УТВЕРЖДЕНЫ
Приказом ПАО «АКИБАНК»
от 27 июня 2014 г. №387,
с изменениями и дополнениями,
внесенными приказом:
- от 15 октября 2014 г. №629;
- от 24 июня 2015 г. №367;
- от 23 июля 2015 г. №428;
- от 30 сентября 2015 г. №533;
- от 02 ноября 2015 г. №588;
- от 30 декабря 2015 г. №693,
- от 02 мая 2017 г. №177;
- от 30 марта 2018 г. №125;
- от 06 июля 2018 г. №325;
- от 03 октября 2018 г. №510.

ПРАВИЛА

электронного документооборота с использованием системы “iBank 2” в Акционерном коммерческом ипотечном банке «АКИБАНК» (публичное акционерное общество)

Оглавление:

1. ПРИМЕНЯЕМЫЕ ТЕРМИНЫ

1.1. **Система дистанционного банковского обслуживания «iBank 2» (Система «iBank 2»)** – корпоративная информационная система электронного документооборота между Банком и его Клиентами, с использованием сети Интернет, обеспечивающая подготовку, защиту, передачу, проверку и обработку документов в электронном виде с использованием электронно-вычислительных средств обработки информации.

1.2. **Электронный документ («ЭД»)** – документ, представленный в электронной форме в виде файла или записи в базе данных, заверенный электронной подписью, подготовленный с помощью программного обеспечения Системы “iBank 2” в соответствии со всеми процедурами защиты информации.

1.3. **Электронная подпись («ЭП»)** – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1.4. **Электронный документооборот («ЭДО»)** – обмен электронными документами в соответствии с настоящими Правилами, подписанные необходимым количеством ЭП, проверка которых дала положительный результат, юридически эквивалентны получению идентичного по смыслу и содержанию документа, составленного на бумажном носителе и подписанного собственноручными подписями уполномоченных лиц стороны, отправившей Электронный документ и скрепленного печатью (при наличии).

1.5. **Договор об организации электронного документооборота с использованием системы «iBank 2» (Договор)** – договор присоединения, заключение которого означает принятие Клиентом порядка и условий ЭДО, осуществляемого в соответствии с Правилами, который заключается между Банком и новым Клиентом путем представления Клиента Заявления о распространении электронного документооборота в ПАО «АКИБАНК» по форме Приложения №4 к настоящим Правилам.

1.6. **Базовый договор** – сделка, заключенная между Банком и Клиентом, ЭДО по которому обеспечивается в соответствии с настоящими Правилами и Договором.

1.7. **Средства ЭП** - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание ЭП с использованием Закрытого ключа ЭП, проверка подлинности ЭП с использованием Открытого ключа ЭП, создание Закрытого ключа ЭП и Открытого ключа ЭП.

1.8. **Ключ ЭП (Ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи.** Ключ состоит из Открытого и Закрытого ключей ЭП, которые связаны между собой с помощью особого математического соотношения.

1.9. **Открытый ключ ЭП (ключ проверки ЭП)** – уникальная последовательность криптографических символов, однозначно связанная с Закрытым ключом ЭП и предназначенная для проверки подлинности ЭП.

1.10. **Закрытый ключ ЭП** – уникальная последовательность криптографических символов, известный только Владельцу сертификата открытого ключа ЭП и предназначенный для создания ЭП с использованием Средств ЭП. Закрытый ключ ЭП генерируется в USB-токене и используется участниками Системы “iBank 2” при формировании ЭП.

1.11. **Каталог открытых ключей ЭП** – база данных Банка, элементами которой являются: наименования/ Ф.И.О. участников Системы, действующие Открытые ключи ЭП и идентификаторы Открытых ключей ЭП.

1.12. **Сертификат открытого ключа ЭП (сертификат ключа проверки ЭП)** – документ на бумажном носителе, оформленный по форме Приложения №2 настоящих Правил, выдаваемый Банком (выступающим в качестве удостоверяющего центра) уполномоченному участнику

Системы для подтверждения **принадлежности ключа проверки ЭП Владельцу сертификата открытого ключа проверки ЭП.**

1.13. **Компрометация ключа** – событие, связанное с утратой доверия к тому, что используемые Ключи ЭП обеспечивают возможность установления авторства и целостности содержания ЭД. К таким событиям относятся, включая но, не ограничиваясь следующие:

- утрата носителей информации (USB-токенов) с Закрытыми ключами ЭП;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- случаи, когда нельзя достоверно установить, что произошло с носителем информации (USB-токеном), содержащим ключевую информацию (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника),
- иные события, в результате которых используемый Ключ ЭП в целом или его часть (Открытый либо Закрытый ключи ЭП) могут стать, известны или доступны третьим лицам, не уполномоченным на пользование ими.

1.14. **Блокировочное слово** - уникальное слово, определяемое Клиентом при регистрации в Системе, для блокирования работы Клиента по телефонному звонку в Банк.

1.15. **USB-токен «iBank 2 Key» или смарт-карта «iBank 2 Key» или «Рутокен ЭЦП» (далее - «USB-токен»)** - представляет собой компактное USB-устройство с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. USB-токен предназначен для генерации и защищенного хранения ключей шифрования и электронной подписи, выполнения шифрования и электронной подписи в самом устройстве, хранения цифровых сертификатов и иных данных. Аппаратная реализация криптографических алгоритмов (электронной подписи, хеш-функции и шифрования) внутри устройства обеспечивает конфиденциальность обрабатываемой информации при передаче и хранении, целостность обрабатываемой информации, а так же подтверждение авторства посредством электронной подписи.

1.16. **One-Time Password токен («OTP-токен»)** - аппаратное устройство производства компании ActivIdentity, Inc. (США), предназначенное для генерации одноразовых паролей и используется для аутентификации Клиента в Системе «iBank 2».

1.17. **MAC-токен** – автономное устройство производства компании ActivIdentity, Inc. (США), оснащенное дисплеем и цифровой клавиатурой, предназначенное для вычисления усиленной неквалифицированной электронной подписи под документом по средствам хранящегося в устройстве секретного ключа, счетчика времени и/или состояний, а также значений полей документа (например, для платежного поручения – сумма, номер счета и БИК банка получателя).

1.18. **SMS-Банкинг** – дополнительная услуга Банка для Клиентов Системы «iBank 2», предусматривающая составление и передачу Клиенту SMS-сообщений на номер мобильного телефона, указанный Клиентом о текущих остатках и о движении средств по счетам Клиента, а так же о иных событиях.

1.19. **Тикер для корпоративного клиента («Тиккер»)** - дополнительный сервис Банка для Клиентов Системы «iBank 2», предусматривающий оперативное информирование Клиента о движении средств по расчетным счетам Клиента обслуживаемым в системе «iBank 2», а также о входящих письмах Банка.

1.20. **Центр финансового контроля («ЦФК»)** - дополнительная услуга Банка для обслуживания крупных корпоративных Клиентов Системы «iBank 2» с территориально удаленными подразделениями и дочерними организациями (Подчиненные организации), предусматривающая централизованное управление счетами нескольких организаций, финансовый мониторинг и визирование документов по счетам Подчиненных организаций, входящих в группу ЦФК.

1.21. **«Модуль iBank2 для 1С» -** дополнительный сервис Банка для Клиентов Системы «iBank 2», позволяющий Клиенту напрямую из любой из указанных в п.15.3 настоящих Правил конфигураций на платформе «1С:Предприятие 8»:

- создавать, подписывать электронной подписью и отправлять в Банк платежные поручения;

- отслеживать статусы ранее отправленных документов;

- получать из Банка выписки по счетам за произвольный период;

- вести переписку с сотрудниками Банка по защищенному каналу.

1.22. **Статус Электронного документа** – состояние ЭД в базе данных Банка, однозначно соответствующее стадии обработки ЭД в Банке.

1.23. **Подтверждение подлинности ЭП (Корректная ЭП) в ЭД** - положительный результат проверки Средством ЭП с использованием Сертификата открытого ключа ЭП (Открытого ключа ЭП) принадлежности ЭП Владельцу сертификата открытого ключа подписи и отсутствия искажений в подписанном данной ЭП.

1.24. **Целостность ЭД** - означает, что после его создания и заверения подписью в его содержание не вносилось никаких изменений.

1.25. **Авторство ЭД** - принадлежность ЭП конкретному физическому лицу - участнику электронного документооборота в Системе “iBank 2”.

1.26. **Владелец сертификата открытого ключа ЭП (сертификата ключа проверки ЭП)** – уполномоченное лицо, осуществляющее от имени Клиента работу в Системе “iBank 2”, на имя которого Банком выдан Сертификат открытого ключа ЭП и которое владеет соответствующим Закрытым ключом ЭП, позволяющим с помощью Средств ЭП создавать свою ЭП (подписывать ЭД).

1.27. **Группа подписи** – очередность подписания ЭД ЭП Уполномоченных лиц Стороны, определяемая организационно-распорядительными документами Стороны:

а) группа подписи № 1 – уполномоченное/ые лицо/а Клиента, обладающее/ие правом подписи ЭД. Возможные сочетания подписей лиц, наделенных правом подписи, необходимых для подписания документов, определяются соглашением между Банком и Клиентом;

б) группа без права подписи – уполномоченное/ые лицо/а Клиента, обладающее/ие правом работы с Электронными документами Клиента, за исключением права подписывать ЭП Электронные документы.

1.28. **Форма ЭД** - совокупность реквизитов, установленных в соответствии с целями и характером правоотношений, определяемых действующим законодательством РФ, договорами Сторон, и расположенных в определенном порядке в ЭД.

1.29. **Формат ЭД** - структура ЭД как файла, определяющая способ его хранения и отображения на экране или при печати.

1.30. **Уполномоченное лицо** – физическое лицо, наделенное правом подписи соответствующих документов от имени Стороны на основании распорядительного акта Стороны, либо на основании доверенности, выданной в порядке, установленном законодательством РФ.

1.31. **Web-сайт** – официальный сайт Банка имеющий уникальный сетевой адрес http://www.akibank.ru/ на котором в целях информирования Клиентов, размещается необходимая информация о деятельности и функционировании Системы “iBank 2”.

1.32. **Компания-разработчик Системы «iBank 2»** - АКЦИОНЕРНОЕ ОБЩЕСТВО "БИФИТ" (адрес местонахождения: 105203, г.Москва, ул.Нижняя Первомайская, дом 46, Помещение XIII, ИНН 7719617469, ОГРН 1077746075461), обладающая исключительными правами на Систему «iBank 2».

1.33. **«Доверенные получатели»** – дополнительный сервис Банка для Клиентов Системы «iBank 2», предоставляется при совершении Клиентом в системе “iBank 2” операций по его банковским счетам в валюте РФ путем получения на выделенный Клиентом номер мобильного телефона или иного устройства одноразового пароля для подтверждения внесения контрагентов в список доверенных получателей платежей.

