

Приложение № 4  
к Общим условиям  
использования  
электронных документов в  
группе филиалов «РОСБАНК»  
АО «ТБАНК»

**ПОРЯДОК ВЗАИМОДЕЙСТВИЯ СТОРОН ПО ОСУЩЕСТВЛЕНИЮ ОБМЕНА  
ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ**

Настоящий Порядок определяет порядок взаимодействия Сторон при использовании Клиентом подсистемы «ИКБ» и/или подсистемы «Прямая интеграция».

**I. При использовании Подсистемы «ИКБ»**

**1. Обмен Электронными документами**

1.1. Для работы в Системе Пользователь Системы использует программно-технические средства, удовлетворяющие требованиям, приведенным в Списке технических и программных средств, необходимых для работы подсистемы «Клиент» (далее – Список).

1.2. В процессе работы Пользователь Системы выполняет в Системе следующие действия:

- Регистрация в Системе – формирование специального ЭД «регистрация», подписанного ЭП Клиента (далее – ЭПК). Работа в Системе возможна только после успешной проверки ЭПК сервером Системы;
- Работа с ЭД, исходящими от Клиента, предполагает формирование новых ЭД на основе ЭД, имеющихся в Системе и предусмотренных в заявлении. Для каждого типа ЭД в Системе имеется соответствующая экранная форма. Для документов «Платежное поручение» возможен импорт в Систему файлов определенного Банком формата. Описание структуры файла импорта имеется на сервере Банка;
- Подписание каждого ЭД одной или несколькими ЭПК. Количество ЭПК для каждого типа ЭД определено в заявлении. После подписания ЭД всеми необходимыми ЭПК в соответствии с заявлением происходит автоматическая пересылка ЭД в Банк для исполнения;
- Акцепт ЭД. Необходимость акцепта различных ЭД по тому или иному счету Клиента определяется в заявлении и в Договоре банковского счета, на основании которого открыт соответствующий счет Клиента;
- Просмотр, печать, сохранение в файл поступивших из Банка ЭД;
- Выход из Системы.

1.3. Процедура обработки ЭД сервером Системы происходит следующим образом:

- По окончании формирования ЭД Пользователи Системы подписывают ЭД ЭПК в количестве, определенном в заявлении, и отправляют ЭД в Банк. При необходимости пользователь подсистемы «ИКБ» от Клиента или пользователь подсистемы «ИКБ» от Согласующего акцептует ЭД в порядке, описанном в пункте 2.18 Общих условий.
- Сервер Банка получает ЭД и проверяет действительность всех имеющихся в нем ЭПК, и наличие акцепта при необходимости.
- Основанием для принятия Банком ЭД, переданного Клиентом по Системе, является наличие в количестве, установленном в соответствии с заявлением, и действительность всех ЭПК в ЭД и наличие, если предусмотрено заявлением или Договором банковского счета, для ЭД акцепта. При положительном результате проверки сервер Банка проставляет в документе отметку о времени приема ЭД и ЭП Банка (далее – ЭПБ), свидетельствующую о получении Банком ЭД, и сохраняет данный ЭД в Системе. При отрицательном результате проверки ЭПК ЭПБ в ЭД не проставляется, Клиент получает сообщение об ошибке средствами Системы.

1.4. Процедуры, описанные в п.1.3 настоящего Порядка, представляют собой единый и неделимый на части процесс получения Банком ЭД, не могут быть выполнены в другой последовательности или рассматриваться независимо друг от друга.

1.5. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл должен быть подписан ЭПК, содержать отметку о акцепте, отметку о времени приема документа Банком и ЭПБ. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.

1.6. Переданный Клиентом в Банк ЭД в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус ЭД изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк ЭД. Сервер Банка присваивает полученным от Клиента ЭД следующие статусы:

Рублевые платежные поручения:

- получен Банком
- документ отправлен на исполнение
- ожидание даты исполнения
- Рассчитана комиссия за РКО хх.хх.
- Принято или «обработано с ошибкой» с указанием причины, по которой документ отвергнут
- Отправлен на валютный контроль

Статусы по иным типам документов устанавливаются в Системе в зависимости от конкретного типа документа.

Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса «документ отправлен на исполнение» («ожидание даты исполнения» - для ЭД, направленных Клиентом в соответствии с п. 2.18 Общих условий), а при работе в Депозитарном модуле Системы - получение Клиентом документа типа «Статус обработки распоряжения/запроса», в котором указано, что статус обработки соответствующего ЭД Клиента «Принято к исполнению».

Банк информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Системы.

Примечание: Перечень и описание статусов ЭД, присваиваемых сервером Банка в Депозитарном модуле Системы, приведены в руководстве пользователя Депозитарного модуля Системы.

1.7. При формировании ЭД для Клиента Банк подписывает его ЭПБ. ЭД считается переданным Банком Клиенту, если он подписан ЭПБ и выложен на сервер Банка, то есть имеется в списке входящих ЭД Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.

1.8. Банк фиксирует электронные архивы полученных от Клиента ЭД, подписанных ЭПК и ЭПБ, и доставленных Клиенту ЭД, подписанных ЭПБ, и хранит их способом, обеспечивающим Клиенту доступ к данным ЭД на сервере Банка.

1.9. Клиент имеет возможность в любой момент времени проверить ЭПБ и ЭПК любого файла архива с помощью:

1.9.1. программы проверки ЭП CryptoManager.exe, установленной на Персональном компьютере. CryptoManager.exe позволяет выполнять проверку ЭП с использованием СКЗИ «Бикрипт 5.0», разрешенных для использования в Системе.

1.9.2. СКЗИ «КриптоПРО CSP» версии 5.0 и выше и программы КриптоАРМ 5 и выше, установленных на Персональном компьютере. Данные программы позволяют выполнять проверку ЭП, созданных с использованием Сервиса электронной подписи (СЭП) удостоверяющего центра

Банка, и подписанных работником Банка на депозитарных документах, при наличии такой возможности.

- Ключи проверки электронной подписи Банка и копии соответствующих Сертификатов ключей проверки электронной подписи размещаются на сервере системы <https://www.bankline.ru>. Сертификат Ключа проверки электронной подписи Банка создается и выдается только удостоверяющим центром Банка, а квалифицированный сертификат ключа проверки электронной подписи создается и выдается только Удостоверяющим центром Центрального Банка России.

- В случае возникновения ошибки при проверке ЭП на ЭД необходимо направить запрос в техническую поддержку Банка по телефону 8 485 937 75 00 (Москва), 8 800 770 75 00 (Россия) или электронную почту [icb@rosbank.ru](mailto:icb@rosbank.ru).

1.10. Разработчик Средства ЭП CryptoManager.exe – АО «ИНИСТ» (Лицензия ФСБ России № 12818Н от 16.04.2013), зарегистрированной по адресу 119334, г. Москва, 5-ый Донской проезд, д. 15, стр. 2.

