УТВЕРЖДЕНЫ
Приказом Первого заместителя
Председателя Правления
АКБ «Алмазэргиэнбанк» АО
В.А. Великих от 28.08.2018
№599

Дата ввода в действие:
«03» сентября 2018г.

Раздел 10 Правил банковского обслуживания корпоративных клиентов в АКБ «Алмазэргиэнбанк» АО

УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ «АЭБ БИЗНЕС»

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

IMSI (InternationalMobileSubscriberIdentity) – международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи GSM, UMTS или CDMA. При регистрации в сети аппарат абонента передает IMSI, по которому происходит его идентификация.

Администратор информационной безопасности – работник Банка, к должностнымобязанностям которого относится рассмотрение и обработка запросов на выдачу,аннулирование, приостановление и возобновление действия ЭП.

Администратор системы Банка – работник Банка, осуществляющий администрирование подсистем ДБО.

Договор - Договор об использовании системы дистанционного банковского обслуживания «АЭБ-Бизнес» между Банком и Клиентом, состоящий из настоящих Условий;

Защита информации – комплекс мероприятий, реализуемых с цельюпредотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения,модификации (подделки), несанкционированного копирования, нарушения доступностиинформации и обеспечения невозможности отказа от совершенных действий.

Заявление - заявление о присоединении к Условиямоб использовании системы дистанционного банковского обслуживания «АЭБ-Бизнес» (Приложение № 1 к настоящим Условиям).

Информационная безопасность – состояниеинформации, информационных ресурсов и информационных систем, при которых с требуемойвероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты,несанкционированного уничтожения, искажения, модификации (подделки), копирования,нарушения доступности, а также обеспечиваются условия невозможности отказа от совершенных действий.

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП (далее – проверка ЭП).

Ключ ЭП - уникальная последовательность символов, предназначенная для создания ЭП.

Ключевая пара – ключ ЭП и соответствующий ему ключ проверки ЭП.

Логин – уникальное имя Клиента в системе дистанционного банковского обслуживания «АЭБ-Бизнес». Логин Клиента в сочетании с паролем обеспечивает однозначнуюаутентификацию Клиента.

Ответственный сотрудник Клиента – представитель Клиента, обязанности которого связаны с контролем за обеспечением конфиденциальности ключей ЭП, а также подачей Запросов на аннулирование/приостановление действия СКП ЭП Уполномоченных лиц Клиента в случае увольнения/смены указанных Уполномоченных лиц.

Пароль – последовательность символов, вводимых с клавиатуры компьютера(или без использования клавиатуры за счет средств автоматизации, имитирующихклавиатурный ввод) в целях аутентификации Клиента.

ПЭП(простая электронная подпись) - значение хэш-функции, вычисленное по всем реквизитам электронного документа (номер лицевого счета, номер телефона, номер обязательства и т.д.), идентификатору Клиента, под которым Клиент был аутентифицирован Системой, и одноразовому паролю, передаваемому Клиенту посредством SMS-сообщений иподтверждающему реквизиты получателя средств и/или реквизиты плательщика, если он использовался при совершении операции.

Сертификат ключа проверки ЭП (СКП ЭП) – ЭД или документ на бумажномносителе, выданный УЦ АКБ Алмазэргиэнбанк АО Субъектам информационного обмена и подтверждающийпринадлежность ключа проверки ЭП владельцу СКП ЭП.

УНЭП(усиленная неквалифицированная электронная подпись) - электронная подпись, которая соответствует следующим признакам:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее ЭД;

3) позволяет обнаружить факт внесения изменений в ЭД после момента его подписания;

4) создается с использованием средств электронной подписи.

Уполномоченное лицо Клиента- индивидуальный предприниматель/физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой (адвокат, учредивший адвокатский кабинет, арбитражный управляющий, нотариус), руководитель, главный бухгалтер или физическое лицо, уполномоченное распоряжаться расчетным счетом Клиента на основании доверенности или распорядительного акта Клиента и включенное в Карточку с образцами подписей и оттиска печати, и одновременно уполномоченные на использование аналога собственноручной подписи (в соответствии с требованиями Инструкции Банка России от 30.05.2014 года № 153- И «Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам), депозитных счетов»);

ЭД (электронный документ) – информация, представленная в электроннойформе и подписанная ЭП.

Электронный ключ - программно-аппаратное устройство, используемое в Системе для генерации ключей ЭП, ключей шифрования, формирования и проверки УНЭП. «Электронный ключ» реализует алгоритмы шифрования и электронной подписи, соответствующие требованиями нормативно-правовых актов Российской Федерации в области криптографии.

ЭП (электронная подпись) –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. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Условия об использовании системы дистанционного банковского обслуживания «АЭБ-Бизнес» (далее – «Условия») устанавливают порядок обслуживания Клиента с использованием системы дистанционного банковского обслуживания «АЭБ-Бизнес» (далее – «Система»), позволяющей обеспечить проведение расчетных операций с использованием электронных платежных документов, а также обмен служебно-информационными электронными документами между Банком и Клиентом.

1.2. Обслуживание Банком Клиента осуществляется в соответствии с настоящими Условиями и действующими Тарифами, на основании Заявления о присоединении к Условиям.

1.3. Заключение Договора между Банком и Клиентом осуществляется путем присоединения Клиента к настоящим Условиям в соответствии со статьей 428 Гражданского кодекса РФ и производится путем передачи Клиентом или его уполномоченным представителем в Банк Заявления о присоединении к Условиям.

1.4. ЗаключениеДоговора может осуществляться Клиентами, не находящимися на расчетно-кассовом обслуживании в Банке.

1.5. Клиенты, желающие заключить договор с использованием дистанционного банковского обслуживания «АЭБ-Бизнес» и не имеющие действующих Расчетных счетов, открытых в Банке, для заключения Договора одновременно с предоставлением в Банк подписанного Заявления настоящих Условий, предоставляют в Банк в полном объеме документы согласно приложению № 1 к «Правилам банковского обслуживания корпоративных клиентов в АКБ «Алмазэргиэнбанк» АО» (далее – Перечень).