1.34. **Сервис проверки контрагентов «Индикатор» (Сервис «Индикатор»)** – сервис, позволяющий Клиенту в процессе оформления платежного поручения по переводу денежных средств в системе «iBank 2» получать информацию на основе данных из открытых источников федеральных органов власти (ФНС, ФССП, Росреестр, Генпрокуратура и др.) о фактах деятельности юридических лиц и индивидуальных предпринимателей.

1.35. **Мобильное приложение «АКИБАНК Бизнес» (Приложение «АКИБАНК Бизнес» или «Mobile-Банкинг для корпоративных клиентов»)** – программа для работы в Системе “iBank 2”, исключительные права на которую принадлежат Компании - разработчику Системы «iBank 2», предоставляющая уполномоченным сотрудникам Клиента получить круглосуточный доступ к услугам электронного банкинга посредством Мобильных устройств.

1.36. **Сервис «Мобильный-банк»** – услуга, оказываемая Банком, которая позволяет Клиенту получать доступ к Приложению «АКИБАНК Бизнес».

1.37. **Мобильное устройство** – мобильный телефон, планшетный компьютер, умные часы или аналогичное мобильное устройство уполномоченного сотрудника Клиента, используемое для работы в Приложении «АКИБАНК Бизнес».

1.38. **Ключ серверной подписи** – ключ электронной подписи уполномоченного сотрудника Клиента, который хранится в зашифрованном на пароле виде только на Мобильном устройстве Клиента и используемый для подписания документов в Приложении «АКИБАНК Бизнес».

Для ключа серверной подписи пароль задается уполномоченным сотрудником Клиента в Приложении «АКИБАНК Бизнес», при этом пароль доступа известен только данному уполномоченному сотруднику Клиента. В процессе работы вместо пароля может использоваться механизм подтверждения действий с использованием отпечатка пальца, что равносильно вводу пароля.

1.39. **Серверная подпись** – электронная подпись, созданная посредством Ключа серверной подписи.

1.40. **Ключ проверки серверной подписи** – сертификат ключа проверки ЭП, соответствующий Ключу серверной подписи. Выпускается с использованием ЭД «Заявление на выпуск сертификата ключа проверки ЭП», который формируется Управляющим Сервисом «Мобильный-банк» в Приложении «АКИБАНК Бизнес» и направляется в Банк по Системе «iBank 2». Принадлежность Ключа проверки серверной подписи владельцу Сертификата ключа проверки серверной подписи подтверждается с помощью ЭД «Заявление на выпуск сертификата ключа проверки ЭП», при этом этот документ равнозначен Сертификату ключа проверки серверной подписи.

Сертификат ключа проверки серверной подписи может быть выпущен только для уполномоченного сотрудника Клиента, имеющего право подписи платежных документов.

1.41. **Управляющий Сервисом «Мобильный-банк» –** единоличный исполнительный орган Клиента (для Клиентов, являющихся юридическим лицом) или индивидуальный предприниматель (для Клиентов, являющихся индивидуальными предпринимателями и лицами, занимающимися частной практикой), далее по умолчанию – «Руководитель», либо иной сотрудник Клиента, уполномоченный Руководителем, согласно соответствующего Заявления по форме Приложения №4 к настоящим Правилам, управлять Сервисом «Мобильный-банк», осуществлять добавление и удаление уполномоченных сотрудников Клиента, которым предоставлен доступ к такому сервису, добавление, изменение и удаление номеров мобильных телефонов таких сотрудников Клиента.

1.42. «**Налоговый календарь»** – дополнительный сервис, предусматривающий просмотр подробной информации о выбранном налоге или сборе, поиск нужного налога по ключевым словам, создание напоминаний в календаре Мобильного устройства. Сервис доступен в Приложении «АКИБАНК Бизнес» по умолчанию на безвозмездной основе.

1.43. **«Аналитика»** – дополнительный сервис, предусматривающий просмотр отчетов об изменении остатка средств, поступлениях и списаниях по всем счетам за выбранный период, возможность выбора временных периодов просмотра отчетов – 7, 30 или 90 дней. Сервис доступен в Приложении «АКИБАНК Бизнес» по умолчанию на безвозмездной основе».

1.44. Термины их понятия указанные в настоящем разделе распространяются и используются в рамках настоящих Правил и Договора.

2. ПРЕДМЕТ РЕГУЛИРОВАНИЯ НАСТОЯЩИХ ПРАВИЛ

2.1. Настоящие Правила, а также Приложения к настоящим Правилам устанавливают общие принципы осуществления ЭДО между Банком и Клиентами, определяют требования к оформлению и содержанию ЭД, их форматы и реквизиты, особенности порядка их обработки, исполнения и хранения.

2.2. Положения настоящих Правил применяются, если иное не предусмотрено законодательными или иными правовыми актами РФ, включая нормативные акты Банка России.

2.3. Настоящие Правила не регулируют вопросы обмена электронными сообщениями, не являющимися ЭД в соответствии с настоящими Правилами.

2.4. ЭДО между сторонами возможен только при условии присоединения к Правилам путем представления Клиентом Заявления о распространении электронного документооборота в ПАО «АКИБАНК» по форме Приложения №4 к настоящим Правилам.

2.5. С момента присоединения к Правилам и внесения платы, согласно Тарифам за подключение к Системе «iBank 2» и соответствующим сервисам, Клиент получает возможность пользоваться следующими услугами (сервисами) в рамках Системы «iBank2»:

а) **совершение операций по банковскому счету Клиента в рублях** (при наличии открытого банковского счета в Банке и представлении в Банк Заявления по форме Приложения №4 к настоящим Правилам);

б) **совершение операций по банковскому счету Клиента в иностранной валюте** (при наличии открытого банковского счета в Банке в иностранной валюте и представлении в Банк Заявления по форме Приложения №4 к настоящим Правилам);

в) **поддержка зарплатных проектов Банка:** направление реестров о зачислении денежных средств на счета банковских карт сотрудников Клиента и иных операций с банковскими картами (при наличии открытого банковского счета в Банке);

г) **услуга «Центр финансового контроля»** для Клиентов, имеющих открытый счет в Банке либо для управляющего Клиента, не имеющего открытого счета в Банке. Услуга предоставляется Банком на основании соответствующего волеизъявления Клиентов Системы «iBank 2», входящих в группу ЦФК, путем заключения соответствующего соглашения между Банком и Подчиненной организацией, а так же между Банком и Управляющим Клиентом и заполнением Заявления о подключении сервисов услуги Центр Финансового Контроля по форме Приложения №11 к настоящим Правилам;

д) **услуга «SMS-банкинг»** (подключается на основании Заявления по форме Приложения №4 к настоящим Правилам);

е) **сервис «Тикер для корпоративного клиента»** (предоставляется по соответствующему Заявлению по форме Приложения №4 к настоящим Правилам);

ж) **сервис «OTP–токен», сервис «MAC–токен»** (предоставляется по соответствующему Заявлению по форме Приложения №4 к настоящим Правилам и считается подключенный с момента подписания обеими сторонами Акта приема передачи устройства OTP-токен/ MAC–токен по форме Приложения №7 к настоящим Правилам);

з) **услуга по проведению депозитных сделок** (при условии заключения соответствующего соглашения, предусматривающего заключение данных сделок с использованием Системы “iBank 2”);

и) **услуга по поддержанию неснижаемого остатка на счете** (при условии заключения соответствующего соглашения, предусматривающего заключение данных сделок с использованием Системы “iBank 2”);

к) **совершение операций по банковскому счету Клиента в рублях с использованием корпоративных карт, эмитированных ПАО «АКИБАНК»** (при наличии заключенного Договора об открытии счета и обслуживании корпоративных карт)**, а так же направление соответствующих заявлений, оформляемых при обслуживании корпоративных карт** (по форме, предусмотренной Условиями обслуживания счета и корпоративных карт, эмитированных ПАО «АКИБАНК»);

л) **согласование условий кредитования банковского счета Клиента в форме овердрафт** (при условии, если базовым договором предусмотрено заключение данных сделок с использованием системы “iBank 2”)»;

м) **направление заявления на предоставление транша в рамках договора об открытии кредитной линии с лимитом задолженности / договора об открытии кредитной линии с лимитом выдачи** (при условии, если базовым договором предусмотрено такое направление с использованием системы “iBank 2”)»;

н) **сервис «Банковский ассистент»** (предоставляется при наличии открытого банковского счета в Банке всем Клиентам, без предоставления отдельного Заявления на его подключение);

о) **услуга «Организация расчетов клиентов с контрагентами, имеющих расчетные счета в ПАО «АКИБАНК» (в т.ч. в филиалах Банка) с использованием реестров к платежным поручениям** (предоставляется при условии заключения соответствующего дополнительного соглашения к договору банковского счета Клиента, предусматривающего осуществление перевода денежных средств одним платежным поручением с приложением реестра, с взиманием платы, согласно Тарифам);

п) **сервис «Модуль iBank2 для 1С»** (предоставляется в рамках пакета обслуживания ЭДО, согласно Тарифам);

р) **сервис «Доверенные получатели»** (предоставляется по соответствующему Заявлению по форме Приложения №4 к настоящим Правилам);

с) **совершение вексельной сделки по выпуску простых векселей Банка** (при условии, если базовым договором предусмотрено заключение данных сделок с использованием системы “iBank 2”)»;

т) **сервис «Индикатор»** предоставляется всем Клиентам системы “iBank 2” в режиме ограниченной версии;

у) **сервис «Мобильный-банк»** (Подключение «Информационного режима» и настройка прав доступа Уполномоченных лиц выполняется Клиентом самостоятельно в разделе «Управление услугами» в Системе «iBank 2». Подключение «Полнофункционального режима» производится после успешного подключения к «Информационному режиму» путем заполнения соответствующего Заявления по форме Приложения №4 к настоящим Правилам и создания на каждого Уполномоченного лица Ключа серверной подписи и соответствующего ему Ключа проверки серверной подписи;

ф) дополнительный сервис «Налоговый календарь» доступен всем Клиентам в Приложении «АКИБАНК Бизнес»;

ч) дополнительный сервис «Аналитика» доступен всем Клиентам в Приложении «АКИБАНК Бизнес»;

ш) предоставление иных услуг, ЭДО которого предусмотрен Базовыми договорами.

3. ГЕНЕРАЦИЯ И РЕГИСТРАЦИЯ КЛЮЧЕЙ ЭП

3.1. Генерация и регистрация Ключей ЭП Клиента осуществляется в следующей последовательности:

3.1.1. Клиент путем обращения к серверу Системы “iBank 2” по адресу https://ibank.akibank.ru/ самостоятельно осуществляет генерацию Ключей ЭП. В процессе генерации одновременно формируются Закрытый ключ ЭП связанный с ним Открытый ключ ЭП и Сертификат открытого ключа ЭП.