1.11. Разработчик СКЗИ КриптоПРО CSP - ООО «КРИПТО-ПРО» (Лицензия ФСБ России № 12936Н от 11 июня 2013), зарегистрированной по адресу 105037, г. Москва, Измайловский проезд, дом 10, корпус 2, этаж 1, помещение IV.

1.12. Разработчик программы КриптоАРМ 5 - ООО «Цифровые технологии» (Лицензия ФСБ России № 55Н от 14.08.2013), зарегистрированной по адресу 424000, Республика Марий Эл, г. Йошкар-Ола, ул. Карла Маркса, д. 109Б, позиция 48.

## **2. Порядок получения, замены и хранения ключей**

2.1. Для Ключевой информации, созданной для работы на Персональном компьютере Клиентами:

2.1.1. Каждый Пользователь Системы осуществляет создание Ключевой информации лично, согласно заявлению, с помощью программных средств, предоставленных Банком, на Ключевые носители с использованием средств электронной подписи.

Клиент обязуется обеспечить создание Ключевой информации каждым Пользователем Системы лично.

2.1.2. При подключении Подсистемы «ИКБ» Клиентом первый Ключ проверки электронной подписи/Сертификат ключа Пользователя Системы регистрируется Банком на основании подписанного Сторонами Акта о признании ключа проверки электронной подписи. Акт о признании ключа проверки электронной подписи может оформляться:

- на бумажном носителе: в указанном случае Пользователь Системы распечатывает Акт о признании ключа проверки электронной подписи на бумаге, подписывает его и передает оригинал в Банк.

- в электронном виде: в указанном случае Пользователь Системы прикрепляет Акт о признании ключа проверки электронной подписи в виде файла в формате pdf в Контур.Диалог и подписывает его усиленной квалифицированной подписью в указанной системе либо в случае заключенного между Клиентом и Банком Соглашения об электронном обмене документами с использованием простой электронной подписи в АО «ТБАНК» в группе филиалов «РОСБАНК», Пользователь Системы прикрепляет Акт о признании ключа проверки электронной подписи в виде файла в формате pdf в Личном кабинете и подписывает простой электронной подписью в Личном кабинете.

При наличии подключенной Подсистемы «ИКБ» у Клиента Акт о признании ключа проверки электронной подписи для нового Пользователя Системы может оформляться:

- на бумажном носителе. В указанном случае Пользователь Системы распечатывает Акт о признании ключа проверки электронной подписи на бумаге, подписывает его Клиентом и передает оригинал в Банк. Акт о признании ключа проверки электронной подписи подписывается Банком.
- в электронном виде. В указанном случае Пользователь Системы:
  - прикрепляет Акт о признании ключа проверки электронной подписи в виде файла в формате pdf в Контур.Диалог и подписывает Акт о признании ключа проверки

электронной подписи усиленной квалифицированной подписью Клиента в указанной системе, либо

- прикрепляет Акт о признании ключа проверки ЭП в виде файла в формате pdf в Подсистеме ИКБ и подписывает Акт о признании ключа проверки электронной подписи усиленной неквалифицированной подписью Клиента в указанной системе, либо

- в случае заключенного между Клиентом и Банком Соглашения об электронном обмене документами с использованием простой электронной подписи в АО «ТБАНК» Пользователь Системы прикрепляет Акт о признании ключа проверки ЭП в виде файла в формате pdf в Личном кабинете и подписывает простой электронной подписью в Личном кабинете.

- при наличии у Клиента активированного Ключа проверки электронной подписи/Сертификата ключа проверки электронной подписи, созданного и выданного для единоличного исполнительного органа Клиента, и при наличии технической возможности, Клиент может сформировать запрос на Сертификат ключа проверки электронной подписи для нового Пользователя Системы в электронном виде в подсистеме ИКБ. Запрос на Сертификат ключа проверки электронной подписи подписывается единоличным исполнительным органом Клиента усиленной неквалифицированной подписью в указанной подсистеме и передается в Банк. По запросу на Сертификат ключа проверки электронной подписи Банк создает и выдает сертификат ключа проверки электронной подписи Пользователю Системы.

При этом, Клиент обязан предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия лица, подписавшего Акт о признании ключа проверки электронной подписи, если такие документы не были предоставлены Банку ранее.

2.1.3. Второй и последующий Акт о признании ключа проверки электронной подписи для существующего Пользователя Системы могут оформляться:

- на бумажном носителе: в указанном случае Пользователь Системы распечатывает Акт о признании ключа проверки электронной подписи на бумаге, подписывает его единоличным исполнительным органом Клиента и передает оригинал в Банк. Акт о признании ключа проверки электронной подписи подписывается Банком.
- в электронном виде. В указанном случае Пользователь Системы
  - прикрепляет Акт о признании ключа проверки электронной подписи в виде файла в формате pdf в Контур.Диалог и подписывает Акт о признании ключа проверки электронной подписи усиленной квалифицированной подписью в указанной системе.
  - прикрепляет Акт о признании ключа проверки ЭП в виде файла в формате pdf в Подсистеме ИКБ и подписывает Акт о признании ключа проверки электронной подписи усиленной неквалифицированной подписью Клиента в указанной системе либо
  - в случае заключенного между Клиентом и Банком Соглашения об электронном обмене документами с использованием простой электронной подписи в АО «ТБАНК» Пользователь Системы прикрепляет Акт о признании ключа проверки ЭП в виде файла в формате pdf в Личном кабинете и подписывает простой электронной подписью в Личном кабинете.
- при наличии у Клиента активированного Ключа проверки электронной подписи/Сертификата ключа проверки электронной подписи, созданного и выданного для единоличного исполнительного органа Клиента, и при наличии технической возможности, Клиент может сформировать запрос на Сертификат ключа проверки электронной подписи для нового Пользователя Системы в электронном виде в подсистеме ИКБ. Запрос на Сертификат ключа проверки электронной подписи подписывается единоличным исполнительным органом Клиента усиленной неквалифицированной подписью в указанной подсистеме и передается в Банк. По запросу на Сертификат ключа проверки электронной подписи Банк создает и выдает Сертификат ключа проверки электронной подписи Пользователю Системы.

Клиент обязан предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия лица, подписавшего Акт о признании ключа проверки ЭП, если такие документы не были предоставлены Банку ранее.

При этом, Банк вправе запрашивать, а Клиент обязан по запросу Банка предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя, в том числе являющимся единоличным исполнительным органом.

2.1.4. Срок действия Ключевой информации, в случае её создания с использованием Средства криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт», указывается в Сертификате ключа проверки электронной подписи.

2.1.5. Срок действия Сертификата ключа проверки электронной подписи, в случае создания Ключевой информации с использованием СКЗИ КриптоПро CSP, указывается в Сертификате ключа проверки электронной подписи.

2.1.6. Оформленный и подписанный со стороны Банка Акт о признании ключа проверки электронной подписи Клиента на бумажном носителе вручаются УПК либо направляются Клиенту посредством почтовой связи по адресу Клиента, указанному в Договоре.