1.6. Для обеспечения конфиденциальности пересылаемой коммерческой информации используются два варианта защиты электронной подписи: sms-пароли (ПЭП) и электронный ключ (УНЭП), гарантирующие достоверность передаваемой информации и не позволяющие третьим лицам вмешиваться во взаимные расчеты.

1.7. Стороны обязуются обеспечить допуск к работе в Системетолько уполномоченным лицам Клиента в соответствии с Заявлением о присоединении к Условиям.

1.8. Банк до приема на обслуживания обязан проводить идентификацию Клиентов, представителей Клиентов, выгодоприобретателей, бенефициарных владельцев в соответствии с требованиями Федерального закона №115-ФЗ, Положения Банка России №499-П, ПВК №1124-ПВ, с занесением сведений Клиента в АБС.

1.9. Настоящие Условия устанавливают случаи признания ЭД равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». ЭД признается равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случае если соблюдены следующие условия:

- ЭД передан одной Стороной другой Стороне с использованием программного обеспечения Системы;
- для ЭД пройдена проверка ЭП в соответствии с настоящими Условиями с использованием средств криптографической защиты информации;
- для ЭД, переданных Клиентом в Банк, пройдена проверка в соответствии со всеми процедурами защиты информации.

1.10. Исполнение ЭД Клиента, производится Банком не позднее рабочего дня, следующего за днем подачи Клиентом электронного документа, при условии корректности электронной подписи (далее - «ЭП») Клиента в ЭД, если иные сроки не установлены Договором, законодательством РФ, либо не вытекают из содержания ЭД.

1.11. Плата за услуги Банка в соответствии с действующими Тарифами списывается Банком со счета Клиента, указанного в Заявлении о присоединении к Условиям.

1.12. Стороны признают используемые в Системе средства криптографической защиты информации и используемые Банком и КлиентомПЭП/УНЭП достаточными для защиты ЭД от несанкционированного доступа, а также подтверждения их авторства и подлинности.

1.13. Полномочия Клиента, а также его уполномоченных лиц на совершение операций с использованием средств криптографической защиты информации являются для Банка действующими до истечения срока их действия или предоставления Клиентом документов, свидетельствующих об их прекращении, или до получения от Клиента извещения о совершении операций с использованием Системы без согласия Клиента.

1.14. Клиентская часть Системы, состоящая из Программного обеспечения, указанного в п. 3 настоящих Условий, устанавливается на персональном компьютере Клиента, оснащенном в соответствии с п. 3.3.2. настоящих Условий, и обеспечивает обмен ЭД согласно п. 2 настоящих Условий.

2. ЭЛЕКТРОННЫЙ ДОКУМЕНТ

2.1. Виды электронных документов, направляемых Клиентом Банку:

2.1.1. Платежное поручение в рублях РФ;
2.1.2. Запрос на отзыв платежного поручения;
2.1.3. Сообщение свободного формата;
2.1.4. Валютный перевод;
2.1.5. Покупка валюты;
2.1.6. Продажа валюты.

2.2.Форматы электронных документов, направляемых Клиентом Банку:

2.2.1. Платежное поручение в валюте РФ – заполняется в порядке, определенном в экранной форме подсистемы «Клиент»;
2.2.2. Запрос на отзыв платежного поручения - заполняется в порядке, определенном в документации подсистемы «Клиент»;
2.2.3. Запрос на выписку по счету - заполняется в порядке, определенном в документации подсистемы «Клиент»;

2.2.4. Сообщение свободного формата может включать любой текст (например, согласие на акцепт) и любой прикрепленный файл;
2.2.5. Валютный перевод – заполняется в порядке, определенном в документации подсистемы «Клиент»;
2.2.6. Покупка валюты – заполняется в порядке, определенном в документации подсистемы «Клиент»;
2.2.7. Продажа валюты – заполняется в порядке, определенном в документации подсистемы «Клиент».

2.3.Виды электронных документов, направляемых Банком Клиенту:

2.3.1. Выписка по счету за день;
2.3.2. Выписка по счету за период;
2.3.3. Справочная и прочая информация из Банка;
2.3.4. Сообщение свободного формата (например, объявления, запрос на акцепт и пр.).

2.4.Требования по оформлению электронных расчетных документов:

2.4.1. Все ЭД должны содержать необходимые банковские реквизиты согласно требованиям Положения «О правилах осуществления перевода денежных средств», утвержденного ЦБ РФ 19.06.2012г. № 383-П и описанию системного комплекса «АЭБ-Бизнес», должны быть подписанными необходимым количеством ЭП и зашифрованными абонентом Системы «АЭБ-Бизнес», от которого поступает данный документ.
2.4.2. Отзыв электронного документа производится только если имеется возможность отменить его исполнение, при условии, что на этот момент сумма по электронному документу не списана с корреспондентского счета Банка/не зачислена на счет получателя в Банке. Отзыв осуществляется посредством направления в Банк письма об отзыве электронного документа.
2.4.3. Банк проводит операции Клиента по переводу иностранной валюты при наличии подтверждающих документов в соответствии с требованиями действующего законодательства РФ.
2.4.4. Покупка иностранной валюты производится при наличии денежных средств на расчетном счете Клиента в соответствии с требованиями действующего законодательства РФ.
2.4.5. Продажа валюты производится при наличии подтверждающих документов в соответствии с требованиями действующего законодательства РФ.