3.1.2. Закрытый ключ ЭП создается и в последующем хранится только в памяти USB-токена.

3.1.3. Открытый ключ ЭП автоматически направляется по защищенному соединению сети Интернет в Банк и предварительно регистрируется.

3.1.4. Полученный в результате генерации Сертификат открытого ключа ЭП распечатывается Клиентом на бумажных носителях в количестве 2 (Двух) экземпляров и заверяется собственноручными подписями Владельца сертификата открытого ключа, руководителя Клиента (либо соответствующего Уполномоченного лица) и скрепляется печатью.

3.1.5. После надлежащего оформления, Сертификат открытого ключа ЭП в 2 (Двух) экземплярах направляется в Банк посредством личного обращения Клиента либо через его представителя наделенного соответствующими полномочиями.

3.1.6. Одновременно с Сертификатом открытого ключа ЭП в Банк предоставляются документы в отношении Уполномоченных лиц указанных в нем, удостоверяющие их личности (оригиналы или нотариально заверенные копии), и документы, подтверждающие полномочия указанных лиц на подписание ЭД (оригиналы или заверенные в установленном Банком порядке копии с предоставлением оригиналов для сверки), если актуальные версии данных документов в Банк не представлялись ранее.

3.1.7. После получения Сертификата открытого ключа ЭП и документов указанных в п. 3.1.6. Правил, Банк производит сверку предварительно зарегистрированного Открытого ключа ЭП переданного в Банк в электронном виде в момент генерации, с данными Открытого ключа ЭП указанного в представленном Сертификате открытого ключа ЭП. Помимо этого проверка производится в отношении идентификационных данных Клиента, паспортных данных Уполномоченных лиц Клиента и их полномочий (в части соответствия присвоенной Группе подписей, и сроков действия полномочий), а также соответствия собственноручных подписей Уполномоченных лиц Клиента.

3.1.8. При положительном результате проверки Банк регистрирует Открытый ключ ЭП в Каталоге открытых ключей Системы “iBank 2”, после чего проставляет на 2 (Двух) экземплярах бумажных носителей Сертификата открытого Ключа ЭП дату приема, сроки действия Сертификата открытого Ключа ЭП, подпись уполномоченного лица Банка и скрепляет их печатью. После заверения, Клиенту передается один экземпляр Сертификата открытого ключа ЭП, второй экземпляр остается на хранении в Банке.

3.1.9. Сертификат открытого ключа ЭП считается зарегистрированным, а соответствующие Ключи ЭП активированными, с даты проставленной Банком на бумажных носителях Сертификата открытого ключа ЭП.

3.1.10. Сертификат открытого ключа ЭП (Ключи ЭП) Клиента считается действующим в момент проверки ЭП при одновременном выполнении следующих условий:

- сертификат открытого ключа ЭП зарегистрирован в Банке;

- срок действия Сертификата открытого ключа ЭП не истек;

- действие Сертификата открытого ключа ЭП не приостановлено и не отменено.

4. СМЕНА, БЛОКИРОВКА И ИСКЛЮЧЕНИЕ КЛЮЧЕЙ ЭП

4.1. Смена (перегенерация) Ключей ЭП может быть инициирована любой из Сторон по следующим основаниям:

а) Компрометация Ключей ЭП;

б) Истечение сроков действия Ключей ЭП;

в) Смена Уполномоченных лиц Клиента;

г) Утрата (отмена) прав на подписание ЭД Уполномоченными лицами Клиента;

д) Любое иное основание заявленное Сторонами.

4.2. Если смена Ключей ЭП производится по инициативе Банка, Банк обязан проинформировать об этом Клиента посредством Системы “iBank 2”. С указанной Банком даты прежние Ключи ЭП Клиента считаются недействительными.

4.3. Если смена Ключей ЭП производится по инициативе Клиента, Клиент обязан предоставить в Банк письменное уведомление об отмене Ключей ЭП, в котором указывает реквизиты ключа и причину смены. При этом прежние ключи Клиента независимо от факта перегенерации считаются недействительными с даты и времени, указанных Клиентом в соответствующем уведомлении, при условии получения Банком данного уведомления до истечении указанной даты и времени.

4.4. Смена Ключей ЭП осуществляется Клиентом самостоятельно в порядке, изложенном в п. 3.1. Правил.

4.5. Действие Ключей ЭП может быть временно приостановлено (заблокировано) по инициативе любой из Сторон вне зависимости от причин и оснований, повлекших данную приостановку.

4.6. Блокировка Ключей ЭП по инициативе Клиента, может быть инициирована в течение установленного режима работы Банка одним из следующих способов:

а) При личной явке Клиента (уполномоченного представителя Клиента) в Банк путем предоставления письменного уведомления, оформленного в соответствии с требованиями Банка;

б) По телефону либо иному доступному каналу связи, используя Блокировочное слово, с последующим предоставлением в Банк письменного уведомления, оформленного в соответствии с требованиями Банка.

4.7. С момента получения Банком уведомления Клиента, либо с момента принятия соответствующего решения со стороны Банка, любые действия Клиента в Системе “iBank 2” с использованием заблокированных Ключей ЭП приостанавливаются. Время начала блокировки фиксируется в Системе “iBank 2”.

4.8. Возобновление (разблокировка) действия Ключей ЭП производится на основании письменного заявления Клиента, оформленного в соответствии с требованиями Банка, либо после устранения причин их приостановления на основании решения Банка.

4.9. Исключение Открытых ключей ЭП Клиента из Каталога открытых ключей Системы “iBank 2” производится на основании прекращения действия Договора, а также в случаях перегенерации Ключей ЭП.

4.10. После исключения из Каталога, Открытые ключи ЭП Клиента и соответствующие им Сертификаты открытых ключей ЭП хранятся в течение всего срока хранения ЭД, для подтверждения, подлинности которых они могут быть использованы.

4.11. Уничтожение Открытых ключей ЭП после истечения срока их хранения осуществляется Сторонами самостоятельно.

5. ПОРЯДОК ХРАНЕНИЯ И СРОК ДЕЙСТВИЯ КЛЮЧЕЙ ЭП

5.1. Срок действия Ключей ЭП определяется сроком полномочий Владельца сертификата открытого Ключа ЭП, но не может превышать 3 (Три) года с даты начала действия Открытого ключа ЭП.

5.2. Банк уведомляет Владельца сертификата открытого ключа ЭП о предстоящем истечении срока действия ключа по Системе “iBank 2” за 30 календарных дней до даты окончания срока.

5.3. По окончании срока действия Ключи ЭП подлежат обязательной перегенерации Клиентом в соответствии с п.3.1 Правил, при этом прежние Ключи ЭП Клиента, по которым истек срок действия, считаются недействительными с даты, следующей за датой окончания срока их действия.

5.4. Способ хранения Клиентом Закрытых ключей ЭП и паролей должен исключать утрату и использование неуполномоченными лицами. Клиент обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение Закрытых ключей ЭП.

5.5. В Системе “iBank 2” Банка хранятся только Открытые ключи ЭП Клиента. Закрытые ключи ЭП Клиента третьим лицам и Банку не известны.

5.6. Ответственность за все возможные последствия использования Ключей ЭП Клиента неуполномоченными лицами несет Клиент.

6. ПОРЯДОК РАБОТЫ В СИСТЕМЕ “IBANK 2” И СОЗДАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

6.1. Стороны имеют право обмениваться ЭД, формат и перечень которых приведен в Перечне ЭД (Приложение №1 к Правилам), предназначенных для передачи по Системе “iBank 2”, при условии подключения Клиента к той или иной дополнительной услуге (сервису). Пересылка по Системе «iBank 2» ЭД, формат и перечень которых неоговорен настоящими Правилами, а также файлов, содержащих различные активные (исполняемые) элементы, вирусы и т.п., недопустима. Ответственность за причиненный ущерб ложится на Сторону – отправителя такого файла.

6.2. Формирование и последующее представление ЭД может производиться только в соответствии с установленной Правилами формой и форматом, определенных в Системе «iBank 2».

6.3. Формы ЭД установленные Банком приведены в виде шаблонов ЭД. Банк посредством Системы «iBank 2» обеспечивает доступ Клиента к описанию формы и правилам заполнения реквизитов ЭД. Банк может в одностороннем порядке изменять форму и правила заполнения ЭД, размещая актуальную версию Правил в соответствующих разделах Web-сайта.

6.4. Указание на источник формы по каждому конкретному ЭД, а также возможный формат исполнения приведен в Перечне ЭД.

6.5. Инициатором передачи ЭД в Банк, а также получения от Банка ЭД или информации, переданной по Системе «iBank 2», является Клиент. Для получения по Системе «iBank 2» от Банка интересующей его информации Клиент формирует соответствующие запросы, в ответ на которые Банк предоставляет запрашиваемую информацию.

6.6. Клиент самостоятельно устанавливает соединение с Интернет - сервером Системы «iBank 2» и следит за поддержанием сеанса связи во время работы в Системе «iBank 2».

6.7. После осуществленной Системой «iBank 2» идентификации Клиента последний получает доступ к Системе «iBank 2».

6.8. Для отправки созданного ЭД, Клиент средствами Системы «iBank 2», формирует электронное сообщение, присваивая ему, наименование которое четко должно указывать на цель отправки, наименование ЭД, а также во исполнение какого Базового договора производится передача. После чего программным путем прикрепляет соответствующий ЭД к электронному сообщению.

6.9. После формирования электронного сообщения прикрепленный к нему ЭД должен быть заверен ЭП Клиента в строгом соответствии с установленным порядком подписания документов на бумажном носителе, аналогом которых являются соответствующие ЭД.

6.10. Система «iBank 2» автоматически отображает сведения о текущем этапе обработки Клиентом и/или Банком ЭД посредством присвоения ЭД определенного статуса в Системе «iBank 2».

6.11. Система «iBank 2» присваивает ЭД следующие статусы:

а) «новый»: присваивается вновь созданному в Системе «iBank 2» ЭД;

б) «подписан»: присваивается ЭД, заверенному необходимым количеством ЭП Клиента;

в) «доставлен»: присваивается ЭД, успешно прошедшему проверку в соответствии с п. 7.2. Правил;

г) «отвергнут»: присваивается ЭД, не прошедшему проверку в соответствии с п. 7.2. Правил, либо последующую проверку по причине его несоответствия требованиям Формы и Формата, а также в иных случаях на усмотрение Банка;

д) «на исполнении»: присваивается ЭД, находящемуся на этапе проверки предусмотренной п. 7.5. Правил;

е) «на обработке»: присваивается ЭД, после успешного прохождения проверки предусмотренной п. 7.5. Правил;

ж) «исполнен»: присваивается ЭД – после исполнения ЭД в соответствии с условиями Базовых договоров. Извещением о подтверждении списания денежных средств с банковского счета Клиента, считается ЭД в статусе «Исполнен».