В случае оформления Акта о признании ключа проверки электронной подписи в электронном виде он направляется Клиенту:

- через Контур.Диадок с подписанием со стороны Банка УКЭП уполномоченного лица Банка, либо
- с использованием ИКБ с подписанием со стороны Банка УНЭП уполномоченного лица Банка.

Акт о признании ключа проверки электронной подписи должен храниться у каждой из Сторон не менее пяти лет после окончания срока действия Сертификата ключа проверки электронной подписи.

2.1.7. При поступлении электронного запроса на выдачу Сертификата ключа проверки электронной подписи, подписанного действующей на момент подписания ЭП Пользователя Системы, Банк направляет Клиенту с использованием Системы Акт о признании ключа проверки электронной подписи, подписанный ЭП уполномоченного представителя Банка.

2.1.8. В случае информирования Банком Клиента в Системе о необходимости осуществить замену Ключевого носителя, Клиент обязан осуществить замену Ключевого носителя.

2.1.9. Клиент вправе обратиться в Банк с Квалифицированным сертификатом Пользователя, указанным в Заявлении Клиента. Квалифицированный сертификат Клиента проверяется Банком на действительность и актуальность сведений в нем. Если Квалифицированный сертификат действителен и сведения в нем соответствуют сведениям о клиенте, Клиент подтверждает предоставление владельцу Квалифицированного сертификата полномочий для передачи распоряжений в Банк путем оформления Акта о признании ключа проверки ЭП (Приложение №10 к Общим условиям) со сведениями из Квалифицированного сертификата.

2.2. Для Ключевой информации, созданной средствами ЭП, встроенными в Мобильное приложение:

2.2.1. Пользователь вправе создать Ключевую информацию для использования в Мобильном приложении с помощью средств ЭП, предоставленных Банком и/или встроенных в Мобильное приложение.

2.2.3. Статус ЭП Пользователя Системы, сгенерированной посредством Ключевой информации для Мобильного приложения, соответствует Статусу ЭП Пользователя Системы, указанному в заявлении при создании Ключевой информации на Ключевом носителе.

2.2.4. Обязательная замена Ключевой информации проводится в следующих случаях:

- окончание срока действия ключей ЭП;
- прекращение действия Сертификата ключа проверки электронной подписи.

2.3. В случае лишения Клиентом Пользователя Системы права подписывать ЭП ЭД соответствующие Сертификаты ключей проверки электронной подписи прекращают действие на основании письменного заявления Клиента или ЭД свободного формата, направленного в Банк посредством Системы и подписанного уполномоченным лицом Клиента.

2.4. УЦ Банка аннулирует Сертификат ключа проверки электронной подписи в следующих случаях:

- не подтверждено, что владелец Сертификата владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком сертификате;
- установлено, что содержащийся в Сертификате ключ проверки ЭП уже содержится в ином ранее созданном Сертификате;
- вступило в силу решение суда, которым, в частности, установлено, что Сертификат содержит недостоверную информацию.

#### 2.4.1. Сертификат ключа проверки электронной подписи прекращает свое действие:

- в связи с истечением установленного срока его действия;
- на основании заявления владельца сертификата ключа проверки электронной подписи, подаваемого в форме документа на бумажном носителе или в форме электронного документа;
- в случае прекращения деятельности удостоверяющего центра без перехода его функций другим лицам;
- в иных случаях, установленных Федеральным законом 63-ФЗ, другими федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между удостоверяющим центром и владельцем сертификата ключа проверки электронной подписи.

Информация о прекративших действие и аннулированных сертификатах вносится УЦ Банка в соответствующий реестр сертификатов в срок, установленный действующим законодательством Российской Федерации.

2.5. Стороны подтверждают, что услуги, связанные с использованием Систем ЭДО, позволяющих использовать усиленную квалифицированную электронную подпись, предоставляются Клиенту третьим лицом, и Банк не несет какой-либо ответственности перед Клиентом, связанной с негативными последствиями для Клиента использования таких Систем ЭДО (в том числе, но не исключительно, Банк не несет какой-либо ответственности за ущерб, причиненный Клиенту и/или третьим лицам в результате: разглашения неуполномоченным лицам ключа электронной подписи Клиента (его уполномоченного лица), его утраты, передачи или иной формы компрометации вне зависимости от причин; реализации угроз несанкционированного доступа неуполномоченных лиц к части системы электронного документооборота, подлежащей использованию со стороны Клиента; неработоспособности оборудования и программных средств Клиента и третьих лиц, повлекшей за собой невозможность доступа Клиента к соответствующей системе электронного документооборота; каких-либо иных негативных последствий, возникших в результате использования Системы ЭДО, позволяющей использовать усиленную квалифицированную электронную подпись).

Клиент согласен с тем, что обмен документами с использованием Системы ЭДО, позволяющей использовать усиленную квалифицированную электронную подпись, не является разглашением Банком сведений, составляющих банковскую тайну Клиента.

### 3. Обеспечение безопасности процедуры обмена документами

#### 3.1. Безопасность обмена ЭД достигается за счет применения следующих средств:

##### 3.1.1. Для Персонального компьютера:

- Средство криптографической защиты информации (СКЗИ) на базе Программного комплекса «Бикрипт 5.0.» (вариант исполнения 2 модификация 1), разработанного ООО Фирма «ИнфоКрипт». Клиент имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (реестр компьютера, жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов.

- Использованием СКЗИ «Криптотокен 2 ЭП» в составе USB-токенов JaCarta-2 ГОСТ, разработанных АО «Аладдин Р.Д.». Ключ электронной подписи никогда не покидает внутренней защищенной памяти USB-токена. Генерация и хранение Ключа электронной подписи, а также подписание документов производится во внутренней защищенной памяти USB-токена. Доступ к Ключу электронной подписи осуществляется с использованием пароля. Клиент имеет право вместо USB-токенов использовать для хранения Ключа электронной подписи иные носители информации (жесткий диск, съемные носители (флеш-память, внешний винчестер) и т.п.). Клиент уведомлен Банком о том, что использование вместо USB-токенов иных носителей информации существенно снижает уровень безопасности при обмене ЭД и полностью осознает возникающие при этом риски. Банк не рекомендует использование любых носителей информации за исключением USB-токенов.
- Шифрования данных в телекоммуникационных каналах с использованием СКЗИ КриптоПро CSP версии 5.0 и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security<sup>1</sup> (TLS v. 1.2, RFC 2246 и выше).
- Удостоверения принадлежности сервера Системы АО «ТБАНК» с помощью сертификата, выданного АО «ТБАНК» аккредитованным Удостоверяющим центром ООО «КРИПТО-ПРО».

#### 3.1.2. Для Мобильного приложения:

- Средства криптографической защиты информации с использованием алгоритма RSA для защиты данных от несанкционированного доступа в телекоммуникационных каналах.

