронной подписи УЦ в соответствии с требованиями пункта 9.1 настоящего Регламента.

9.4*.*Внеплановая смена ключа электронной подписи Пользователя УЦ

9.4.1. Внеплановая смена ключа электронной подписи Пользователя УЦ осуществляется следующих случаях:

- компрометации ключа электронной подписи Пользователя УЦ;
- компрометации ключа электронной подписи УЦ;
- выход из строя ключевого носителя, содержащего ключ электронной подписи Пользователя УЦ;
- изменения данных Клиента или Пользователя УЦ, включенных в сертификат;
- в иных предусмотренных законодательством Российской Федерации случаях.

9.4.2. Процедура внеплановой смены ключа электронной подписи и сертификата выполняется в порядке, определенном процедурой плановой смены ключа электронной подписи в соответствии с требованиями пункта 9.3 настоящего Регламента.

9.4.3. В ходе процедуры внеплановой смены ключа электронной подписи Пользователя УЦ, предыдущий сертификат Пользователя УЦ аннулируется (отзывается) путем внесения сведений в Реестр сертификатов и формируется список отозванных сертификатов в порядке, установленном требованиями раздела 6 настоящего Регламента.

10. Компрометация ключа электронной подписи

10.1. К связанным с компрометацией ключа электронной подписи событиям относятся (включая, но не ограничиваясь) следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил хранения и уничтожения (после окончания срока действия) ключа электронной подписи;
- возникновение подозрений на утечку информации или ее искажение при передаче электронных документов в Корпоративной информационной системе;
- нарушение печати на сейфе с ключевыми носителями;
- случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

10.2. Порядок действий Пользователя УЦ при компрометации

10.2.1. Пользователь УЦ самостоятельно принимает решение о факте или угрозе компрометации своего ключа электронной подписи.

10.2.2. В случае компрометации Пользователь УЦ осуществляет блокировку своих ключей в соответствии с порядком, определенным Корпоративной информационной системой (например, по телефону с использованием контрольного ответа), аннулирование (отзыв) сертификата в порядке, установленном требованиями раздела 6 настоящего Регламента, а для возобновления работы в Корпоративной информационной системе проводит действия по внеплановой смене ключа электронной подписи в соответствии с пунктом 9.2 настоящего Регламента.

10.3. Порядок действия УЦ при компрометации

10.3.1. При компрометации ключей электронной подписи УЦ корневой сертификат УЦ аннулируется (отзывается), Пользователи УЦ уведомляются об указанном факте путем публикации информации о компрометации на официальном сайте Банка https://www.1mbank.ru. Все сертификаты, подписанные с использованием скомпрометированного ключа электронной подписи УЦ, считаются аннулированными. Обмен электронными документами в Корпоративной информационной системе должен быть остановлен.

10.3.2. УЦ проводит следующие действия:

- формирует новый ключ электронной подписи и сертификат ключа проверки электронной подписи УЦ;
- формирует список отозванных сертификатов с указанием в нем отзываемого сертификата УЦ;
- обеспечивает надежную доставку нового сертификата УЦ и списка отозванных сертификатов всем Пользователям УЦ посредством Корпоративной информационной системы или размещением на официальном сайте https://www.1mbank.ru;
- организовывает выпуск и получение Пользователями УЦ новых сертификатов.

11. Ответственность сторон

11.1. УЦ не несет ответственности за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если УЦ обоснованно полагался на сведения, указанные в заявлениях, предоставленных Клиентом, Пользователем УЦ.

11.2. УЦ несет ответственность за убытки при использовании ключа электронной подписи и сертификата ключа проверки электронной подписи Пользователя УЦ только в случае, если данные убытки возникли при компрометации ключа электронной подписи УЦ.

11.3. Ответственность Сторон, не урегулированная Регламентом, регулируется законодательством Российской Федерации.

12. Порядок рассмотрения и разбора конфликтных ситуаций

12.1. Применение электронной подписи в Корпоративной информационной системе может вызвать конфликтные ситуации, заключающиеся в оспаривании Сторонами авторства и/или содержимого электронного документа, подписанного электронной подписью.