з) «принято»: присваивается ЭД - после зачисления денежных средств на расчетный счет.

6.12. Информация и ЭД, направленные Банком Клиенту по Системе «iBank 2», признаются полученными Клиентом - в день их передачи по Системе «iBank 2», независимо от фактического их получения либо восприятия Клиентом.

6.13. Информация и ЭД, направленные Клиентом в Банк по Системе «iBank 2» считается направленными непосредственно владельцем ключа ЭП.

6.14. Извещением о подтверждении зачисления денежных средств на банковский счет Клиента считается электронный расчетный документ с отметкой Банка «Принято». Денежные средства, зачисленные на банковский счет Клиента в течение рабочего дня, считаются подтвержденными, если Клиент до 9:00 часов местного времени следующего рабочего дня не известит Банк о несогласии операции, указанной в его выписке.

6.15. При подключении Клиента к Системе «iBank 2» выписки по банковским счетам Клиента и приложения к выпискам Банк предоставляет в электронном виде в порядке и сроки, которые предусмотрены соответствующим договором банковского счета.

7. ПОРЯДОК ПЕРЕДАЧИ КЛИЕНТОМ И ПРИЕМА БАНКОМ ЭД

7.1. Прием ЭД, передаваемых Клиентом посредством Системы «iBank 2», производится Банком в автоматическом режиме ежедневно и круглосуточно. Платежные ЭД поступившие до 15:00 часов московского времени, Банк принимает к исполнению в тот же день в случае, если они получат статус «На исполнении»; документы, поступившие позже указанного времени, а также не имеющие статуса «На исполнении» – на следующий рабочий день. Зачисление денежных средств, поступивших на расчетный счет Клиента, согласно платежных ЭД, производиться Банком на основании реквизитов:

- номер расчетного счета;

- идентификационный номер налогоплательщика (ИНН).

7.2. В момент приема Система «iBank 2» автоматически проверяет в электронном сообщении и прикрепленному к нему ЭД наличие необходимого количества ЭП Клиента и их соответствия имеющимся в Банке Открытым ключам Клиента.

7.3. При положительном результате проверки Система «iBank 2» проставляет в электронном сообщении время поступления и ЭП Банка, свидетельствующую о получении ЭД Банком, сохраняя его в Системе «iBank 2». Данному ЭД присваивается статус «доставлен».

7.4. При отрицательном результате проверки в электронном сообщении ЭП Банка не проставляется и ЭД не сохраняется Системой «iBank 2». Данному ЭД присваивается статус «отвергнут».

7.5. После прохождения первоначальной проверки на корректность, ЭД направляется в соответствующую службу Банка для осуществления проверки соответствия Формы и Формата установленным требованиям. Срок проверки определяется Банком по своему усмотрению, но не может превышать сроки исполнения (приема) ЭД предусмотренные соответствующими Базовыми договорами, во исполнение которых был направлен ЭД либо настоящими Правилами. С момента поступления документа на проверку система присваивает ЭД статус «на исполнении».

7.6. В случае положительного результата проведенной проверки ЭД присваивается статус «на обработке».

7.7. При отрицательном результате проверки ЭД не подлежит дальнейшему исполнению. Данному ЭД Системой «iBank 2» присваивается статус «отвергнут».

7.8. С момента прохождения проверки соответствия Форме и Формату Банк исполняет ЭД в полном соответствии с условиями, предусмотренными соответствующими Базовыми договорами, во исполнение которых был направлен ЭД либо настоящими Правилами. После исполнения (приема) ЭД присваивается статус «исполнен».

7.9. ЭД прошедший проверку ЭП и соответствующий Форме и Формату, определенному для него, признается Сторонами, документом, имеющим равную юридическую силу с надлежащим образом, оформленным документом на бумажном носителе, подписанного собственноручными подписями Уполномоченных лиц и заверенным печатью Клиента.

7.10. Статус каждого ЭД, однозначно отражающий текущий этап его обработки Банком, автоматически отслеживается программными средствами Системы «iBank 2» и сообщается Клиенту во время сеансов связи проводимых им.

7.11. В случае, если Клиент использует Систему «iBank 2» для передачи платежных ЭД, то основанием для отказа Банка от исполнения такого документа служат:

- отрицательный результат проверки ЭП;
- недостаток денежных средств для проведения операций на счете Клиента (за исключением случаев предоставления овердрафта, оговоренных соответствующими договорами);
- несоответствие даты документа требуемой;
- неверно указанные реквизиты;
- несоответствие ЭД требованиям Банка России и Банка

8. ПОРЯДОК ИНФОРМИРОВАНИЯ О СОВЕРШЕННЫХ В СИСТЕМЕ «IBANK 2» ОПЕРАЦИЯХ

8.1. Банк обязуется информировать Клиента о каждой совершенной в Системе «iBank 2» операции не позднее следующего рабочего дня со дня ее совершения следующими способами:

8.1.1. Основной способ - информирование через Систему «iBank 2» (бесплатный способ). Данным способом Банк информирует всех Клиентов путем:

а) направления по Системе «iBank 2» соответствующего уведомления (письма) в котором будут отражены все проведенные по Системе «iBank 2» в течение указанного в уведомлении времени операции;

б) отражения в Системе «iBank 2» статуса ЭД о переводе денежных средств, сформированного в Системе «iBank 2». Изменение статуса ЭД производится по мере приема, проверки и исполнения Банком распоряжения о переводе денежных средств;

в) предоставления Клиенту возможности в любой момент выгрузить из Системы «iBank 2» выписку по банковскому счету в которой будут отражены все совершенные в Системе «iBank 2» операции на дату формирования выписки за выбранный Клиентом период.

При данном способе информирования датой получения Клиентом уведомления Банка о совершенной им в Системе «iBank 2» операции является дата направления Банком по Системе «iBank 2» соответствующего уведомления (письма) и/или дата указания в Системе «iBank 2» статуса ЭД о переводе денежных средств и/или дата размещения в Системе «iBank 2» выписки по банковскому счету.

8.1.2. Дополнительный способ - информирование с помощью услуги «SMS-Банкинг» (платный способ). Данным способом Банк информирует Клиентов, подключившихся к услуге «SMS-Банкинг», путем направления на номер мобильного телефона SMS-сообщения с информацией о каждой совершенной в Системе «iBank 2» операции. Номер мобильного телефона указывается Клиентом в заявлении на подключение к услуге «SMS-Банкинг», направляемом в Банк по форме приложения №4 к Правилам. Подробное описание услуги «SMS-Банкинг» изложено в разделе 11 Правил.

При данном способе информирования датой получения Клиентом уведомления Банка о совершенной Клиентом в Системе «iBank 2» операции является дата направления Банком на указанный Клиентом номер мобильного телефона соответствующего SMS-сообщения.

Клиент самостоятельно определяет необходимость подключения к услуге «SMS-Банкинг».

9. ПОРЯДОК ПЕРЕДАЧИ И ИСПОЛЬЗОВАНИЯ USB-ТОКЕНА

9.1. Применение Системы «iBank 2» подразумевает обязательное использование Клиентом в течение всего периода обслуживания USB-токена, который предназначен для противодействия хищениям Закрытого ключа ЭП вредоносными программами и третьими лицами.

9.2. Закрытый ключ ЭП генерируется только внутри USB-токена, хранится в защищенной памяти USB-токена.

9.3. Формирование ЭП Клиента происходит в соответствии с ГОСТ Р34.10-2001 непосредственно внутри SIM-карты USB-токена: на вход передается ЭД, на выходе - сформированная ЭП под данным документом.

9.4. Доступ ко всем криптографическим функциям USB-токена предоставляется только после ввода пользователем корректного пароля Ключа ЭП, указанного при создании ключа. Для каждого Закрытого ключа ЭП применяется отдельный пароль, определяемый и устанавливаемый Клиентом самостоятельно.

9.5. В одном USB-токене допускается одновременно хранить секретные ключи:

- нескольких Уполномоченных лиц одного корпоративного клиента;

- нескольких корпоративных клиентов.

9.6. USB-токен является собственностью Банка и предоставляется Клиенту во временное пользование на срок действия Договора.

9.7. Банк передает один USB-токен Клиенту в момент заключения Договора по Акту приема-передачи устройства USB-токен «iBank 2 Key» (Приложение №6 к настоящим Правилам), подписанному Сторонами, после оплаты Клиентом соответствующей комиссии согласно Тарифам.

9.8. Клиент в праве по собственной инициативе получить в пользование на срок действия Договора, дополнительные USB-токены, уплатив соответствующую комиссию согласно Тарифам.

9.9. В случае расторжения Договора Клиент обязан возвратить Банку предоставленные USB-токены. Возврат производится в момент расторжения. В случае не возврата, USB-токен считается утраченным Клиентом.

9.10. Клиент возмещает Банку стоимость утраченного или непригодного для использования USB-токена или неочищенного Клиентом от сохранённых на USB-токене ключей ЭП, предоставленного Клиенту, согласно Тарифам на дату возмещения стоимости.

9.11. Клиент не возмещает Банку стоимость непригодного для использования USB-токена, если Клиент докажет, что неработоспособность произошла не по вине Клиента в течение 1 (Одного) месяца (гарантийный срок) с момента передачи USB-токена Клиенту по акту приема-передачи. При этом USB-токен должен быть возвращен Банку не позже 1 (одного) рабочего дня, по истечении указанного в настоящем пункте, месячного срока. В противном случае USB-токен считается утраченным Клиентом.

9.12. Механическое повреждение не является основанием освобождения Клиента от возмещения стоимости USB-токена.

9.13. В случае, предусмотренном п.9.11 Правил, Банк обязуется представить Клиенту в пользование новый USB-токен взамен испорченного.

10. ПОРЯДОК ПЕРЕДАЧИ И ИСПОЛЬЗОВАНИЯ OTP-ТОКЕН, MAC-ТОКЕН

10.1. Применение OTP-токена, MAC-токена в системе «iBank 2» является необходимыми дополнительными мерами защиты Клиента при совершении платежей, а так же для обеспечения информационной безопасности.

10.2. Сервисы OTP-токен, MAC-токен считаются подключенными с момента подписания обеими сторонами Акта приема передачи устройства OTP-токен, MAC-токен по форме Приложения №7 к настоящим Правилам.

10.3. Для работы в системе «iBank 2» Банк передает Клиенту в пользование необходимое количество OTP-токенов, MAC-токенов предназначенных для работы в системе «iBank 2».

10.4. По требованию Клиента Банк предоставляет необходимые рекомендации/консультации для работы с системой «iBank 2», в том числе по сервису OTP-токен, MAC-токен.