3.2. Клиент уведомлен Банком о том, что создание и хранение Ключа электронной подписи, а также подписание ЭД производится во внутренней защищенной памяти Мобильного устройства. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих правил безопасности:

#### 3.2.1. Для работы на Персональном компьютере:

- Организовать выделенный компьютер подсистемы «Клиент», предназначенный исключительно для работы с Банком;
- Создание и запись Ключевой информации, а также подписание документов производить с использованием Ключевых носителей со встроенным СКЗИ JaCarta -2 ГОСТ;
- Ввести ограничение сетевого взаимодействия компьютера подсистемы «Клиент» только с необходимым доверенным перечнем IP-адресов;
- Проверять, что установлено защищенное TLS-соединение с официальным ресурсом сервиса <https://www.bankline.ru>.
- Средствами подсистемы «Клиент» закрепить за Пользователями Системы IP-адрес/список IP-адресов компьютеров подсистемы «Клиент» в целях обеспечения контроля на стороне Банка;
- Обеспечить на выделенном компьютере наличие средств защиты от вредоносного программного обеспечения, их работоспособность и регулярное обновление;
- Исключить на выделенном компьютере открытие писем с вложениями, полученными от неизвестных или недоверенных источников;
- Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;
- Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;
- Исключить использование средств удаленного администрирования;

---

<sup>1</sup> Используется протокол Transport Layer Security (TLS v.1.2, RFC 2246), применяются криптографические международные алгоритмы шифрования RSA (3072 bit), обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с SHA 512.

- Обеспечить применение лицензионного межсетевого экрана (допускается использование персонального межсетевого экрана);
- Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);
- Контролировать соблюдение требований безопасности.

#### 3.2.2. Для работы с Мобильным устройством:

- Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;
- Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;
- Исключить использование средств удаленного администрирования;
- Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты);
- Контролировать соблюдение требований безопасности;
- Обеспечить наличие антивирусного программного обеспечения.

#### 3.3. Клиент обязан:

- Исключить появление на Персональном компьютере или Мобильном устройстве подсистемы «Клиент» вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение подсистемы, скомпрометировать ключи Пользователя Системы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления;
- Исключить возможность несанкционированных Банком изменений в технических и программных средствах Клиента, определенных в Списке;
- Исключить возможность Компрометации ключей в процессе их транспортировки, эксплуатации и хранения.

#### 3.4. Стороны обязаны:

- обеспечивать конфиденциальность Ключей электронных подписей, в частности не допускать использование принадлежащих им Ключей электронных подписей без их согласия;
- уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;
- не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена.

3.5. Банк вправе в одностороннем порядке прекратить действие Сертификата ключа проверки электронной подписи Пользователя Системы в случае появления обоснованных подозрений в наличии на Персональном компьютере и/или Мобильном устройстве Пользователя Системы вирусов или других программ деструктивного действия. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон.

Если произошла Компрометация ключей любого Пользователя Клиента, последний обязан:

- В случае подозрения на несанкционированный доступ к ключу немедленно послать в Банк ЭД «Блокировка ключа». При этом Система автоматически прекратит действие Сертификата ключа проверки электронной подписи Пользователя Системы;
- В случае недоступности (утрата, хищение и т.п.) Ключевой информации сообщить Администратору Системы по телефону (телефон и электронный адрес Администратора системы указаны на сайте **Ошибка! Недопустимый объект гиперссылки.**, а также в заявлении, используя для авторизации кодовую фразу, приведенную в Акте о признании



ключа проверки электронной подписи, о факте Компрометации ключей;

- В случае утраты Пользователем Системы кодовой фразы Администратор Системы вправе произвести дополнительные действия по авторизации Пользователя Системы (обратный звонок по указанному в заявлении телефону, запрос на предоставление дополнительной информации: о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае предоставления необъективной информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о продолжении/блокировании работы Клиента в Системе;
- В срок не более трех рабочих дней после сообщения по телефону о факте Компрометации ключей направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены Ключевой информации;
- В случае принятия решения о замене Ключевой информации, созданной для Персонального компьютера, создать новую Ключевую информацию самостоятельно и направить своего представителя в Банк для её регистрации. В случае принятия решения о замене Ключевой информации, созданной в Мобильном приложении, создать новую Ключевую информацию самостоятельно в соответствии с Порядком.

Если произошла Компрометация ключей Банка, последний обязан:

- Известить Клиента о факте компрометации Ключевой информации Банка, продолжении/приостановлении работы Системы и смене Ключевой информации Банка посредством Системы с указанием даты и точного времени смены Ключевой информации Банка;
- Произвести внеплановую смену Ключевую информацию Банка, опубликовать новый Ключ проверки электронной подписи и/или копию Сертификата ключа Банка, содержащего новый Ключ проверки электронной подписи Банка, на сервере Системы.

3.6. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного по кодовой фразе Клиента Банк немедленно приостанавливает использование Системы данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде.

Дальнейшее использование Системы Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.

## **II. При использовании Подсистемы «Прямая интеграция»**

### **4. Общие правила обмена электронными документами**

4.1. Клиент самостоятельно определяет способ интеграции учетной системы и Банка. Банк поддерживает следующие варианты интеграции (каждому из вариантов интеграции соответствует свой набор электронных документов):

- через сервис «1С:ДиректБанк»;
- через протокол «SOAP» / «FTP» / «Open API»;
- через сервис «Транзит НРД» (транзит документов Клиентов через систему электронного документооборота Небанковской кредитной организации акционерного общества «Национальный расчетный депозитарий» (ИНН 7702165310);

Для перевода средств с корпоративной банковской карты необходимо использовать интеграцию с Банком через соответствующие методы REST API.

4.2. Для работы в Подсистеме «Прямая интеграция» Клиент самостоятельно производит настройки учетной системы и выполняет необходимые доработки своей системы в зависимости от выбранного способа интеграции с Банком.

4.3. Для подключения к Банку по выбранному каналу прямого обмена Клиент использует:

- web-сервис «1С:ДиректБанк», опубликованный Банком по адресу <https://www.bankline.ru/h2h/db1c/>;
- SOAP-сервер, опубликованный Банком по адресу <https://www.bankline.ru/h2h/iso/H2HService/>;
- FTPs-ресурс, предоставленный Банком персонально каждому клиенту;
- интеграционный сервис «Транзит 2.0», предоставляемый НКО АО НРД;
- REST API для перевода средств с корпоративной банковской карты, опубликованное Банком по адресу <https://www.bankline.ru/ibc/scrapBusinessController/>;
- Open API – сервер, опубликованный Банком по адресу <https://www.bankline.ru/ibc/h2h/openapi/>.