3. ОРГАНИЗАЦИЯ ЭЛЕКТРОННЫХ РАСЧЕТОВ

3.1.Настоящий раздел Условий устанавливает порядок организации и проведения электронных расчетов между Банком и Клиентом.
3.2.Виды ЭД и требования по их оформлению установлены в п. 2 настоящих Условий.
3.3.Требования к программно-техническим средствам для проведения электронных расчетов:
3.3.1. Банк предоставляет Клиенту следующие программные и аппаратные средства:
3.3.1.1.Ключевой носитель (аппаратное средство для хранения закрытого ключа).
3.3.1.2.Драйвера для аппаратного средства для хранения закрытого ключа (доступны на официальном сайте Банка в сети интернет www.albank.ru).
3.3.1.3.Электронную документацию по Системе (Инструкции по использованию систем ДБО) на официальном сайте Банка в сети интернет www.albank.ru.
3.3.2. Требования к программно-техническим средствам:
3.3.2.1.Персональный компьютер с операционной системой, поддерживаемой браузерами из списка: InternetExplorer 11 и выше; Firefoxактуальной версии; Safari9 и выше; Opera и GoogleChromeактуальной версии.
3.3.2.2.Канал доступа в Интернет;
3.3.2.3.Свободный USB порт.

3.4. Расчеты проводятся через Систему, которая состоит из Центрального абонентского пункта Банка, Центра Регистрации Ключей Банка (далее ЦРК Банка) и Абонентских пунктов Клиентов.

3.5. Абонентский пункт Клиента - канал отправки ЭД в Банк, не требующий установки специализированного программного обеспечения на рабочее место Клиента, работа Клиента в Системе производится посредством браузера и в соответствии с требованиями, указанными в п. 3.3.2. настоящих Условий.

3.6. Для работы в Системе Клиент в Заявлении о присоединении к Условиям указывает предоставление/удаление доступаОтветственнымсотрудникам на работу в Системе.

3.7. При подаче Заявления о присоединении Клиент может выбрать для каждого из своих Уполномоченных лиц один из следующих вариантов защиты данных:

- с использованием ПЭП и одноразовых паролей, передаваемых посредством SMS-сообщений. При каждом подписании документа/сообщения в Системе, Система запрашивает одноразовый пароль, который Уполномоченное лицо Клиента получает на мобильный телефон посредством SMS-сообщения. SMS-сообщение с одноразовым паролем содержит основные реквизиты подписываемого документа/сообщения, которые Клиент обязан проверять.
- с использованием УНЭП, формируемой клиентом и хранимом на устройстве «Электронный ключ».

Клиент имеет возможность изменить для Уполномоченного лица вариант защиты путем подачи соответствующим образом заполненного Заявления о присоединении с пометкой «корректирующее».

3.8. Функции Ответственного сотрудника Клиента:

- создание личных ключей НЭП, в соответствии с документацией на программное обеспечение;
- отслеживание сроков действия ключей, своевременное их обновление и регистрация открытых ключей ЭП в ЦРК Банка;
- подписание ЭД с помощью своего личного ключа ПЭП/УНЭП;
- ответственное хранение своего личного ключевого носителя (аппаратной системы хранения закрытого ключа));
- ответственное хранение своего личного Логина и Пароля;
- своевременное извещение Банка о случаях потери, возможного несанкционированного доступа к ключу ЭП и/или Паролю и их компрометации;
- участие в процедуре проверки ПЭП/УНЭП при рассмотрении конфликтных ситуаций.

3.9. Абонентский пункт Банка принимает документы, передаваемые Клиентом по Системе через Интернет, а также размещает всю необходимую информацию на интернет-сервере Системы в автоматическом режиме, авторизованно доступную Клиенту.

3.10. Для обслуживания Системы Банк назначает ответственное лицо (Администратора), тел.: (4112)-42-29-30.

3.11. Администратор системы Банка выполняет следующие функции:

- отвечает за работу Абонентского пункта Банка в Системе;
- обеспечивает бесперебойное функционирование Абонентского пункта Банка;
- организует регулярную обработку поступившей информации от Клиента и своевременное размещение на интернет-сервере Системы всей необходимой информации по Системе;

3.12. Администратор информационной безопасности Банка выполняет следующие функции:

- Запросы на генерацию сертификатов ключей ПЭП;
- запросы на регистрацию сертификатов ключей УНЭП;
- отзывает существующие сертификаты ключей УНЭП;

- блокирует учетные записи/сертификаты ключей ПЭП/УНЭП клиентов в Системе;
- участвует в процедуре проверки ПЭП/УНЭП при решении конфликтных ситуаций.

4. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ КЛЮЧЕЙ И ПАРОЛЕЙ

4.1. В целях безопасности ключи выдаются на ключевом носителе (аппаратной системе хранения закрытого ключа).

4.2. Клиент обязан хранить в безопасном месте Логин и Пароль входа в Систему.

4.3. В Банке хранятся только открытые ключи Клиента.

4.4. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение ключей ПЭП/УНЭП и Паролей согласно «Правилам информационной безопасности при работе в системе дистанционного банковского обслуживания АКБ «Алмазэргиэнбанк» АО» (Приложение № 3) размещенного на официальном сайте Банка.

4.5. При утрате или компрометации ключа и/или Пароля у Клиента, Клиент обязан немедленно по телефону и в письменной форме оповестить Банк согласно «Правилам информационной безопасности при работе в системе дистанционного банковского обслуживания АКБ «Алмазэргиэнбанк» АО» размещенного на официальном сайте Банка.

4.6. В том случае, если Клиент разрешает кому-либо использовать свои ключи и/или Пароли, то он несет полную ответственность за соблюдение условий настоящих Правил, как со своей стороны, так и со стороны лиц, пользующихся его Ключами и/или Паролями.

5. ПОРЯДОК ПЕРЕДАЧИ И ПРИЕМА ДОКУМЕНТОВ ПО СИСТЕМЕ

5.1. ЭД представляют собой электронные бланки документов, заполняемые Клиентом в соответствии с банковскими требованиями и пересылаемые в Банк по каналам связи с использованием Системы для исполнения.

5.2. Заполняемые в клиентском модуле документы проходят предварительную автоматическую проверку (на дату документа, наприсутствие обязательной информации в полях документа, на соответствие вводимых данных –реквизитам, записанным во встроенном справочнике, а также другую проверку в соответствии с принятой технологией).