10.5. В случае расторжения Договора Клиент обязан возвратить Банку предоставленный OTP-токен. Возврат производится в момент расторжения Договора. В случае порчи или механического повреждения OTP-токен, MAC-токен возвращается в недельный срок со дня свершившегося факта, согласно Акта приема передачи устройства OTP-токен, MAC-токен по форме Приложения №7 к настоящим Правилам. В случае не возврата, OTP-токен, MAC-токен считается утраченным Клиентом.

10.6. Клиент обязан хранить в тайне и не передавать третьим лицам OTP-токен, MAC-токен, используемый в системе «iBank 2».

10.7. Клиент имеет право по собственной инициативе получить в пользование на срок действия Договора дополнительные OTP-токены, MAC-токены, согласно Тарифам, заполнив и представив в Банк Заявление, по форме Приложения №7 к настоящим Правилам.

10.8. Клиент возмещает Банку стоимость нового OTP-токена, MAC-токена, полученного взамен утраченного, поврежденного или испорченного устройства (неработоспособного по вине Клиента), согласно Тарифам на дату возмещения стоимости.

10.9. Не подлежит возмещению стоимость поврежденного или испорченного OTP-токена, MAC-токена, если Клиент докажет, что порча (неработоспособность) или повреждение произошли не по вине Клиента в течение 1 (Одного) месяца с момента передачи устройства Клиенту по Акту приема-передачи. При этом OTP-токен, MAC-токен должен быть возвращен Банку не позже 1

(одного) рабочего дня, по истечении указанного в настоящем пункте, месячного срока. В противном случае OTP-токен, MAC-токен считается утраченным Клиентом.

10.10. За действие третьих лиц по отношению к OTP-токену, MAC-токену Клиент отвечает как за свои собственные. Механическое повреждение не является основанием освобождения Клиента от возмещения стоимости OTP-токена, MAC-токена.

11. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ИСПОЛЬЗОВАНИЯ УСЛУГИ «SMS-БАНКИНГ»

11.1. Услуга «SMS-Банкинг» предоставляется по соответствующему заявлению, заполняемому Клиентом по форме Приложения №4 к настоящим Правилам.

11.2. В соответствии с условиями услуги «SMS-Банкинг» Банк информирует Клиента Системы «iBank 2» о каждом событии (о текущих остатках и о движении средств по счетам Клиента, а так же о иных событиях, оповещение о которых предусмотрено в системе «iBank 2»), посредством составления и передачи Клиенту SMS-сообщений.

11.3. Рассылка указанных оповещений осуществляется по каналу для доставки сообщений уполномоченным лицам Клиента (номер мобильного телефона), регистрируемому Клиентом самостоятельно в интерфейсе системы «iBank 2».

11.4. Банк информирует Клиента об изменениях в настройках услуги «SMS-Банкинг» посредством составления и передачи Клиенту сообщений по каналу для доставки сообщений, определенному Клиентом в интерфейсе системы «iBank 2».

11.5. За предоставление услуги «SMS-Банкинг» взимается комиссия, предусмотренная Тарифами, действующими в момент оказания услуги. Банк на основании соответствующих расчетных документов списывает комиссию за предоставление услуги «SMS-Банкинг», предусмотренную Тарифами Банка с любых расчетных счетов Клиента.

11.6. При подключении к услуге «SMS-Банкинг» Клиент самостоятельно настраивает каналы доставки, типы уведомлений, и условия рассылки SMS-сообщений. При этом Клиент подтверждает и согласен, что используемые для передачи SMS-сообщений коммуникации являются открытыми и не гарантируют полную защиту информации.

11.7. Банк не несет ответственности за не доставленные, либо доставленные не полностью SMS-сообщения Клиенту по причинам, не зависящим от Банка, в том числе в случаях: а) перевыпуска (создание дубликата) SIM-карты Клиента третьими лицами, в том числе без согласия Клиента; б) смены Клиентом номера мобильного телефона без уведомления об этом Банка.

11.8. Клиент несет полную ответственность за обеспечение доступа к мобильному телефону только полномочных лиц Клиента.

11.9. В случае отсутствия денежных средств на расчетном счете Клиента для оплаты комиссии, предусмотренной в п.11.4 Правил, Банк вправе приостановить оказание услуги «SMS-Банкинг».

11.10. В случае утери телефона или SIM-карты, а также наступления других обстоятельств, следствием которых может стать несанкционированный доступ к информации третьих лиц, Клиент обязан сообщить в Банк об указанном факте не позднее 1 (одного) рабочего дня, следующего за днем наступления события. Сообщение должно быть составлено в виде письменного заявления, заполненного в свободной форме. После получения сообщения Банк незамедлительно приостанавливает оказание услуги «SMS-Банкинг».

11.11. Для возобновления услуги «SMS-Банкинг» Клиент направляет в Банк письменное заявление, заполненное в свободной форме. После получения заявления Банком со следующего рабочего дня будет возобновлено оказание услуги «SMS-Банкинг».

11.12. Смена канала для доставки сообщений (номер мобильного телефона) производится Клиентом самостоятельно в интерфейсе системы «iBank 2». Новый канал для доставки сообщений будет действовать не позднее следующего рабочего дня.

11.13. Клиент может отказаться от предоставления Банком услуги «SMS-Банкинг». Для отказа от Услуги Клиент направляет в Банк письменное заявление, заполненное по форме приложения №4 к Правилам. После получения заявления Банком со следующего рабочего дня Банк прекращает оказывать услугу «SMS-Банкинг».

12. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ИСПОЛЬЗОВАНИЯ СЕРВИСА «ДОВЕРЕННЫЕ ПОЛУЧАТЕЛИ»

12.1. В рамках сервиса «Доверенные получатели» Клиент может создавать список контрагентов (доверенных получателей), в пользу которых регулярно совершаются платежи, а также можно задать индивидуальный лимит по сумме платежей для каждого такого доверенного получателя. Платежи, совершаемые в пользу указанных доверенных получателей, и в рамках заданного Клиентом индивидуального лимита, не будут требовать дополнительного подтверждения, а сразу получают статус «доставлен».

12.2. В случае превышения порогового значения заданного Клиентом указанного индивидуального лимита необходимо выполнить процедуру подтверждения платежного поручения путем использования дополнительного кода подтверждения платежа, направленного системой “iBank 2” на номер мобильного телефона, выделенного Клиентом для работы с сервисом «Доверенные получатели» или путем использования иного устройства Клиента, позволяющего получать одноразовый пароль или выполнить процедуру изменения индивидуального лимита для данного получателя на усмотрение Клиента.

12.3. Для работы сервиса «Доверенные получатели» Клиенту необходимо самостоятельно настроить справочник «Доверенные получатели» информацией о контрагенте (доверенном получателе), в пользу которого производится платеж, содержащей:

- наименование получателя платежа (Корреспондент);
- БИК банка получателя платежа (БИК);
- номер счета получателя платежа (Счет);
- лимит платежа, заданный для данного получателя платежа (Лимит), устанавливаемый на усмотрение Клиента.

12.4. Для использования сервиса «Доверенные получатели» Клиенту необходимо представить Банку соответствующее заявление на бумажном носителе за подписью единоличного исполнительного органа Клиента (с приложением печати), в котором будет указано:

- ФИО лица, на которое оформлен сертификат ключа проверки электронной подписи с правом совершения операций в системе “iBank 2”, которое будет уполномочен управлять сервисом «Доверенные получатели»;
- номер мобильного телефона или иное устройство указанного уполномоченного лица, на который будет направляться дополнительный код подтверждения платежа.

12.5. Банк не несет ответственности за не доставленные, либо доставленные не полностью сообщения на номер мобильного телефона или иное устройство уполномоченного лица Клиента по причинам, не зависящим от Банка, в том числе в случаях: а) перевыпуска (создание дубликата) SIM-карты Клиента третьими лицами, в том числе без согласия Клиента; б) смены Клиентом номера мобильного телефона или иного устройства без уведомления об этом Банка.

12.6. Клиент несет полную ответственность за доступ к мобильному телефону или иному устройству не уполномоченных лиц, не отвечающих требованиям пункта 12.4 Правил.

12.7. В случае утери мобильного телефона, иного устройства или SIM-карты, а также наступления других обстоятельств, следствием которых может стать несанкционированный доступ к информации третьих лиц, Клиент обязан незамедлительно приостановить совершение в системе “iBank 2” всех операций по его банковским счетам путем направления в Банк сообщения об указанном(ых) факте(ах). Сообщение должно быть составлено в виде письменного заявления в

свободной форме. После получения указанного сообщения Банк незамедлительно приостанавливает совершение в системе “iBank 2” всех операций по банковским счетам Клиента в рублях.

12.8. Для смены номера мобильного телефона или иного устройства лица, уполномоченного управлять сервисом «Доверенные получатели» и для возобновления Клиентом совершение в системе “iBank 2” операций по банковским счетам в рублях Клиент представляет в Банк письменное заявление, отвечающее требованиям, указанным в пункте 12.4 Правил.

12.9. Клиент может отказаться от использования сервиса «Доверенные получатели». Для отказа от сервиса Клиент направляет в Банк письменное заявление, заполненное по форме Приложения №4 к Правилам. Со следующего рабочего дня после получения указанного заявления Банк прекращает оказание Клиенту сервиса «Доверенные получатели».

13. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ИСПОЛЬЗОВАНИЯ СЕРВИСА «ТИКЕР»

13.1. Сервис «Тикер» предоставляется по соответствующему Заявлению, заполняемому Клиентом по форме Приложения №4 к настоящим Правилам.

13.2. В соответствии с условиями сервиса «Тикер» Банк предоставляет клиенту дополнительный модуль Системы «iBank 2» «Тикер для корпоративных клиентов» на срок действия Договора. В соответствии с условиями сервиса «Тикер» Банк посредством Тикера обязуется оперативно информировать Клиента о движении средств по расчетным счетам Клиента обслуживаемым в системе «iBank2», а также о входящих банковских письмах.

13.3. Банк информирует Клиента об изменениях настроек услуги «Тикер» посредством составления и передачи Клиенту информационного письма рассылаемого в системе «iBank 2».

13.4. За предоставление услуги «Тикер» взимается плата, предусмотренная Тарифами, действующими в момент оказания услуги. Банк на основании соответствующих расчетных документов списывает плату за предоставление услуги «Тикер», предусмотренные Тарифами Банка с любых расчетных счетов Клиента.

13.5. При подключении к услуге «Тикер» Клиент самостоятельно устанавливает и настраивает модуль системы «iBank 2» «Тикер». Банк предоставляет данный модуль посредством размещения соответствующего файла на официальном сайте Банка.