4.4. Банк поддерживает следующие типы электронных документов в зависимости от выбранного варианта интеграции:

- «1С:ДиректБанк»:
  - о документы от Клиента:
    - платежные поручения в рублях РФ;
    - платежные поручения в валюте;
    - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
  - о документы от Банка:
    - статус исполнения платежного поручения;
    - подтверждение зачисления денежных средств на счета сотрудников;
    - выписки по рублевым и валютным счетам.
- протокол «SOAP» / «FTPS» / «Open API»:
  - о документы от Клиента:
    - платежные поручения в рублях РФ и валюте;
    - заявления на покупку/продажу валюты;
    - заявления об обязательной продаже валюты;
    - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
    - документы валютного контроля;
    - заявления о размещении денежных средств;
    - документы свободного формата;
    - запросы на отзыв документа.
  - о документы от Банка:
    - статус исполнения платежного поручения;
    - подтверждение зачисления денежных средств на счета сотрудников;
    - выписки;
    - статус отзыва документа.
- через «Транзит НРД»:
  - о документы от Клиента:
    - платежные поручения в рублях РФ и валюте;
    - заявления на покупку/продажу валюты;
    - заявления об обязательной продаже валюты;
    - зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке;
    - документы валютного контроля;
    - заявления о размещении денежных средств;
    - документы свободного формата;

- о документы от Банка:
  - статус исполнения платежного поручения;
  - подтверждение зачисления денежных средств на счета сотрудников;
  - выписки.
- через REST API для перевода средств с корпоративной банковской карты:
  - о документ от Клиента:
    - поручение на перевод средств с корпоративной банковской карты на карту физического лица;
  - о документ от Банка:
    - статус исполнения поручения на перевод.

4.5. Банк поддерживает следующие форматы электронных документов в зависимости от выбранного варианта интеграции:

- «1С:ДиректБанк»: XML-формат технологии DirectBank (ДиректБанк) фирмы 1С. Описание приведено на сайте компании по адресу <https://v8.1c.ru/its/services/1c-direktbank/>.
- «SOAP» / «FTPS» / «Open API»: XML-формат стандарта ISO 20022:
  - о для платежей в рублях РФ на базе формата pain.001.001.03 (06)
  - о для статусов исполнения платежей на базе формата pain.002.001.03 (06)
  - о для выписок по окончанию операционного дня на базе формата camt.053.001.02
  - о для промежуточных выписок по запросу на базе формата camt.052.001.02
  - о для платежей в валюте и конверсии на базе формата pain.001.001.03 (06)
  - о для отзывов поручений клиента на базе формата camt.055.001.06
  - о для постановки на учет кредитного договора/контракта на базе формата auth.018.001.01
  - о для внесения изменений в ВБК на базе формата auth.021.001.01
  - о для снятия с учета контракта на базе формата auth.020.001.01
  - о для сведений о валютных операциях на базе формата auth.024.001.01
  - о для справки о подтверждающих документах на базе формата auth.025.001.01
  - о для статусов по документам Валютного контроля на базе формата auth.027.001.01
  - о для возврата ранее размещенных денежных средств на базе формата trea.325.001.01.RU
  - о для подтверждения о размещении депозита на базе формата trea.320.001.01.RU
  - о для писем свободного формата из/в банк auth.026.001.01

Детальное описание форматов предоставляется Банком в Правилах Имплементации (TIG).

- «Транзит НРД»: XML-формат стандарта ISO 20022:
  - о для платежей на базе формата pain.001.001.03 (06)
  - о для статусов исполнения платежей на базе формата pain.002.001.03 (06)
  - о для выписок по окончанию операционного дня на базе формата camt.053.001.02
- REST API для перевода средств с корпоративной банковской карты:
  - о поручение на перевод средств с корпоративной банковской карты на карту физического лица (метод /pay);
  - о статус исполнения поручения на перевод (метод /showStatus).

4.6. Для начала работы в Системе Пользователь Системы должен быть зарегистрирован в Системе, иметь действующий Сертификат/Квалифицированный сертификат и соответствующий ему ключ ЭП.

4.7. Работа с ЭД в Системе происходит с ЭД, подписанными ЭП Клиента с использованием

действующего Сертификата/Квалифицированного сертификата. Банк исполняет ЭД, полученные от Клиента, только после успешной проверки ЭП Клиента сервером Системы. ЭП Клиента под пакетом документов приравнивается к ЭП Клиента под каждым документом внутри пакета.

4.8. Клиент может создать неограниченное количество Сертификатов, либо предоставить Квалифицированные сертификаты для работы в Системе. При этом количество одновременно используемых Сертификатов/Квалифицированных сертификатов для подписания ЭД ЭП Клиента:

- для технологии «1С:ДиректБанк» - не более 4 (четырёх) Сертификатов;
- для технологий на базе протокола «SOAP» / «FTPS» / «Open API» / «Транзит НРД»/ – не ограничено.

4.9. Для технологии на базе протокола «SOAP» / «FTPS» / «Open API» / «Транзит НРД»/ Клиент может установить дополнительные требования к подписанию ЭД по сумме, заполнив соответствующий раздел заявления о настройке пользователей системы и перечне электронных документов подсистемы «Прямая интеграция» при наличии открытого расчетного счета (Приложение 1.2 к Общим условиям). В этом случае ЭД, получаемый Банком, должен быть сформирован таким образом, чтобы удовлетворять требованиям сочетания ЭП Клиента как для верификации на сервере Подсистемы «Прямая интеграция», так и для дополнительной проверки подписей на базе заявления о дополнительной настройке подписей по типам электронных документов. В случае, если Клиент уже имеет действующее соглашение для работы в подсистеме «ИКБ» и требования к подписанию ЭД, настроенные в подсистеме «ИКБ», то данные требования будут применяться к ЭД, полученным по Подсистеме «Прямая интеграция» до отмены такого требования.

4.10. Процедура обработки ЭД сервером Подсистемы «Прямая интеграция» происходит следующим образом:

- сервер Банка получает ЭД и проверяет действительность ЭП.

4.11. основанием для принятия Банком ЭД, переданного Клиентом по Подсистеме «Прямая интеграция», является наличие в количестве, установленном в соответствии с заявлением, и действительность ЭП Клиента под ЭД. При положительном результате проверки сервер Банка проставляет в ЭД отметку о времени и ЭП Банка, свидетельствующую о получении пакета Банком, и сохраняет данный документ в Подсистеме «Прямая интеграция». При отрицательном результате проверки ЭП Клиента ЭП Банка в документе не проставляется, Клиент получает сообщение об ошибке средствами Подсистемы «Прямая интеграция». Сертификат ключа проверки ЭП Банка выдается Удостоверяющим центром Центрального Банка. Документ считается переданным Клиентом в Банк, если он сохранен в архиве исходящих документов Клиента на сервере Банка. При наличии действующего договора для работы в подсистеме «ИКБ» все входящие документы будут отображаться в «Исходящих документах» Клиента на сервере Банка. Клиент может сохранить любой исходящий документ в файл для ведения собственного архива. Файл содержит ЭП Клиента, отметку о времени приема документа Банком и ЭП Банка. Файлы с сервера Банка и из архива Клиента могут затем использоваться при процедуре разрешения разногласий между Сторонами.