5.3. На этапе обработки документов банковским модулем осуществляется автоматический контроль (на соответствие ПЭП/УНЭП содержимому документа, на правильность указанного номера счета Клиента, на соответствие реквизитов Банка и БИК/наименование Банка получателя,установленным Банком России, а также другой контроль в соответствии с принятой технологией,в том числе получение дополнительного подтверждения подлинности и авторства ЭД).

5.4. После заполнения электронной формы документа Клиентом осуществляется подписание документа ПЭП/УНЭП и отправка ЭД в Банк с использованием Системы. В зависимости от принятой Клиентом технологии, если используется вторая ЭПвторого Уполномоченного лица, Клиент подписывает ЭД и второй своей ПЭП/УНЭП. ПЭП/УНЭП подтверждает авторство отправленного по Системе документа и гарантирует его целостность, так как любое изменение в документе после его подписания сделает ПЭП/УНЭП недействительным.

5.5. Основанием для принятия к исполнению Банком переданного Клиентом по Системеплатежного документа является аутентификация соединения Клиента, а также наличие и корректность необходимого количества ПЭП/УНЭП, соответствие требованиям действующего законодательства РФ к оформлению платежных документов.

5.6. Система автоматически отражает сведения о текущем состоянии документов в Банке (получении, приеме к исполнению и исполнении или неисполнении документа) посредством изменения статусов ЭД.
5.7. Активной стороной при установлении связи является Клиент.
5.8. Основанием для отказа Банка от исполнения ЭДслужат:
-отрицательный результат проверки подлинности ПЭП/УНЭП;
-отсутствие ПЭП/УНЭП под документами, наличие ЭП неуполномоченного лица;
-недостаток денежных средств для проведения операции на счете Клиента;
-несоответствие даты документа требуемой;
-неверно указанные реквизиты;
-проведение Клиентом сомнительных/подозрительных операций;
-неоплата Клиентом в установленный срок услуг Банка по установке и обслуживанию Системыв соответствии с Тарифами Банка.
5.9. Клиент запрашивает и получает выписки по Счету, служебные сообщения, а также иную информацию, адресованную ему Банком.
5.10. По отдельным платежным документам Банк может запросить дополнительное подтверждение или разъяснение. Подтверждение запрашивается по Системе в свободном формате, либо иным образом в день получения платежного документа. В этом случае платежный документ принимается к исполнению после получения требуемого подтверждения в свободном формате.

6. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

6.1. Для обеспечения идентификации, безопасности и конфиденциальности при передаче документов посредством Интернет используется Логин и Пароль Клиента, а также система шифрования и ПЭП/УНЭП.
6.2. Ответственномусотруднику Клиента Администратором Системы передаются Логин (идентификатор) и Пароль Клиента.
6.3. Ответственному сотруднику Клиента передаются технологические ключи шифрования и УНЭП Системы. Технологические ключи не позволяют передавать платежную информацию, и предназначены для самостоятельного изготовления Клиентом ключей шифрования и ЭП. Изготовленные Клиентом ключи шифрования и электронной подписи признаются действительными на основании Акта о признании открытого ключа (сертификата) для обмена сообщениями (Приложение № 2 к настоящим Условиям).
6.4. Банк гарантирует, что используемые системы защиты информации являются достаточными для защиты ЭД от несанкционированного доступа, сохранения конфиденциальности, подтверждают подлинность ЭД, исключают искажение информации третьими лицами.
6.5. Клиент признаёт метод шифрования информации и ЭП, используемую для передачи документов между Банком и Клиентом.
6.6. Клиент признает, что в целях выполнения Банком функций, установленных Федеральным законом № 115 «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» от 07.08.2001 года Банк вправе отказать Клиенту в приеме к исполнению распоряжений Клиента, подписанных ЭП, и требовать для исполнения надлежащим образом оформленные распоряжения Клиента на бумажном носителе.
6.7. Используемые во взаимоотношениях между Банком и Клиентом при электронных расчетах документы в электронной форме, заверенные ЭП и соответствующие требованиям настоящих Условий, признаются эквивалентными соответствующим бумажным документам и порождают аналогичные им права и обязанности Сторон. Для заверения ЭД Клиент может использовать одну или две ЭП. В случае, если

используются две ЭП, заполняются два акта согласно Приложению № 2 к Условиям.

6.8. В случае изменения подписей в Карточке с образцами подписей и оттиска печати, Клиент обязан предоставить Банкуновые Акты о признании открытого ключа (сертификата) для обмена сообщениями с образцами ЭП, корректирующее Заявление о предоставлении/удалении доступов Уполномоченных лиц Клиента.

6.9. При получении каждой из Сторон от другой Стороны документа, подписанного ЭП, в Системе выполняется процедура подтверждения достоверности документа, подписанного ЭП. В случае отрицательного результата подтверждения, документ к исполнению не принимается.

6.10. При невозможности проведения платежей в Системе, Клиент имеет право провести их в обычном порядке (в соответствии с действующим «Положением о правилах осуществления перевода денежных средств» (утв. Банком России 19.06.2012 № 383-П).

6.11. Проверка индивидуального номера абонента (IMSI) совершается в момент инициации процесса подписания ЭД в Системе. Электронный документ не проходит процедуру подписания с незарегистрированным индивидуальным номером абонента (IMSI) в Системе, соответственно, в обработку Банком не принимается.

6.12. Клиент уведомлен, что в случае использования услуг оператора сотовой связи, который не поддерживает использование дополнительного механизма контроля защиты систем дистанционного банковского обслуживания - международного идентификатора мобильного абонента (IMSI), увеличивается риск мошеннических действий третьих лиц, которые могли бы быть предотвращены с помощью указанного механизма защиты. Все риски, связанные с выбором Системы без использования дополнительного механизма контроля защиты, Клиент принимает на себя.