12.2. Разбор подобных конфликтных ситуаций в соответствии с действующим законодательством и особенностями формирования самой электронной подписи осуществляется с применением программного обеспечения СКЗИ, сертифицированного ФСБ России.

12.3. Разбор конфликтной ситуации заключается в доказательстве авторства электронной подписи конкретного электронного документа конкретным исполнителем. Данный разбор основывается на математических свойствах алгоритма электронной подписи, реализованного в соответствии со стандартами Российской Федерации ГОСТ 34.10-2001 и ГОСТ Р 34.11-94, гарантирующем невозможность подделки значения электронной подписи любым лицом, не обладающим ключом электронной подписи.

12.4. При проверке значения электронной подписи используется ключ проверки электронной подписи, парный тому ключу электронной подписи, с помощью которого выполнялась процедура формирования электронной подписи.

12.5. Разбор конфликтной ситуации выполняется по инициативе Стороны и включает:

- предъявление претензии одной Стороны другой;
- формирование комиссии;
- проведение проверки электронной подписи.

12.6. Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить установленным порядком другой Стороне мотивированный отказ.

12.7. По соглашению Сторон формируется комиссия, состоящая из представителей Сторон и внешних технических экспертов (при необходимости).

12.8. Проверка подписанного электронного документа включает в себя выполнение следующих действий:

- определение сертификата или нескольких сертификатов, необходимых для проверки электронной подписи;
- проверка электронной подписи электронного документа с использованием каждого сертификата;
- проверка электронной подписи каждого сертификата, путем построения цепочки сертификатов до корневого сертификата УЦ;
- проверка действительности сертификатов на текущий момент времени;
- проверка действительности сертификатов на момент формирования электронной подписи;
- проверка отсутствия сертификатов в списке отозванных сертификатов.

12.9. Если сертификат, с использованием которого проверяется электронной подписи, отозван (т.е. включен в список отозванных сертификатов), комиссия принимает решение о действительности электронной подписи документа, используя дату создания документа и дату отзыва сертификата в списке отозванных сертификатов.

12.10. При проверке электронной подписи документа, верификации цепочки сертификатов, отсутствии сертификата в списке отозванных сертификатов, составляется протокол проверки электронной подписи, в котором фиксируются сертификаты ключей проверки электронной подписи, использованные для проверки, и факт подтверждения или неподтверждения подписи. Данный протокол является основным документом работы комиссии и должен быть подписан всеми ее членами.

12.11. В случае подтверждения электронной подписи, значения ключей проверки электронной подписи в составе сертификатов, указанных в протоколе проверки, хранящихся в Реестре сертификатов, необходимо сравнить со значениями ключей проверки электронной подписи, указанных

соответствующих бумажных экземплярах запросов на сертификат или бумажных копий сертификата. При совпадении их значений, авторство подписи под документом считается установленным.

12.12. Доказать авторство документа, подписанного электронной подписью, не представляется возможным при отсутствии в архивах сертификата ключа проверки электронной подписи Пользователя УЦ, выполнившего электронную подпись, или его бумажного экземпляра запроса на сертификат, заверенной Пользователем УЦ.

12.13. Оспаривание результатов работы комиссии выполняется в установленном действующим законодательством Российской Федерации порядке.

13. Прекращение деятельности УЦ

13.1. Решение о прекращении деятельности УЦ может быть принято Банком в одностороннем порядке.

13.2. В случае прекращения деятельности УЦ, не менее чем за один месяц до даты прекращения деятельности, Банк уведомляет об этом публикацией на официальном сайте Банка Клиентов и Пользователей УЦ, которым выданы сертификаты УЦ и срок действия сертификатов не истек.

13.3. Если функции УЦ не переходят другим лицам, то Банк осуществляет уничтожение информации, внесенной в Реестр сертификатов после завершения деятельности УЦ.

13.4. В случае перехода его функций другим лица информация, внесенная в Реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность.

14. Риски, связанные с использованием электронных подписей

14.1. Настоящим разделом Банк уведомляет Клиента о рисках, связанных с использованием электронных подписей.

14.2. При использовании электронной подписи существуют определенные риски, основными из которых являются следующие:

14.2.1. Риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает подпись под документом, может заявить о том, что подпись сфальсифицирована и не принадлежит данному лицу.