13.6. Банк не несет ответственности в случае неполучения Клиентом информации предусмотренной услугой «Тикер» в связи с техническими проблемами, в том числе по вине лиц, оказывающих услуги интернет связи, а также в иных случаях, произошедших не по вине Банка.

14. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ИСПОЛЬЗОВАНИЯ ДОПОЛНИТЕЛЬНОГО СЕРВИСА «БАНКОВСКИЙ АССИСТЕНТ»

14.1. Дополнительный сервис «Банковский ассистент» предоставляется Клиенту при наличии открытого банковского счета в Банке всем Клиентам, без предоставления отдельного Заявления на его подключение. Подключение к данному сервису происходит при предоставлении Клиентом прав на совместную с Банком работу над ЭД.

14.2. В соответствии с условиями дополнительного сервиса «Банковский ассистент» Банк оказывает Клиенту услугу по согласованию или подготовке ЭД, подтверждающих проведение валютных операций (документы валютного контроля). Наименования ЭД, допустимых к совместной работе в данном сервисе приведено в Перечне ЭД (Приложение №1 к Правилам).

14.3. В рамках дополнительного сервиса «Банковский ассистент» возможны следующие варианты совместной работы Банка и Клиента над документами, с присвоением следующих статусов:

а) «На согласовании»: статус присваивается ЭД, подготовленному Клиентом и отправленному в Банк для внесения последним соответствующих исправлений в ЭД, подтверждающих проведение валютных операций (документы валютного контроля) и

последующего согласования ЭД Клиентом. Совместная работа Банка и Клиента при данном статусе подразумевает:

- самостоятельное создание Клиентом ЭД, подтверждающего проведение валютных операций (валютного контроля) и заполнение значимых полей ЭД;

- передача ЭД в Банк, созданного Клиентом, на корректировку/согласование;

- скорректированный/согласованный Банком ЭД возвращается Клиенту на согласование;

- после согласования Клиентом ЭД оказанная Банком услуга считается исполненной, документ может быть использован Клиентом.

б) «подготовлен банком»: статус присваивается ЭД, подтверждающему проведение валютных операций (документы валютного контроля), подготовленному Банком и отправленному Клиенту для дальнейшего его согласования, оформления и подписания без использования ЭП. Совместная работа Банка и Клиента при данном статусе подразумевает:

- создание Банком ЭД, подтверждающего проведение валютных операций (валютного контроля) и заполнение необходимых полей ЭД и направление его Клиенту для использования в работе;

- при согласовании Клиентом ЭД может быть согласован (подписан) Клиентом или ЭД может быть отредактирован Клиентом и вновь направлен в Банк на согласование;

- после согласования Клиентом ЭД оказанная Банком услуга считается исполненной, документ может быть использован Клиентом.

15. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ИСПОЛЬЗОВАНИЯ СЕРВИСА «МОДУЛЬ IBANK2 ДЛЯ 1С»

15.1. Возможность использования сервиса «Модуль iBank2 для 1С» предоставляется всем Клиентам в рамках выбранного пакета обслуживания ЭДО, согласно Тарифам. Для настройки и установки «Модуля iBank2 для 1С» Клиент самостоятельно скачивает его дистрибутив по соответствующей ссылке, размещенной на http://www.akibank.ru/.

15.2. Необходимыми требованиями для использования сервиса «Модуль iBank2 для 1С» являются:

- наличие зарегистрированного в Банке ключа электронной подписи (ЭП), хранимого в USB-токене;

- обеспечение Клиентом доступа в Internet: модуль взаимодействует с банковским сервером, а также с порталом «iBank2.RU».

15.3. В соответствии с условиями сервиса «Модуль iBank2 для 1С» Банк предоставляет Клиенту возможность напрямую из любой из нижеуказанных конфигураций на платформе «1С:Предприятие 8»:

- создавать, подписывать электронной подписью и отправлять в Банк платежные поручения;

- отслеживать статусы ранее отправленных документов;

- получать из Банка выписки по счетам за произвольный период;

- вести переписку с сотрудниками Банка по защищенному каналу.

15.4. Сервис «Модуль iBank2 для 1С» совместим со следующими конфигурациями на платформе «1С:Предприятие 8»:

- Бухгалтерия предприятия, редакция 3.0;

- Бухгалтерия предприятия, редакция 2.0;

- Управление торговлей, редакция 11.1;

- Управление торговлей, редакция 11.0;

- Управление торговлей, редакция 10.3;
- Комплексная автоматизация, редакция 1.1;
- Управление производственным предприятием, редакция 1.3;
- Управление небольшой фирмой, редакция 1.5;
- 1С:ERP Управление предприятием 2.0.

15.5. Банк не несет ответственности в случае непредставления Клиенту услуг, предусмотренных сервисом «Модуль iBank2 для 1С» в связи с техническими проблемами, в том числе по вине лиц, оказывающих услуги интернет связи, а также в иных случаях, произошедших не по вине Банка.

16. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ИСПОЛЬЗОВАНИЯ СЕРВИСА «ИНДИКАТОР»

16.1. Сервис «Индикатор» позволяет Клиенту в процессе оформления платежных поручений по переводу денежных средств в системе «iBank 2» получать информацию на основе данных из открытых источников федеральных органов власти (ФНС, ФССП, Росреестр, Генпрокуратура и др.) о фактах деятельности юридических лиц и индивидуальных предпринимателей.

16.2. Сервис «Индикатор» предоставляется в 2-х режимах:

- в режиме ограниченной версии сервиса – предоставление информации о контрагенте в виде цветных индикаторов, зависящихся от категории выявленных фактов:

(Красный)
Негативные факты. Свидетельствуют о том, что контрагент уже прекратил деятельность, либо может ее прекратить. Например, находится в состоянии банкротства.

(Желтый)
Подозрительные факты. Свидетельствуют о действиях контрагента, которые могут служить признаками нарушения его нормальной деятельности. Например, недавняя смена руководителя или наличие исполнительных производств по заработной плате.

(Зеленый)
Позитивные факты. Свидетельствуют о наличии нормальной деловой активности в организации за последнее время. Например, контрагент за прошлый год получал лицензии на некоторые виды деятельности.

(Синий)
Достижения. Свидетельствуют о значительных успехах в деятельности контрагента. Например, о значительной сумме выполненных государственных контрактов.

- в полной версии сервиса – предоставление информации о контрагенте с возможностью детализации результатов проверки контрагента в виде экспресс-отчета.

16.3. Сервис «Индикатор» предоставляется по соответствующему Заявлению, заполняемому Клиентом по форме Приложения №4 к настоящим Правилам.

16.4. За предоставление сервиса «Индикатор» взимается плата, согласно Тарифам.

16.5. Банк не несет ответственности за полноту и достоверность открытой информации, содержащейся в общедоступных источниках, доступ к которой будет получен Клиентом с использованием Сервиса «Индикатор».

16.6. Банк не несет ответственности за ущерб и/или упущенную выгоду, возникшие у Клиента в результате использования Сервиса «Индикатор».

17. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ИСПОЛЬЗОВАНИЯ СЕРВИСА «МОБИЛЬНЫЙ БАНК»

17.1. Сервис «Мобильный-банк» предоставляется Клиенту при наличии действующего ЭДО в рамках Системы «iBank 2» путем предоставления доступа к Приложению «АКИБАНК Бизнес» Уполномоченным лицам Клиента.

17.2. В пределах функциональных и технических возможностей в Приложении «АКИБАНК Бизнес» доступны следующие варианты его использования:

- «Информационный режим» – доступен только просмотр ЭД;
- «Полнофункциональный режим» – доступно создание ключей ЭП, создание ЭД и их подписание, подтверждение ЭД с использованием одноразового пароля, полученного в SMS или в Push-уведомлении (при наличии технической возможности).

17.3. Подключение Сервиса «Мобильный-банк» («Информационный режим») и настройка прав доступа Уполномоченных лиц выполняется Клиентом самостоятельно. В разделе «Управление услугами» в Системе «iBank 2», Клиент выбирает Сервис «Мобильный банк» и нажимает кнопку «Подключить», что подтверждает ознакомление Клиента с порядком предоставления и использования Сервиса «Мобильный банк».

Для работы Приложения «АКИБАНК Бизнес» в «Полнофункциональном режиме» Клиенту необходимо завершить подключение к «Информационному режиму», а также Управляющий Сервисом «Мобильный банк» определяет сотрудников Клиента, которым будет предоставлен доступ к Сервису «Мобильный банк» и их номера мобильных телефонов (заполняется соответствующий раздел Заявления по форме Приложения №4 к настоящим Правилам), а также необходим выпуск сертификата ключа проверки ЭП на указанных сотрудников (в Приложении «АКИБАНК Бизнес» формируется ЭД «Заявление на выпуск сертификата ключа проверки ЭП»).

17.4. Управляющий Сервисом «Мобильный банк» после указанных выше настроек уведомляет сотрудников, которым предоставлен доступ, о необходимости установки Приложения «АКИБАНК Бизнес» на их Мобильные устройства.

17.5. Сотрудник, которому предоставлен доступ к Сервису «Мобильный банк», совершает действия:

- получает через магазины приложений Google Play или AppStore Приложение «АКИБАНК Бизнес» и устанавливает его на свое Мобильное устройство;
- проходит идентификацию по номеру своего мобильного телефона;
- создает свой код доступа к Приложению «АКИБАНК Бизнес», который хранит в тайне от третьих лиц (восстановление кода доступа к Приложению «АКИБАНК Бизнес» инициируется Клиентом самостоятельно через процедуру «Сброса кода доступа» в самом Приложении «АКИБАНК Бизнес» и создания нового кода доступа).

После успешного завершения указанных процедур сотрудник Клиента может работать в Приложении «АКИБАНК Бизнес» в «Информационном режиме».

17.6. Изменение перечня сотрудников, которым предоставлен доступ к Сервису «Мобильный банк», их номеров мобильных телефонов производится Управляющим Сервисом «Мобильный банк» в разделе «Управление услугами» в Системе «iBank 2»:

- для изменения перечня сотрудников, которым предоставлен доступ к Сервису «Мобильный банк», Управляющий Сервисом «Мобильный банк» удаляет сотрудника и, при необходимости, создает нового сотрудника;
- для изменения номера мобильного телефона сотрудника, которому предоставлен доступ к Сервису «Мобильный банк», Управляющий Сервисом «Мобильный банк» удаляет сотрудника и создает нового с новым номером телефона.
- для отключения Сервиса «Мобильный банк» Управляющий Сервисом «Мобильный банк» нажимает кнопку «Отключить».

17.7. Управляющий Сервисом «Мобильный банк» для работы в «Полнофункциональном режиме» заполняет соответствующий раздел Заявления по форме Приложения №4 к настоящим Правилам и направляет его в Банк. «Полнофункциональный режим» предназначен для работы только сотрудникам Клиента, имеющих действующий Ключ ЭП для стационарной версии Системы «iBank 2» с правом подписи платежных документов.