4.12. Переданный Клиентом в Банк документ в каждый момент времени имеет на сервере Банка определенный статус с отметкой времени его получения. Статус документа изменяется Банком. Клиент имеет возможность постоянно получать на сервере Банка информацию об изменении статуса (в том числе о времени его изменения) переданного в Банк документа. Сервер Банка присваивает полученным от Клиента документам следующие статусы:

- для технологии «1С:ДиректБанк»:
  - о Платежные поручения в рублях РФ, платежные поручения в валюте:
    - «Принят» – электронный документ прошел первичный контроль и поступил в обработку;
    - «Исполнен» – платежный документ исполнен Банком;
    - «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен;
    - «Приостановлен» – платежный документ отложен Банком по причине недостатка

средств на счете Клиента;

- «Аннулирован» – Электронный документ был отозван Клиентом с одобрения Банка;
- «Не подтвержден» – Платежный документ ожидает подтверждения по SMS или личном кабинете Клиента;
- o Зарплатные реестры на распределение зарплаты сотрудникам на счета в Банке:
  - «Принят» – электронный документ прошел первичный контроль и поступил в обработку;
  - «Исполнен» – электронный документ исполнен Банком;
  - «Отклонен банком» – электронный документ не прошел первичный контроль в Банке и был отклонен;

Стороны признают, что надлежащим уведомлением Банком Клиента о приеме к исполнению ЭД Клиента будет являться присвоение Банком ЭД Клиента статуса «Принят». Банк информирует Клиента об исполнении каждого ЭД Клиента путем направления Клиенту соответствующего уведомления посредством Подсистемы «Прямая интеграция».

- для технологии «SOAP» / «FTPS» // «Open API» / «Транзит НРД»/ используются следующие статусы:
  - «RCVD» - получено Банком;
  - «RJCT» - отклонено;
  - «ACTC» - принято, проверены подлинность и формат;
  - «ACCP» - принято, документ отправлен на исполнение;
  - «ACSP» - конечный успешный для внешних платежей;
  - «ACSC» - конечный успешный для внутренних платежей.

4.13. При формировании ЭД для Клиента Банк подписывает его ЭП Банка. Документ считается переданным Банком Клиенту, если он подписан ЭП Банка и помещен во входящие документы Клиента на сервере Банка. При наличии действующего договора для работы в Подсистеме «ИКБ», исходящие документы от Банка будут присутствовать в списке «Входящие документы» Клиента на сервере Банка. Клиент может сохранить любой входящий документ в файл для ведения собственного архива. Файлы архива могут затем использоваться при разрешении разногласий.

4.14. Банк фиксирует электронные архивы полученных от Клиента ЭД, подписанных ЭП Клиента и ЭП Банка, и доставленных Клиенту ЭД, подписанных ЭП Банка, и хранит их.

## **5. Порядок получения, замены и хранения ключей**

5.1. Клиент может запросить у Банка создание и выдачу Сертификатов своих Пользователей Подсистемы «Прямая интеграция» согласно заявлению о настройке пользователей системы (Приложение 1.2, Приложение 1.3 к Общим Условиям) в соответствии с Руководством по генерации сертификатов электронной подписи пользователя для Подсистемы «Прямая интеграция», опубликованном на сайте Банка, либо предоставить в Банк Квалифицированные сертификаты. В рамках Договора Клиент может использовать сертификаты ЭП, выданные УЦ Банка, для Пользователей Клиента в рамках заключенного договора об использовании электронных документов, либо использовать принятые Банком Квалифицированные сертификаты.

При подключении Подсистемы «Прямая интеграция» Клиентом первый Ключ проверки электронной подписи/Сертификат Пользователя Системы регистрируется Банком на основании подписанного Сторонами Акта о признании ключа проверки электронной подписи. Акт о признании ключа проверки электронной подписи может оформляться:

- на бумажном носителе. В указанном случае Пользователь Системы распечатывает Акт о признании ключа проверки электронной подписи на бумаге, подписывает его и передает оригинал в Банк.
- в электронном виде: в указанном случае Пользователь Системы прикрепляет Акт о признании ключа проверки электронной подписи в виде файла в формате pdf в Контур.Диалог и подписывает его усиленной квалифицированной подписью в указанной системе либо в случае заключенного между Клиентом и Банком Соглашения об электронном обмене документами с

использованием простой электронной подписи в АО «ТБАНК» Пользователь Системы прикрепляет Акт о признании ключа проверки электронной подписи в виде файла в формате pdf в Личном кабинете и подписывает простой электронной подписью в Личном кабинете.

При наличии подключенной Подсистемы «ИКБ» у Клиента Акт о признании ключа проверки электронной подписи для нового Пользователя Системы может также оформляться: при наличии у Клиента активированного Ключа проверки электронной подписи/Сертификата выданного для единоличного исполнительного органа Клиента и при наличии технической возможности Клиент может сформировать запрос на Сертификат ключа проверки электронной подписи для нового Пользователя Системы в электронном виде в подсистеме ИКБ. Сформированный запрос на Сертификат ключа проверки электронной подписи подписывается единоличным исполнительным органом Клиента усиленной квалифицированной подписью в указанной подсистеме. Подписанный Клиентом Акт о признании ключа проверки электронной подписи проверяется и активируется Банком. При этом Акт о признании ключа проверки электронной подписи Банком может не подписываться.

Второй и последующий Акты о признании ключа проверки электронной подписи для существующего Пользователя Системы могут оформляться в порядке, предусмотренном в п. 2.1.3. настоящего Порядка Общих условий.

При этом, Клиент обязан предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия лица, подписавшего Акт о признании ключа проверки электронной подписи, если такие документы не были предоставлены Банку ранее. Заполненный Акт о признании ключа проверки электронной подписи формируется и предоставляется Клиенту автоматически.

5.2. Стороны подтверждают, что услуги, связанные с использованием Систем ЭДО, позволяющего использовать усиленную квалифицированную электронную подпись, предоставляются Клиенту третьим лицом, и Банк не несет какой-либо ответственности перед Клиентом, связанной с негативными последствиями для Клиента использования таких Систем ЭДО (в том числе, но не исключительно, Банк не несет какой-либо ответственности за ущерб, причиненный Клиенту и/или третьим лицам в результате: разглашения неуполномоченным лицам ключа электронной подписи Клиента (его уполномоченного лица), его утраты, передачи или иной формы компрометации вне зависимости от причин; реализации угроз несанкционированного доступа неуполномоченных лиц к части системы электронного документооборота, подлежащей использованию со стороны Клиента; неработоспособности оборудования и программных средств Клиента и третьих лиц, повлекшей за собой невозможность доступа Клиента к соответствующей системе электронного документооборота; каких-либо иных негативных последствий, возникших в результате использования Систем ЭДО, позволяющего использовать усиленную квалифицированную электронную подпись).

Клиент согласен с тем, что передача Акта о признании ключа проверки электронной подписи/иной обмен документами с использованием Системы ЭДО, позволяющей использовать усиленную квалифицированную электронную подпись, не является разглашением Банком сведений, составляющих банковскую тайну Клиента.