14.2.2. Риски, связанные с отрекаемостью (отказом от содержимого документа). Лицо, на которое указывает подпись под документом, может заявить о том, что документ был изменен и не соответствует документу, подписанному данным лицом.

14.2.3. Риски, связанные с юридической значимостью электронной подписи. В случае судебного разбирательства одна из сторон может заявить о том, что документ с электронной подписью не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.

14.2.4. Риски, связанные с несоответствием условий использования электронной подписи установленному порядку. В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.

14.2.5. Риски, связанные с несанкционированным доступом (использованием электронной подписи без ведома владельца). В случае компрометации ключа электронной подписи или несанкционированного доступа к средствам электронной подписи может быть получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

14.3. Свою деятельность УЦ осуществляет в строгом соответствии с законодательством и настоящим Регламентом. Благодаря соблюдению необходимых требований исключаются риски, связанные с юридической значимостью документов, подписанных электронной подписью, и снижаются риски несоответствия условий использования электронной подписи установленному порядку.

14.4. Сертификат заверяется электронной подписью УЦ и подтверждает факт владения того или иного участника документооборота тем или иным ключом проверки электронной подписи и соответствующим ему ключом электронной подписи. Благодаря Сертификату, Банк и Клиент могут опознавать друг друга, а, кроме того, проверять принадлежность электронной подписи конкретному пользователю и целостность (неизменность) содержания подписанного электронного документа. Таким образом исключаются риски, связанные с подтверждением подлинности пользователя и отказом от содержимого документа.

14.5. Преобразования сообщений с использованием ключей производятся с помощью средств электронной подписи. В Корпоративной информационной системе для этих целей используются СКЗИ, имеющие в том числе сертификаты соответствия установленным требованиям для средств электронной подписи. СКЗИ − это программное обеспечение, которое решает основные задачи защиты информации, а именно:

- обеспечение конфиденциальности информации − шифрование для защиты от несанкционированного доступа электронных документов при передаче в сети Интернет;
- подтверждение авторства документа — применение электронной подписи, которая ставится на электронные документы; впоследствии она позволяет решать на законодательно закрепленной основе любые споры в отношении авторства документа;
- обеспечение неотрекаемости − применение электронной подписи и обязательное сохранение передаваемых документов на сервере Корпоративной информационной системы у отправителя и получателя; подписанный документ обладает юридической силой с момента подписания: ни его содержание, ни сам факт существования документа не могут быть оспорены никем, включая автора документа;
- обеспечение целостности документа − применение электронной подписи, которая содержит в себе хэш-значение (усложненный аналог контрольной суммы) подписываемого документа; при попытке изменить хотя бы один символ в документе или в его подписи после того, как документ был подписан, будет нарушена электронная подпись, что будет немедленно диагностировано;
- аутентификация участников взаимодействия в Корпоративной информационной системе − каждый раз при начале сеанса работы сервер Корпоративной информационной системы и пользователь предъявляют друг другу свои сертификаты и, таким образом, избегают опасности вступить в информационный обмен с анонимным лицом или с лицом, выдающим себя за другого.

Для снижения или избежания указанных рисков Клиенту необходимо соблюдать меры безопасности непосредственно на рабочих местах Пользователей УЦ в соответствии с разделом 15 настоящего Регламента.

15. Меры, необходимые для обеспечения безопасности электронных подписей и их проверки

15.1. Настоящим разделом Банк уведомляет Клиента о рекомендуемых и обязательных мерах, которые необходимо соблюдать Клиенту для обеспечения безопасности электронных подписей и снижения рисков, связанных с использованием электронной подписи.

15.2. Клиент обязан определить порядок обеспечения информационной безопасности при работе с электронной подписью на основе организационно-технических мер защиты, изложенных в данном разделе, мер защиты для конкретной Корпоративной информационной системы, эксплуатационной документации на СКЗИ, а также действующего российского законодательства в области защиты информации.

15.3. Организация работ по защите ключевой информации.

Клиент обязан организовать защиту информации, содержащейся в ключах электронной подписи, соблюдая следующие требования:

15.3.1. Защита ключевой информации должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

15.3.2. Защита ключевой информации должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль должен периодически выполняться администратором безопасности на основе требований документации на средства защиты от НСД.