17.8. Банк, при получении от Клиента Заявления по форме Приложения №4 к настоящим Правилам, соответствия всех указанных данных и подписания его уполномоченным лицом Клиента, Банк подключает «Полнофункциональный режим».

17.9. Каждый сотрудник Клиента, который был допущен к работе с сервисом «Мобильный-банк» в «Полнофункциональном режиме», посредством Приложения «АКИБАНК Бизнес» создает

на себя Ключ серверной подписи и соответствующий ему Ключ проверки серверной подписи, задает пароль на доступ к Ключу серверной подписи. Затем, вместе с указанными документами, сформированными сотрудником Клиента, Управляющим Сервисом «Мобильный-банк» в Приложении «АКИБАНК Бизнес» подписывается ЭД «Заявление на выпуск сертификата ключа проверки ЭП», которое направляется в Банк через Систему «iBank 2».

В случае, если Управляющий Сервисом «Мобильный-банк» желает произвести замену ранее выпущенного сертификата ключа проверки ЭП путем выпуска нового сертификата ключа проверки ЭП, то в разделе «Комментарии» в указанном заявлении указывается о реквизитах прежнего сертификата ключа проверки ЭП, замену которого следует произвести.

17.10. Банк при получении ЭД «Заявление на выпуск сертификата ключа проверки ЭП» совершает одно из нижеуказанных действий:

- выпускает сотруднику Клиента Сертификат ключа проверки серверной подписи, если сотрудник Клиента, для которого выпускается соответствующий сертификат, имеет право подписи платежных документов. Выпуск Сертификата ключа проверки серверной подписи осуществляется при исполнении ЭД «Заявление на выпуск сертификата ключа проверки ЭП» и активации данного ключа администратором Системы «iBank2»;

- отказывает Клиенту в выпуске для сотрудника Клиента Сертификата ключа проверки серверной подписи. В данном случае сотрудник Клиента может работать в «Информационном режиме».

17.11. Клиент по своему усмотрению может изменить Управляющего Сервисом «Мобильный-банк» при одновременном выполнении условий:

- у сотрудника Клиента имеется действующий Ключ ЭП для стационарной версии Системы «iBank 2» с правом подписи платежных документов;

- Клиент назначил Управляющего Сервисом «Мобильный-банк» и определил его в соответствующем Заявлении по форме Приложения №4 к настоящим Правилам.

17.12. Блокировка Ключей серверной подписи осуществляется аналогично блокировки Ключей ЭП, изложенной в разделе 4 Правил.

Блокировка Ключей серверной подписи также возможна при смене изменении списка сотрудников Клиента, которым предоставлен доступ к Сервису «Мобильный банк» (необходимо заполнение соответствующего раздела Заявления по форме Приложения №4 к настоящим Правилам), а также необходим выпуск сертификата ключа проверки ЭП на новых сотрудников (в Приложении «АКИБАНК Бизнес» формируется ЭД «Заявление на выпуск сертификата ключа проверки ЭП»).

Клиент обязан уведомлять Банк о смене лиц, уполномоченных работать с Системой «iBank2». Для возобновления работы в «Полнофункциональном режиме» Клиенту необходимо создать новые Ключи серверной подписи и новые сертификаты ключа проверки серверной подписи.

17.13. Дополнительная информация по подключению, настройке и использованию приложения «АКИБАНК Бизнес» и безопасной работы содержатся в «Руководстве пользователя», размещенного по соответствующей ссылке, размещенной на http://www.akibank.ru/, а так же в разделе 21 Правил.

17.14. Каждый сотрудник Клиента обязан хранить в тайне пароль для доступа к своему Приложению «АКИБАНК Бизнес» и свои пароли для доступа к Ключам серверной подписи.

Клиент обязан хранить в тайне аутентификационную информацию и обеспечить сохранность Мобильного устройства и SIM-карты, с помощью которых осуществляется доступ к Приложению «АКИБАНК Бизнес». Клиент обязуется принимать все возможные меры для предотвращения компрометации (несанкционированного использования) Мобильного устройства и SIM-карты.

В случае утери мобильного телефона, иного устройства или SIM-карты, а также наступления других обстоятельств, следствием которых может стать несанкционированный доступ к информации третьих лиц, Клиент обязан незамедлительно приостановить совершение в системе “iBank 2” всех операций по его банковским счетам путем направления в Банк сообщения об указанном(ых) факте(ах). Сообщение должно быть составлено в виде письменного заявления в свободной форме. После получения указанного сообщения Банк незамедлительно

приостанавливает совершение в системе “iBank 2” всех операций по банковским счетам Клиента в рублях.

17.15. За предоставление доступа к Сервису «Мобильный банк» в «Полнофункциональном режиме» взимается плата, согласно Тарифам».

18. КОНФИДЕНЦИАЛЬНОСТЬ

18.1. Банк принимает меры для предотвращения несанкционированного доступа третьих лиц к информации, составляющей банковскую тайну Клиента. Любая информация такого рода может быть предоставлена третьим лицам не иначе как в порядке, установленном законодательством Российской Федерации.

18.2. Клиент поставлен в известность и в полной мере осознает, что передача конфиденциальной информации по каналу доступа влечет риск несанкционированного доступа к такой информации третьих лиц.

18.3. Защита информации в Системе «iBank 2» является многоуровневой и задействует возможности всех компонентов Системы «iBank 2»:

- операционной системы;
- прикладного программного обеспечения;
- специализированных программных и технических средств;
- организационных мер (наличие соответствующих администраторов);
- организации хранения ПО, используемых в работе Системы «iBank 2», как на стороне Клиента, так и на стороне Банка.

18.4. Система «iBank 2» комплексной защиты информации, состоящая из набора аппаратно-программных средств и административных мер, обеспечивает:

- создание ключей шифрования и ЭП в USB-токенах;
- защиту от компрометации секретного ключа ЭП вредоносными программами;
- ЭП под документами;
- шифрование передаваемой информации;
- аутентификацию Клиентов и разграничение их прав;
- достоверность факта получения документа получателем;
- подтверждение авторства и целостность электронных документов;
- выявление ошибок, сбоев и несанкционированных действий обслуживающего персонала;
- разбор конфликтных ситуаций.

18.5. Для разрешения возможных споров в Банке ведутся контрольные архивы ЭД подписанных ЭП, а также архивы открытых ключей ЭП. Хранение контрольных архивов ЭД осуществляется в течение трех лет с момента проведения операции.

18.6. При проверке подписи под документом используется соответствующий ключ подписи абонента, подписавшего электронный документ.

19. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

19.1. Стороны в рабочем порядке урегулируют все споры, возникающие между ними в ходе работы в Системе «iBank 2», за исключением споров, указанных в п. 19.2. Правил.

19.2. Споры Сторон по поводу авторства, неизменности и содержания ЭД рассматриваются согласительной комиссией, формируемой сторонами (далее по тексту – «Комиссия»). Процедура рассмотрения спора состоит из следующих этапов:

а) Предъявление претензии одной из Сторон другой Стороне;

б) Формирование Комиссии для рассмотрения спора;

в) Разрешение Комиссией спора по существу.

19.3. Претензия предъявляется соответствующей Стороной в письменной форме путем официального вручения под расписку другой Стороне или направления по почте другой Стороне заказным письмом с уведомлением о вручении.

19.4. Получив претензию, соответствующая Сторона официально в письменной форме информирует другую Сторону о результатах ее рассмотрения в течение 5 (Пяти) рабочих дней с даты получения претензии.

19.5. Сторона, предъявившая претензию, в течение 5 (Пяти) рабочих дней после получения результатов рассмотрения претензии от другой Стороны должна рассмотреть представленные объяснения и письменно уведомить другую Сторону о снятии претензии или о несогласии с представленными объяснениями.

19.6. Если Сторона не согласна с представленными объяснениями, Стороны обязаны в течение 5 (Пяти) рабочих дней с даты уведомления о несогласии сформировать Комиссию для рассмотрения и разрешения указанного спора по существу.

19.7. До передачи спора на рассмотрение Комиссии Сторонам следует удостовериться, что причиной возникновения спора не является нарушение целостности программного обеспечения, произошедшее в результате сбоев аппаратуры, воздействия компьютерных вирусов, в том числе полученных через Интернет, и т.п. В этом случае Стороны руководствуются п.19.1 Правил.

19.8. В состав Комиссии включается равное количество представителей Банка и Клиента. При необходимости в состав Комиссии могут быть включены независимые эксперты, в частности, представители компании - разработчика Системы «iBank 2». Максимальное количество членов Комиссии не должно превышать 6 (Шести) человек.

19.9. Полномочия представителей Сторон для участия в Комиссии должны подтверждаться оформленными надлежащим образом доверенностями.

19.10. Заседание Комиссии проводится не позднее 2 (Двух) рабочих дней со дня ее формирования.

19.11. При рассмотрении спора об авторстве и неизменности содержания ЭД Комиссия устанавливает следующие факты:

а) предмет спора Сторон;

б) перечень ЭД, относящихся к предмету спора;

в) идентичность созданного одной из Сторон ЭД документу на бумажном носителе, распечатанному Банком и хранимому в Банке;

г) принадлежность ЭП ЭД одной из Сторон.

19.12. При рассмотрении спора Комиссия использует следующие данные в качестве эталонных:

а) Данные имеющегося в Банке архива отправленных/принятых ЭД;

б) Сертификаты открытых ключей ЭП Уполномоченных лиц Сторон, хранящиеся в Банке (Эталонные сертификаты).

19.13. Разрешение споров осуществляется на основании результатов проверки ЭП Сторон в спорном ЭД.

19.14. Комиссия осуществляет свою работу на территории Банка с использованием персонального компьютера, свободного от вирусов и программных закладок, с установленными на нем эталонными DLL-библиотеками ключей ЭП, предоставляемыми компанией - разработчика Системы «iBank 2».

19.15. Для рассмотрения спора Комиссией администратор Банка предоставляет Эталонный(е) сертификат(ы).

19.16. Клиент для рассмотрения спора Комиссией предоставляет оригиналы Сертификатов открытого ключа ЭП Клиента, хранящихся у Клиента.

19.17. Если инициатором рассмотрения спора является Клиент, Комиссией устанавливается актуальность Открытых ключей ЭП Клиента на момент передачи ЭД, являющегося объектом спора. Открытые ключи ЭП Клиента считаются актуальными, если они были зарегистрированы в Каталоге открытых ключей и действовали в момент, когда спорный ЭД был передан Клиентом в Банк.

19.18. Принимая во внимание математические свойства алгоритма ЭП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94, гарантирующими невозможность подделки значения сертифицированной ЭП любым лицом, не обладающим Закрытым ключом ЭП, Стороны признают, что рассмотрение спора в отношении авторства и неизменности содержания ЭД заключается в доказательстве принадлежности ЭП конкретного ЭД конкретной Стороне.