6.13. Стороны признают:

- в соответствии с настоящими Условиями Сторонами может использоваться простая электронная подпись (ПЭП) и/или усиленная неквалифицированная электронная подпись (УНЭП);
- после подписания ЭД ЭП изменение, добавление или удаление символов значимых данных документа (данных, участвующих в расчёте ЭП) делает ЭП некорректной, т.е. проверка ЭП Клиента дает отрицательный результат;
- создание Корректной УНЭПЭД возможно исключительно с использованием ключа ЭП;
- создание корректной ПЭП возможно только в рамках непрерывного защищенного интернет-соединения с Банком после идентификации и аутентификации Клиента, с использованием одноразовых паролей, передаваемых Банком Клиенту посредством SMS-сообщений, при корректном SMS-подтверждении им пароля в ограниченный период времени.

7. ПОРЯДОК ПРОВЕДЕНИЯ ЭЛЕКТРОННЫХ РАСЧЕТОВ

7.1. Проведение всех расчетных операций и получение всей информации по Системе осуществляется Клиентом в режиме онлайн посредством Интернет во время сеансов связи с Банком.

7.2. Клиент в соответствии с Условиями оформляет и передает в Банк платежный ЭД на его исполнение. В случае, получения отрицательного результата проведения процедуры подтверждения достоверности документа, подписанного ЭП, документ к исполнению не принимается.

7.3. Клиент получает служебное электронное сообщение об отрицательном результате проверки и, следовательно, об отказе и принятии к исполнению ЭД. Статусы

электронных документов, однозначно отражающие их текущее состояние, автоматически отслеживаются во время сеансов связи, проводимых Клиентом.

7.4. Стороны имеют право в электронной форме передавать или получать по СистемеЭД, перечисленные в п. 2 настоящих Условий, а также любой документ, который может быть дополнительно внесен в п. 2 настоящих Условий, по письменному соглашению Сторон. Допускается передача другой информации по Системе, но эта информация не является основанием возникновения обязательств.

7.5. ЭД порождает обязательства Сторон по настоящим Условиям, если он надлежащим образом Клиентом оформлен в соответствии с требованиями действующего законодательства РФ, заверен ЭП, зашифрован и передан по Системе на исполнение, а Банком получен, расшифрован, проверен на соответствие нормам действующего законодательства РФ и принят к исполнению. Свидетельством того, что платежный ЭД принят к исполнению, является изменение статуса документа в Системе.

7.6. В случае невозможности по каким-либо причинам передачи электронных документов с помощью Системы, Клиент должен доставить эти соответствующим образом оформленные на бумаге документы в Банк.

7.7. В случае расхождений между содержанием полученного Банком от Клиента документа в электронной форме, подписанного ЭП, и содержанием этого же документа на бумажном носителе, подлинным является документ в электронной форме.

8. ПРАВА И ОБЯЗАННОСТИ СТОРОН

8.1. Обязанности Сторон.

8.1.1. Стороны обязуются при проведении электронных расчетов с использованием Системы руководствоваться правилами и требованиями, установленными Центральным Банком Российской Федерации, действующим законодательством РФ и настоящими Условиями.

8.1.2. Банк не несет ответственности за сбои в работе Системы ДБО по причине изменений, вносимых Клиентом в клиентский модуль Системы ДБО без согласования с Администратором Системы ДБО Банка или в результате ненадлежащего исполнения Клиентом требований настоящих Условий, изменения конфигурации рабочего места, заражения вредоносным программным обеспечением.

8.1.3. Стороны обязуются не разглашать третьим сторонам (за исключением случаев, предусмотренных действующим законодательством или соглашением Сторон), конкретные способы защиты информации, реализованные в используемой по настоящим Условиям Системе.

8.1.4. Стороны обязуются сохранять в тайне применяемые в системе защиты информации секретные ключи ЭП и проводить их замену в случаях компрометации ключа одной из Сторон.

8.1.5. Каждая из Сторон обязуется немедленно информировать другую Сторону обо всех случаях компрометации секретных ключей ЭП, их утраты, хищения, несанкционированного использования, а также повреждения программно-технических средств подсистем обработки, хранения, защиты и передачи информации, для проведения смены ключей и других согласованных действий по поддержанию в рабочем состоянии Системы. При этом работа по Системе приостанавливается до проведения смены ключей. Смена ключей оформляется актами согласно Приложения №3 к настоящим Условиям.

8.1.6. Каждая Сторона имеет право запрашивать, и обязана предоставить по запросам другой Стороны, не позднее следующего банковского дня с момента получения

запроса, надлежащим образом оформленные бумажные копии электронных документов.

8.1.7. Стороны устанавливают, что вся информация по Системе считается доведенной до сведения Клиента по истечении 3 (трех) банковских дней с даты ее размещения на интернет-сервере Системы (включая день размещения).

8.2.Клиент обязан:

8.2.1. Ввести в течение 10 банковских дней с момента заключения Договора в эксплуатацию программно-технические средства в соответствии с требованиями п. 3.3.2. настоящих Условий для обеспечения работы по Системе. В случае невыполнения Клиентом данного обязательства Банк вправе в одностороннем порядке отказаться от выполнения своих обязательств по Договору, расторгнув его.

8.2.2. Контролировать правильность реквизитов получателя платежа на своих документах. В случае обнаружения ошибки Клиент имеет право направить отзыв своего электронного документа с помощью Системы. Банк принимает отзыв электронного документа только в том случае, если он еще не исполнен и у Банка имеется технологическая возможность отменить его исполнение в соответствие с нормами действующего законодательства РФ.

8.2.3. Контролировать соответствие суммы платежа и остатка на своем счете в Банке иосуществлять платежи только в пределах этого остатка. Настоящий пункт не применяется приналичии дополнительного соглашения к договору банковского счета о кредитовании счетапутем предоставления кредита в форме «овердрафт».

8.2.4. Обеспечивать защиту клиентского модуля Системы отнесанкционированного доступа, а также заражения вредоносным кодом (вирусами). В случае обнаружения неработоспособности Системы, признаков несанкционированного доступа к системе, а также признаков заражения клиентского модуля Системы вредоносным кодом (вирусами), не позднее следующего рабочего дня с момента обнаружения сообщить об этом Банку любым доступным способом.