15.3.3. Должен быть определен и утвержден список лиц, имеющих доступ к ключевой информации.

15.3.4. К работе с техническими средствами с установленным СКЗИ допускаются только определенные для эксплуатации лица, прошедшие соответствующую подготовку и ознакомленные с пользовательской документацией на СКЗИ, а также другими нормативными документами по использованию электронной подписи и СКЗИ.

15.3.5. К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются доверенные лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее программное обеспечение и на СКЗИ.

15.3.6. Клиент должен назначить администратора безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ и электронной подписи, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности.

Должностные инструкции пользователей и администратора безопасности должны учитывать требования настоящих мер.

15.3.7. В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника Клиента, имевшего доступ к ключевым носителям, должна быть проведена смена ключей, к которым он имел доступ.

15.4. Размещение технических средств с установленными СКЗИ.

Клиентом должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ и ведутся работы с электронной подписью, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия таких лиц в указанных помещениях должен быть обеспечен контроль за их действиями.

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

15.5. Требования по установке СКЗИ, а также общесистемного и специального программного обеспечения.

На технических средствах, предназначенных для работы с СКЗИ и ключами электронной подписи, необходимо использовать только лицензионное программное обеспечение фирм-изготовителей.

Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива Банка, полученного по доверенному каналу.

При установке СКЗИ Клиент должен обеспечить контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент среды функционирования.

На рабочем с СКЗИ не должны устанавливаться средства разработки программного обеспечения и отладчики. Если средства отладки приложений нужны для технологических потребностей Клиента, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ ключевой информации.

Клиент должен предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатывания системного блока и разъемов). Также возможно в этих целях применение специальных средств защиты информации — аппаратных модулей доверенной загрузки или средств защиты от НСД.

После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного СКЗИ, а также его окружения в соответствии с документацией на СКЗИ.

В случае при необходимости инсталляции прикладного программного обеспечения на технические средства, на которых установлены СКЗИ, данное программное обеспечение не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

15.6. Требования по защите информации при эксплуатации СКЗИ.

Клиенту необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

Средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

Пользователям технических средств, на которых установлены СКЗИ, запрещается:

- оставлять без контроля технические средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие-либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- работать с СКЗИ при неисправности средств защиты от НСД.

Администратор безопасности Клиента должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- Не использовать нестандартные, измененные или отладочные версии ОС.

- Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.

- Исключить возможность удаленного управления, администрирования и модификации ОС и её настроек.

- На ПЭВМ должна быть установлена только одна операционная система.

- Правом установки и настройки операционной системы и СКЗИ должен обладать только администратор безопасности.

- Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).

- Режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень.

- Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

- Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):

системный реестр;

файлы и каталоги;

временные файлы;

журналы системы;

файлы подкачки;

кэшируемая информация (пароли и т.п.);

отладочная информация.

Кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

- Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

- В случае подключения компьютера с установленным СКЗИ к сети Интернет, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX) без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. С целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны сети Интернет, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

- Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.

- СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.

- Необходимо проводить перезагрузку технических средств с СКЗИ не реже одного раза в неделю.

15.7. Обращение с ключевыми носителями и ключевой информацией.

Клиент должен определить порядок учета, хранения и использования носителей ключевой информации с ключами электронной подписи и шифрования, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

Пользователям запрещается:

- Снимать несанкционированные администратором безопасности копии с ключевых носителей.

- Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей (монитор) или принтер.

- Устанавливать ключевой носитель в считывающее устройство компьютера в режимах, не предусмотренных функционированием системы, а также устанавливать носитель в другие технические средства.

- Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

Пользователь УЦ **обязан**:

- Хранить в тайне ключ электронной подписи (закрытый ключ).

- Не использовать для электронной подписи ключи, если ему известно, что эти ключи используются или использовались ранее.

- Немедленно требовать приостановления действия сертификата ключа проверки электронной подписи при наличии оснований полагать, что тайна ключа электронной подписи (закрытого ключа) нарушена (произошла компрометация ключа).

- Обновлять сертификат ключа проверки электронной подписи в соответствии с установленным регламентом.