19.19. Рассмотрение Комиссией спора об авторстве и неизменности содержания ЭД проводится с использованием АРМ «Операционист» Системы «iBank 2».

19.20. В целях формирования протокола проверки ЭП администратор Банка в присутствии Комиссии осуществляет следующие действия:

а) выводит на печать Сертификат открытого ключа ЭП из Каталога открытых ключей используя АРМ «Администратор» Системы «iBank 2»;

б) сравнивает распечатанный Сертификат открытого ключа ЭП Клиента из Каталога открытых ключей с Эталонным сертификатом, предоставленным Комиссии администратором Банка, а также с аналогичным сертификатом, хранящимся у Клиента и представленным Комиссии Клиентом. В случае проверки ЭП Уполномоченного лица Банка, сравнению подлежат только Сертификат открытого ключа ЭП из Каталога открытых ключей и Эталонный сертификат. Значения открытого ключа ЭП Клиента, содержащиеся в Каталоге открытых ключей, в Эталонном сертификате и в хранящемся у Клиента сертификате, должны совпасть. В случае их несовпадения верным признается Эталонный сертификат;

в) с помощью АРМ «Операционист» находит спорный документ и, используя меню «Проверить ЭП», формирует результат проверки ЭП, в котором указываются идентификаторы Ключей ЭП, участвовавшие в подписи документа, авторство которого оспаривается;

г) выводит на печать документ со списком идентификаторов подписавших его Ключей ЭП.

В случае, если спорный ЭД был подписан несколькими ЭП, данная процедура повторяется применительно к каждой ЭП.

19.21. Принадлежность ЭП Стороне и авторство ЭД считается установленным, если идентификаторы Открытых ключей ЭП, содержащихся в списке идентификаторов, подписавших документ, и Эталонном сертификате совпадают, в документе сформирована запись «ЭП Корректна», и распечатанный сертификат открытого ключа ЭП из Каталога открытых ключей совпадает с Эталонным сертификатом.

19.22. Заключение Комиссии оформляется письменно в двух экземплярах – по одному для каждой из Сторон - и подписывается всеми членами Комиссии в день составления указанного заключения.

19.23. Заключение Комиссии является окончательным, пересмотру во внесудебном порядке не подлежит и является обязательным для участвующих в рассмотрении спора Сторон.

19.24. Если Стороны не могут урегулировать спор в рабочем порядке, не согласны с заключением Комиссии, или если одна из Сторон уклоняется от создания Комиссии в случаях, когда в соответствии с Правилами Комиссия должна быть создана либо одна из Сторон уклоняется от подписания заключения Комиссии в день ее проведения, возникший спор передается в Арбитражный суд по месту нахождения Банка. В случаях, если Клиент обслуживается в филиале Банка, споры рассматриваются Арбитражным судом по месту нахождения филиала Банка.

20. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И/ИЛИ ДОПОЛНЕНИЙ В ПРАВИЛА И ИХ РАЗМЕЩЕНИЕ

20.1. Банк информирует Клиента об изменениях и/или дополнениях, вносимых им в Правила (включая Тарифы), в том числе об утверждении Банком новой редакции Правил, за 10 (Десять) календарных дней до вступления их в силу одним из следующих способов:

а) информационным сообщением, направляемым Клиентам по Системе “iBank 2”;

б) путем размещения информации на официальном web-сайте Банка;

в) путем размещения информации в операционном зале Банка в доступном для Клиента месте.

20.1.1. При этом, в случае, если указанные изменения и/или дополнения в Правила (включая Тарифы) произведены в связи с изменением законодательства либо в связи с внедрением в Банке нового продукта (услуги, сервиса либо при обновлении перечня пересылаемых ЭД или при утверждении сделок, ЭДО по которым предусмотрен Базовыми договорами), то такие изменения и/или дополнения в Правила (включая Тарифы) становятся обязательными для сторон ЭДО с даты введения в действие изменений законодательства и размещения Банком измененной редакции Правил предусмотренными способами либо с даты внедрения в Банке нового продукта (услуги, сервиса либо при обновлении перечня пересылаемых ЭД или при утверждении сделок, ЭДО по которым предусмотрен Базовыми договорами) и размещения Банком измененной редакции Правил предусмотренными способами соответственно.

20.2. Любые изменения и/или дополнения в Правила (включая Тарифы), в том числе утвержденная Банком новая редакция Правил, с момента вступления их в силу равно распространяется на всех Клиентов заключивших Договор и присоединившимся к Правилам. В случае несогласия Клиента с изменениями и/или дополнениями, внесенными Банком в Правила (включая Тарифы), в том числе с утвержденными Банком новой редакции Правил Клиент имеет право расторгнуть Договор в порядке, предусмотренном п. 6.2. Договора.

20.3. Моментом публикации, а также моментом ознакомления Клиента с опубликованной информацией считается момент их первого размещения одним из способов, предусмотренных п.20.1. Правил.

20.4. Банк не несет ответственности, если информация об изменении и/или дополнении Правил (включая Тарифов), в том числе об утверждении Банком новой редакции Правил, опубликованная в порядке и в сроки, установленные Правилами, не была своевременно изучена и/или верно истолкована Клиентом.

21. РЕКОМЕНДАЦИИ КЛИЕНТУ ПО ПРЕДУПРЕЖДЕНИЮ ХИЩЕНИЙ ДЕНЕЖНЫХ СРЕДСТВ СО СЧЕТА КЛИЕНТА, В РЕЗУЛЬТАТЕ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО УДАЛЕННОГО ДОСТУПА К ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ ЛИЦАМИ, НЕ ОБЛАДАЮЩИМИ ПРАВОМ РАСПОРЯЖЕНИЯ ЭТИМИ ДЕНЕЖНЫМИ СРЕДСТВАМИ

21.1. Необходимо обеспечить физическую безопасность носителя закрытого ключа ЭП и компьютера, с которого осуществляется работа в системе ЭДО.

а) В качестве носителя закрытого ключа ЭП необходимо использовать персональный аппаратный криптопровайдер (USB-токен) с неизвлекаемыми ключами.

б) Исключить копирование данных электронного ключа на жесткий диск компьютера, с которого осуществляется работа в системе ЭДО.

в) Размещение, специальное оборудование и охрана помещения, в котором установлен компьютер для взаимодействия с системой ЭДО, должны обеспечивать невозможность неконтролируемого проникновения в эти помещения посторонних лиц.

г) Доступ неуполномоченных лиц к носителю закрытого ключа ЭП должен быть исключен.

д) По окончании рабочего дня, а также вне времени взаимодействия с системой ЭДО носитель закрытого ключа ЭП должен быть отсоединен от компьютера и помещен в сейф.

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

21.2. Обеспечить целостность программного обеспечения компьютера, с которого осуществляется работа в системе ЭДО.

а) Для работы в системе ЭДО необходимо использовать специально выделенный компьютер. Хорошей практикой является применение ноутбука, используемого только для окончательного подписания электронного документа. Все остальное время такой ноутбук должен быть выключен и находится в недосягаемом для посторонних лиц месте (сейф, шкаф запираемый на ключ).

б) На компьютере рекомендуется использовать только лицензионное программное обеспечение, регулярно устанавливать рекомендуемые производителями обновления, как операционной системы, так и прикладного программного обеспечения, в том числе браузера, это позволит вовремя устранить выявленные уязвимости.

в) На компьютер, с которого осуществляется работа в системе ЭДО необходимо устанавливать лицензионное антивирусное программное обеспечение. Постоянно следить за наличием актуальных обновлений и своевременно устанавливать их.

г) Работать на компьютере только с правами обычного непривилегированного пользователя (не администратора). Используя для работы учетную запись администратора Вы существенно увеличиваете риск заражения вредоносными программами.

д) В обязательном порядке, в операционной системе следует отключать «Автозапуск программ на съемных носителях (флешках)».

е) Не устанавливать на компьютер программы удаленного администрирования.

21.3. Обеспечить безопасность сетевого соединения с системой ЭДО.

а) Сеть Интернет на компьютере, с которого осуществляется доступ в систему ЭДО, использовать исключительно для работы в системе ЭДО. Доступ к социальным сетям, развлекательным и иным ресурсам сети Интернет на таком компьютере должен быть исключен.

б) Рекомендуется использовать на компьютере Клиента персональный межсетевой экран для входа в Интернет. Это позволит значительно снизить риск удаленного управления злоумышленниками из Интернет и локальной сети вашим компьютером и нарушения целостности ЭД. Дополнительно можно настроить брандмауэр на доступ только по адресам системы ЭДО (https://ibank.akibank.ru).

в) В целях контроля соединения при работе с системой ЭДО необходимо использовать только защищенное соединение по протоколу https. Соединение должно быть установлено с официальным сайтом услуги - https://ibank.akibank.ru. Настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка, www.akibank.ru) или поступивших по электронной почте писем.

21.4. Необходимо использовать дополнительные меры противодействия мошенничеству.

а) В качестве меры оперативного оповещения о входе в систему, текущих остатках, принятых и отвергнутых документах, движении средств по счетам, выписки по расписанию используйте рассылки SMS-сообщений.

б) В качестве меры альтернативного канала оповещения рекомендуется использовать программный модуль «Тикер». При этом, модуль «Тикер» необходимо установить на дополнительный компьютер.

в) В качестве защиты платежных документов от подмены рекомендовано применять автономное аппаратное средство «MAC-токен».

г) Для контроля списка контрагентов, необходимо использовать сервис «Доверенные получатели».

д) Не привлекать для администрирования и обслуживания с которого осуществляется взаимодействие с системой ЭДО технических специалистов на условиях предоставления им удаленного доступа к компьютеру.

е) Регулярно контролировать состояние своих счетов и незамедлительно сообщать сотрудникам Банка обо всех подозрительных или несанкционированных операциях.

ж) Не рекомендуется осуществлять платежи за час до окончания операционного времени в пятницу и в предпраздничные дни.

з) Если возникли подозрения в некорректной работе системы ЭДО (компьютер работает медленно, сообщение системы ЭДО о неверно введенном пароле, самопроизвольная перезагрузка компьютера), незамедлительно извлеките ключ электронной подписи, выключите компьютер и свяжитесь со службой круглосуточной технической поддержки по единому номеру телефона: **8 800 100 2542** (звонок по РФ бесплатен).

21.5. Банк не несет ответственность за ущерб, вызванный несанкционированным списанием денежных средств с его банковского счета при несоблюдении указанных рекомендаций и настоящих Правил

21.6. Рекомендации Клиенту о действиях в случае попытки или несанкционированного списания денежных средств с его расчетного счета и рекомендуемые формы документов приведены в Приложении №9 к Правилам.