5.3. Срок действия Сертификата ключа проверки электронной подписи указывается в Сертификате ключа проверки электронной подписи. В случае лишения Клиентом Пользователя Подсистемы «Прямая интеграция» права подписывать ЭП Клиента ЭД на основании заявления об отзыве (аннулировании) сертификата, составленном в свободном формате, Сертификат аннулируется и не подлежит восстановлению, а у владельца Квалифицированного сертификата прекращаются доступ к Системе с использованием указанного Квалифицированного сертификата.

5.4. В случае оформления Акта о признании ключа проверки электронной подписи на бумажном носителе, оформленный со стороны Банка экземпляр вручается лично представителю Клиента, курьеру Клиента, либо направляется Клиенту посредством почтовой связи.

5.5. Акт о признании ключа проверки электронной подписи должен храниться у каждой из Сторон не менее 5 (Пяти) лет после окончания срока действия Сертификата, указанного в Акте о признании ключа проверки электронной подписи.

5.6. Обязательное прекращение действия Сертификата ключа проверки электронной подписи проводится в случае Компрометации Ключей электронной подписи Клиента.

## **6. Использование неквалифицированной электронной подписи физического лица в случае добавления физического лица в качестве представителя юридического лица**

6.1. При наличии у Клиента активированного Ключа проверки электронной подписи/Сертификата ключа проверки электронной подписи и при наличии технической возможности, Клиент может сформировать запрос на добавление физического лица в качестве своего представителя -Пользователя Системы (изменение состава пользователей в Системе).

При этом, Клиент обязан предоставлять в Банк документы (в виде подлинников или надлежащим образом заверенных копий), подтверждающие полномочия Пользователя Системы, если такие документы не были предоставлены Банку ранее.

Банк проверяет полномочия и статус пользователя в соответствии со списком пользователей Системы для Клиента и, при положительном результате проверки - изменяет состав пользователей в Системе и направляет на почту, указанную Клиентом, ссылку на страницу в интернете для создания Пользователем своего пароля для доступа в Систему.

Пользователь авторизуется в Системе и создает запрос на выдачу Сертификата ключа проверки электронной подписи.

Запрос на создание и выдачу Сертификата ключа проверки электронной подписи подписывается Пользователем Системы - физическим лицом в Системе и направляется в Банк через Систему.

После Идентификации добавленного Пользователя Системы – физического лица Банк создает и выдает Сертификат ключа проверки электронной подписи Пользователю Системы в Системе.

Выданный Сертификат ключа проверки электронной подписи Пользователя Системы активируется Банком в Системе.

Банк уведомляет Пользователя Системы об активации Сертификата ключа проверки электронной подписи по электронной почте.

## **7. Обеспечение безопасности процедуры обмена документами**

7.1. Безопасность обмена ЭД достигается за счет применения следующих средств:

7.1.1. Использование СКЗИ «Криптотокен 2 ЭП» в составе USB-токенов JaCarta-2 ГОСТ, разработанных АО «Аладдин Р.Д.».

7.1.2. СКЗИ КриптоПро CSP версии 5.x и выше. Для защиты данных от несанкционированного доступа в телекоммуникационных каналах используется протокол Transport Layer Security (TLS v. 1.2, RFC 2246, Р 1323565.1.020-2020. Рекомендации по стандартизации. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)), применяются криптографические алгоритмы, обеспечивающие аутентификацию сторон, конфиденциальность и целостность. Применяются криптографически алгоритмы, описанные в стандартах:

ГОСТ Р 34.10-2012/ГОСТ Р 34.10-2018 - Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;

ГОСТ Р 34.11-2012/ГОСТ Р 34.11-2018 - Информационная технология. Криптографическая защита информации. Функция хэширования;

ГОСТ Р 34.12-2015/ГОСТ Р 34.12-2018 - Информационная технология. Криптографическая защита информации. Блочные шифры;

ГОСТ Р 34.13-2015/ГОСТ Р 34.13-2018 - Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров;

7.1.3. Аутентификация информационной системы АО «ТБанк» и сайта в информационно-телекоммуникационной сети «Интернет» осуществляется с использованием сертификата безопасности национального удостоверяющего центра, выданного оператором государственной информационной системы национального удостоверяющего центра.

7.2. На основании дополнительных соглашений между Сторонами возможно применение других мер по защите информации.

7.3. Клиенту рекомендуется обеспечить комплекс организационно-технических мер, направленных на выполнение следующих требований безопасности:

7.3.1. Обеспечить использование исключительно лицензионного программного обеспечения и операционной системы;

7.3.2. Организовать регулярную установку обновлений безопасности программного обеспечения и операционной системы;

7.3.3. Исключить использование средств удаленного администрирования;

7.3.4. Обеспечить применение межсетевых экранов (допускается использование персонального межсетевого экрана);

7.3.5. Выполнить комплекс организационных мероприятий по обеспечению информационной безопасности (настройка безопасности операционной системы, ограничение прав доступа информационной системы, организация парольной защиты, подготовка процедур реагирования на инциденты и т.п.);

7.3.6. Контролировать соблюдение требований безопасности.

7.4. Клиент обязан:

7.4.1. Исключить появление в рабочем месте клиента вирусов и других программ деструктивного действия, которые могут разрушить или модифицировать программное обеспечение Подсистемы «Прямая интеграция», скомпрометировать ключи Пользователя Подсистемы посредством применения лицензионных средств защиты от вредоносного кода и регулярного их обновления;

7.4.2. Исключить возможность Компрометации ключей в процессе их эксплуатации и хранения.

7.5. Стороны обязаны:

7.5.1. Обеспечивать конфиденциальность Ключей электронной подписи, в частности не допускать использование принадлежащих им Ключей электронной подписи без их согласия;

7.5.2. Уведомлять другую Сторону о нарушении конфиденциальности Ключа электронной подписи (Компрометации ключа) в течение не более чем 1 (Одного) рабочего дня со дня получения информации о таком нарушении;

7.5.3. Не использовать Ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного Ключа нарушена.

7.6. Банк вправе в одностороннем порядке прекратить действие Сертификата Ключа проверки электронной подписи Пользователя Подсистемы «Прямая интеграция» в случае появления обоснованных подозрений в наличии на компьютере Пользователя Подсистемы «Прямая интеграция» вирусов или других программ деструктивного действия. Для возобновления работы Клиенту после удаления с компьютера Пользователя Подсистемы «Прямая интеграция» вирусов или других программ деструктивного действия потребуется заново запросить создание и выдачу Сертификата ключа проверки электронной подписи и создать новый Ключ электронной подписи.

7.7. В случае возникновения угрозы Компрометации ключей регламентируется следующая последовательность действий Сторон.

7.8. В случае Компрометации ключей любого Пользователя Клиента, Клиент обязан:

7.8.1. В случаях несанкционированного доступа к Ключевой информации сообщить Администратору Подсистемы «Прямая интеграция» по телефону (телефон и электронный адрес Администратора Подсистемы «Прямая интеграция» указаны в заявлении о настройке пользователей Подсистемы «Прямая интеграция») о факте Компрометации или подозрении на Компрометацию), используя для авторизации данные из Акта о признании ключа проверки электронной подписи.