8.2.5. Неукоснительно соблюдать согласно «Правила информационной безопасности при работе в системе дистанционного банковского обслуживания АКБ «Алмазэргиэнбанк» АОразмещенного на официальном сайте Банкаwww.albank.ru.

8.2.6. При уведомлении Банком о необходимости смены программного обеспечениясуществить все необходимые действия для своевременного получения и установки новойверсии программ клиентского модуля Системы.

8.2.7. При смене должностных лиц/Уполномоченных лиц Клиента необходимо написать корректирующее Заявление в Банк для изготовления новых Логинов и Паролей в Систему, признания недействительными ключей шифрования и ЭП, и произвести перегенерацию новых ключей шифрования и ЭП с заполнением Акта признания открытых ключей (сертификата) для обмена сообщениями. В случае отсутствия у Банка информации об изменении состава уполномоченных лиц Клиента, имеющих право подписывать финансовые документы, ответственность за подлинность ЭД, заверенных ЭП Клиента, возлагается на Клиента, в частности, Банк не несет ответственности за убытки, причиненные Клиенту, в случае, если прекращение полномочии лиц, утративших право распоряжаться денежными средствами на счете Клиента, не было своевременно документально подтверждено.

8.2.8. Уничтожить, при расторжении Договора все принадлежащие ему конфиденциальные данные и все программное обеспечение клиентской части Системы, относящиеся к настоящим Условиям, и не передавать их третьим лицам.

8.2.9. Клиент не имеет права тиражировать и передавать третьей стороне программное обеспечение, поставляемое Банком.

8.2.10. Клиент обязан соблюдать условия хранения ключей ЭП и Паролей в соответствии с настоящими Условиями. Банк не несет ответственности за убытки, причиненные Клиенту в случае несоблюдения данных условий.

8.2.11. Клиент обязан соблюдать условия обеспечения безопасности при работе с веб-сайтом Системы. Банк не несет ответственности за убытки, причиненные Клиенту в случае несоблюдения данных условий.

8.2.12. С момента окончания срока действия Сертификата ЭП и до момента оформления Клиенту нового Сертификата, Клиент не вправе проводить в Системе какие-либо операции, а Банк прекращает прием ЭД.

8.2.13. Уплачивать Банку комиссионное вознаграждение в размере и сроки,установленные Тарифами Банка. Указанное условие также является заранее данным акцептомКлиента Банку на списание причитающегося ему вознаграждения и иных сумм по настоящемуДоговору, который предоставлен без ограничения по количеству расчетных документов Банка,выставляемых в соответствии с условиями настоящего Договора, а также без ограничения посумме и требованиям из обязательств, следующих из настоящего Договора.

8.2.14. Предоставлять Банку информацию, необходимую для осуществления расчетно-кассового обслуживания, а также информацию, необходимую для выполнения Банком своих функций, установленных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» № 115-ФЗ от 07.08.2001 года (далее по тексту - Федеральный закон № 115-ФЗ), «Правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в АКБ «Алмазэргиэнбанк» АО» №1124-ПВ(далее по тексту – Правил внутреннего контроля Банка), в том числе, но не исключительно:

- документы и сведения, необходимые Банку для исполнения требований, предусмотренных Федеральным законом № 115-ФЗ, Правилами внутреннего контроля Банка;
- сведения о представителях, выгодоприобретателях и бенефициарных владельцах в объеме и порядке, предусмотренном Банком;
- информацию о целях установления и предполагаемом характере их деловых отношений с Банком, а также о целях его финансово-хозяйственной деятельности, финансового положения и деловой репутации;
- информацию о внесении изменений в учредительные документы Клиента, в течение 3 (трех) банковских дней с момента их регистрации; изменении наименования, организационно-правовой формы, оттиска печати Клиента, местонахождении Клиента, его почтового адреса, номерах контактных телефонов и факсов, реорганизации/ликвидации Клиента, а также обо всех других изменениях идентификационной информации, способных повлиять на исполнение настоящего Договора;
- сведения о должностных лицах, имеющих право подписывать платежные документы, их приеме/ увольнении (при этом одновременно представлять Банку новую банковскую карточку с образцами подписей и оттиска печати), - в течение 3 (трех) банковских дней с даты наступления одного из перечисленных событий.

8.3.БАНК обязан:

8.3.1. Предоставить Клиенту программные и аппаратные средства в соответствии с п. 3.3.1. настоящих Условий в течение 10 (десяти) банковских дней с момента заключения Договора и хранить эталонные экземпляры указанного программного обеспечения.

8.3.2. Оказывать консультационные услуги Клиенту и его персоналу по вопросамэксплуатации Системы(функционирование Системы ДБО, использование средств защитыи передачи/приема информации, технология обработки информации). Контакты и режимработы служб Банка, задействованных в подключении и сопровождении Клиента приобслуживании с использованием Системы, в том числе в региональной сети Банка,размещены на официальном сайте Банка

8.3.3. Осуществлять расчетные операции по списанию средств по банковским счетам Клиента на основании платежных ЭД, поступивших через Систему в операционное время обслуживания корпоративных клиентов проводить текущим операционным днем. Платежи, поступившие послеоперационное время, исполняются следующим рабочим днем.

Операционное время для совершения расчетных операций по банковским счетам корпоративных клиентов в подразделениях Банка размещено на официальном сайте и на информационных стендах Банка.

8.3.4. Осуществлять расчетные операции по зачислению средств на счет Клиента на основании расчетных документов (в том числе и электронных), поступивших от других клиентов, банков-корреспондентов, клиринговых центров и учреждений ЦБ РФ.