7.8.2. При этом, Администратор Подсистемы «Прямая интеграция» вправе произвести дополнительные действия по авторизации Пользователя Подсистемы «Прямая интеграция» (обратный звонок по указанному в заявлении телефону, запрос на предоставление дополнительной



информации: о фамилии куратора Клиента в Банке/уполномоченного сотрудника Банка, количестве пользователей и т.п.). В случае не предоставления информации Администратор ставит в известность куратора Клиента в Банке/уполномоченного сотрудника Банка и по согласованию с ним решает вопрос о продолжении/блокировании работы Клиента в Подсистеме «Прямая интеграция».

7.8.3. В срок не более 3 (Трех) рабочих дней после сообщения по телефону о факте Компрометации ключей, направить в Банк на бланке Клиента письменное объяснение случившегося, заверенное надлежащим образом подписями уполномоченных лиц и печатью Клиента (при наличии). В письме должно содержаться распоряжение Банку о приостановлении дальнейшей обработки ЭД до устранения причин случившегося и (или) замены ключей;

7.8.4. В случае принятия решения о замене Ключевой информации – Клиент обязан создать новую Ключевую информацию самостоятельно и направить своего представителя в Банк для ее регистрации.

7.9. В случае Компрометации ключей Банка, последний обязан:

7.9.1. Известить Клиента о факте компрометации ключевой информации Банка, продолжении/приостановлении работы Подсистемы «Прямая интеграция» и смене Ключевой информации Банка посредством Подсистемы «Прямая интеграция» с указанием даты и точного времени смены Ключевой информации;

7.9.2. Произвести внеплановую смену Ключевой информации Банка и передать Сертификат ключа проверки электронной подписи Банка Клиенту.

7.10. При получении по телефону сообщения о возникновении угрозы Компрометации ключей от авторизованного Клиента Банк немедленно приостанавливает использование Подсистемы «Прямая интеграция» данным Клиентом. С этого момента операции проводятся только на основании документов, оформленных в бумажном виде или с использованием иных, не связанных с Подсистемой «Прямая интеграция», средств дистанционного обслуживания.

7.11. Дальнейшее использование Подсистемы «Прямая интеграция» Клиентом возможно только после устранения угрозы Компрометации ключей Клиента.

### **III. Порядок проверки ЭД и ЭП при разногласиях**

8.1. Для разрешения споров относительно подлинности ЭД по заявлению заинтересованной Стороны, полагающей, что ее права нарушены, Сторонами в двухнедельный срок с даты подачи заявления создается Согласительная комиссия, в присутствии которой производятся все операции по подготовке и проведению процедуры разрешения спора. В состав Согласительной комиссии включаются представители Банка в количестве двух человек и представители Клиента в количестве двух человек, а в случае необходимости (по соглашению Сторон) – независимые эксперты. Представителями Банка и Клиента могут быть назначены как сотрудники этих организаций, так и иные компетентные лица, полномочия которых подтверждаются соответствующими доверенностями.

8.2. Спорным ЭД является ЭД, в отношении которого одна Сторона предъявляет претензии по его подлинности другой Стороне.

8.3. Процедура проверки подлинности ЭД проводится на оборудовании и в помещении Банка.

8.4. В присутствии членов Согласительной комиссии Банк обязан на свободном от программного обеспечения компьютере установить операционную систему Windows 8.1 и выше и программу криптографической проверки ЭП:

- для Подсистемы «ИКБ» при использовании СКЗИ «Бикрипт» - это предоставленная фирмой-разработчиком программа проверки ЭП, указанная в п.1.10-1.12 настоящего Порядка, в зависимости от проверяемых ЭП;
- для Подсистемы «ИКБ» при использовании СКЗИ «КриптоПро CSP» и для Подсистемы «Прямая интеграция» - это программа КриптоПро CSP версии 5.x и выше.

8.4.1. Сторона, отстаивающая подлинность спорного ЭД, обязана предоставить спорный ЭД и действовавшие в момент создания спорного ЭД Сертификаты ключа Стороны, подписавшей спорный ЭД, Банк обязан предоставить Сертификаты/Квалифицированные сертификаты,

записанные на съемном носителе в виде файлов. В случае если Клиент не предоставляет спорный ЭД, он предоставляется Банком.

8.4.2. Стороны обязаны предоставить информацию о проведенных плановых и внеплановых сменах Комплекта ключей Сторон и документы, удостоверяющие факты смены Комплекта ключей. Стороны также обязаны предоставить служебные ЭД Подсистемы «Прямая интеграция», в которых указаны факты получения ЭД из каналов связи и результаты их обработки (проверки).

8.5. Средством подтверждения ЭП являются:

- для Подсистемы «ИКБ» при использовании СКЗИ «Бикрипт» – Сертификаты ключей;
- для Подсистемы «ИКБ» при использовании СКЗИ «КриптоПро CSP» и для Подсистемы «Прямая интеграция» - Сертификаты ключей.

8.6. Члены Согласительной комиссии должны выполнить следующие действия:

8.6.1. Произвести с помощью программы криптографической проверки ЭП и средства подтверждения ЭП, использованного при подписании спорного ЭД, операцию проверки ЭП;

8.6.2. Создать Протокол установления подлинности ЭД – документ на бумажном носителе, в качестве результата проверки ЭП спорного ЭД (далее – Протокол). Протокол должен содержать распечатанные на бумажном носителе Сертификаты, использованные для установления подлинности ЭП, и заключение об итогах проверки ЭП спорного ЭД. Протокол должен быть подписан собственноручно всеми членами Согласительной комиссии;

8.6.3. Сравнить средства подтверждения ЭП с соответствующими средствами подтверждения ЭП, зафиксированными в Протоколе установления подлинности ЭП спорного ЭД, и установить, тождественны ли они, внести об этом запись в Протокол (данная запись заверяется подписями членов Согласительной комиссии);

8.6.4. Установить, являлись ли средство подтверждения ЭП действующим на момент создания ЭП спорного ЭД, и внести запись об этом в Протокол (данная запись заверяется подписями членов Согласительной комиссии). Сертификат/Квалифицированный сертификат признается действующим на момент создания ЭП спорного ЭД в случае, если дата создания спорного ЭД приходится на период действия Сертификата/Квалифицированного сертификата. В противном случае Сертификат/Квалифицированный сертификат признается недействующим на момент создания ЭП.

8.7. Согласительная комиссия признает Электронный документ подлинным, если одновременно выполнены условия:

8.7.1. Средства подтверждения ЭП совпадают с соответствующими средствами подтверждения ЭП, зафиксированными в Протоколе,

8.7.2. Все результаты проверки ЭП в Протоколе положительны,

8.7.3. Согласительная комиссия признала все средства подтверждения ЭП, содержащиеся в Протоколе, действующими на момент выработки ЭП.