8.3.5. Принимать к исполнению полученные по СистемеЭД Клиента, признанныеравнозначными документу на бумажном носителе, подписанному собственноручной подписью,оформленные и подписанные (заверенные) Клиентом в соответствии с Условиями, а такжеосуществлять обработку и исполнение таких ЭД Клиента в строгом соответствии сустановленными нормами, техническими требованиями, стандартами, нормативными актамиБанка России и нормативными документами Банка.

8.3.6. Обеспечивать защиту банковского модуля Системыотнесанкционированного доступа и обеспечивать конфиденциальность информации по счетам.

8.3.7. Обеспечить конфиденциальность информации об электронных расчетах, проводимых в соответствии с настоящими Условиями.

8.3.8. Контролировать правильность реквизитов на электронных расчетных документах Клиента, а также соответствие документа требованиям действующего законодательства РФ. Неправильно оформленные электронные расчетные документы Клиента к исполнению не принимаются. Банк не имеет права самостоятельно корректировать реквизиты платежных ЭД Клиента.

8.4.Банк вправе:

8.4.1. Списывать со счета Клиента без его дополнительного распоряжения на основаниизаранее данного акцепта с формированием расчетных документов (в том числе банковскогоордера) плату за осуществление дистанционного банковского обслуживания Клиента всоответствии с действующими Тарифами по мере совершения операций.

8.4.2. Отказать в проведении операции в случае осуществления операции в Системе, в отношении которой возникают подозрения, что она осуществляется в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, в соответствии с действующим законодательством РФ и нормативными документами Банка России, а также в случае непредставления документов, запрашиваемых Банком.

8.4.3. В случае необходимости требовать от Клиента:
– оформления расчетного документа на бумажном носителе, оформленного в соответствии с требованиями Банка России, и не производить платеж до представления указанного документа, о чем Банк обязан сообщить Клиенту любым доступным Банку способом не позднее следующего рабочего дня с момента получения документа в электронной форме;
- подтверждения подлинности и авторства ЭД путем обращения по контактным номерам телефонов Клиента не позднее следующего рабочего дня с момента получения документа в электронной форме.

8.4.4. Приостанавливать расчетные операции в Системе в случае, если по истечении 10 (десяти) банковских дней со дня выставления требования на оплату услуг согласно Тарифам Клиент не оплатил его. Банк блокирует оказание услуг в Системе до момента полной оплаты услуг Банка. В случае задержки оплаты услуг Банка более 30 (тридцати) банковских дней подряд, Банк вправе в одностороннем порядке расторгнуть Договор.

8.4.5. Производить замену программного обеспечения Системы без согласия Клиента. Банк обязан уведомить об этом Клиента не менее чем за 10 (десять) календарных дней, а Клиент обязан в соответствующий срок получить у Банка или приобрести за свой счет и ввести в эксплуатацию необходимые программные средства.

8.4.6. Пересматривать в одностороннем порядке Условия и Тарифы на обслуживание Клиента по настоящим Условиям. Банк уведомляет о введении новых либо изменении действующих Условий и Тарифов Банка, о порядке обслуживания Клиентов Банка (включая график работы и операционное время Банка, условиях приема и проверки расчетных (платежных) документов) не менее чем за 10 (Десять) календарных дней до их введения / изменения путем размещения информации в операционном зале Банка и на официальном сайте Банка www.albank.ru.

8.4.7. Произвести отключение Клиента от Системы в случае нарушений Клиентом условий п. 3 настоящих Условий.

8.4.8. В целях выполнения Банком функций, установленных Федеральным законом № 115-ФЗ Банк вправе:
- отказать Клиенту в приеме распоряжения на проведение операции по банковскому счету подписанному ЭП, в случае осуществления систематически и/или в значительных объемах операций, в отношении которых возникают подозрения, что они осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма;
- отказать Клиенту в приеме от него распоряжения на проведение операции по банковскому счету, подписанному ЭП;
- приостановить услугу в части использования Клиентом Системы, а также их возобновить;
- требовать для исполнения надлежащим образом оформленные распоряжения Клиенту на только на бумажном носителе.

9. ФИНАНСОВЫЕ ВЗАИМООТНОШЕНИЯ

9.1. Клиент за свой счет приобретает программные и аппаратные средства в соответствии с п. 3.3.2. настоящих Условий (при отсутствии таковых).

9.2. За подключение Клиента к Системе, а также за систему шифрования за каждый приобретаемый Клиентом ключ шифрования взимается единовременная плата в соответствии с Тарифами. Соответствующая денежная сумма должна быть внесена Клиентом на счет Банка согласно выставленным счетам не позднее 10 (десяти) банковских дней.

9.3. За оказываемые Банком услуги по проведению расчетных операций с помощью Системы с Клиента взимается абонентская плата согласно Тарифам Банка.

9.4. Плата за услуги Банка в соответствии с действующими Тарифами списывается Банком со счета Клиента, указанного в Заявлении о присоединении, а в случае отсутствия/недостаточности на нем средств для оплаты услуг Банка с иных счетов Клиента в Банке, без дополнительного распоряжения Клиента, или, в случае отсутствия у Клиента счетов, открытых в АКБ Алмазэргиэнбанк АО, путем безналичного перечисления денежных средств со счетов, открытых в других кредитных организациях.

9.5. При задержке Клиентом оплаты за проведение операций через Систему, в том числе при отсутствии на счете Клиента необходимого остатка денежных средств, Банк блокирует оказание услуг в Системе до момента полной оплаты услуг Банка. В случае задержки оплаты услуг Банка более 30 (тридцати) банковских дней подряд, Банк вправе в одностороннем внесудебном порядке расторгнуть Договор.

9.6. В целях исполнения требований Федерального закона от 27.06.2011 г. № 161-ФЗ «О национальной платежной системе» Банк уведомляет Клиента о совершении каждой операции по счету с использованиемСистемы путем формирования и направления Клиенту выписки по счету сиспользованием Системы. (Подготавливать и представлять Клиенту выписки по счету, содержащие сведения о совершенных по результатам обработки и исполнения ЭД Клиента операциях, а также об иных операциях, в срок до 10:00 часов (по местному времени) следующего рабочего дня виде надлежащим образом оформленных ЭД).

10. ОТВЕТСТВЕННОСТЬ СТОРОН

10.1. Стороны несут ответственность за достоверность информации, представляемой друг другу.

10.2. За неисполнение или ненадлежащее исполнение обязательств по ДоговоруСтороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

10.3. Банк не несет ответственности за неисполнение или ненадлежащее исполнение ЭД Клиента, произошедшее из-за нарушения Клиентом настоящих Условий, в том числе из-за непредоставления Клиентом документов или из-за отсутствия связи по контактным телефонам Клиента для подтверждения подлинности и авторства ЭД в соответствии с п. 8.4.3Риск неправомерного подписания ЭД ЭП несет Клиент, на уполномоченное лицо которого выдан сертификат ключа проверки ЭП соответствующий ключам ЭП. Риск разглашения Логина и Пароля, переданных Клиенту, несет Клиент.

10.4. Банк не несет ответственности за сбои в работе Системы по причине изменений, вносимых Клиентом в клиентский модуль Системыбез согласования с Администратором Системы Банка или в результате ненадлежащего исполнения Клиентом требований настоящих Условий, изменения конфигурации рабочего места, заражения вредоносным программным обеспечением.

10.5. Клиент несет ответственность за выполнение и соблюдение на рабочем месте согласно «Правил информационной безопасности при работе в системе дистанционного банковского обслуживания АКБ «Алмазэргиэнбанк» АОразмещенного на официальном сайте Банка www.albank.ru.

10.6. Банк несет ответственность перед Клиентом за неисполнение/ненадлежащее исполнение операций по счету в соответствии с законодательством Российской Федерации. Ответственность Банка не наступает в случае, если операции по счету Клиента осуществляются несвоевременно, либо не могут быть осуществлены по причинам, не зависящим от Банка, а также в случае нарушения Клиентом обязательств, предусмотренных п. п. 8.2. настоящих Условий.

10.7. Клиент несет ответственность за действия уполномоченных лиц, предоставляющих документы, необходимые для открытия/переоформления/ закрытия счета и проведения операция по нему и для доступа к Системе.

10.8. Банк не несет ответственности за последствия исполнения поручений, выданных неуполномоченными на распоряжение счетом лицами в случаях, когда при соблюдении предусмотренных банковскими правилами и настоящим Договором процедур Банк не мог установить факта выдачи распоряжения неуполномоченными лицами.

10.9. Банк не несет ответственности за последствия исполнения электронного документа, защищенного корректной ПЭП или УНЭП Клиента, в т.ч. в случае использования мобильных телефонов или «Электронных ключей», программно-аппаратных средств клиентской части Системы неуполномоченным лицом.

10.10. Банк не несет ответственности за отказ от приема, неисполнение или ненадлежащее исполнение расчетных документов Клиента и связанные с этим убытки в случаях нарушения Клиентом законодательства РФ, правил ведения документации и сроков предоставления документов, установленных законодательством РФ, нормативными актами Банка России, а также в случае отсутствия на счете Клиента необходимого остатка денежных средств.

10.11. Банк не несет ответственность за невозможность использования Системы вследствие неудовлетворительного качества связи.

10.12. Банк не несет ответственности в случае утери мобильного устройства Клиента.

10.13. Банк не несет ответственность за убытки, возникшие вследствие утери Клиентом ключевого носителя, а также несанкционированного доступа к ней третьих лиц.

10.14. Банк не несет ответственность за техническое состояние компьютерного оборудования Клиента, возможные помехи в телефонных сетях связи, сбоях каналов связи и прекращение использования Системы, вследствие отключения электроэнергии и повреждения линий связи.

10.15. Стороны освобождаются от ответственности за неисполнении либо ненадлежащее исполнение принятых на себя обязательств по настоящим правилам вследствие обстоятельств непреодолимой силы, возникших после заключения Договора, к которым относятся: стихийные бедствия, землетрясения, наводнения, аварии, пожары, отключения электроэнергии, повреждение линий связи, массовые беспорядки, забастовки, революции, военные действия, противоправные действия третьих лиц, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих указанные в настоящих Правилах виды деятельности либо препятствующие выполнению Сторонами своих обязательств по настоящим Правилам. Сторона, пострадавшая от действия (-й) обстоятельств непреодолимой силы обязана в возможно короткие сроки после возникновения таких обстоятельств известить о случившемся другую Сторону, а также предпринять меры для ликвидации последствий обстоятельств непреодолимой силы (обстоятельств форс-мажора). В извещении должен быть указан срок, в течение которого предполагается исполнить обязательства.

11. ОСОБЫЕ УСЛОВИЯ

11.1. Программное обеспечение, а также техническая документация, необходимые для функционирования Системыи сертифицированные средства криптографической защиты информации, предоставляются Клиенту во временное пользование на срок действия Договора и не могут быть переданы третьим лицам, за исключением случаев и порядке, установленных действующим законодательством Российской Федерации.

11.2. Инициатором сеансов связи с Банком всегда является Клиент. Отсутствие инициативы Клиента в установлении сеанса связи с Банком не влечет за собой ответственность Банка за невыполнение им своих обязательств (в том числе по уведомлению Клиента о совершенных операциях по счету).

11.3. Клиент и Банк согласны с тем, что действие Договора в части сохранения конфиденциальности и в неразглашения паролей и ключей системы защиты информации, действительно в течение одного календарного года после прекращения действия Договора по обстоятельствам, определенным в разделе 13 настоящих Условий.

11.4. Все процедуры создания, регистрации, хранения, плановой и внеплановой смены криптографических ключей УНЭП и сертификатов ключей проверки УНЭП осуществляются в соответствии с настоящими Условиями.

11.5. Плановая смена ключей УНЭП и соответствующего им сертификата ключа проверки УНЭП проводится не реже одного раза в год, внеплановая – в случаях компрометации действующих ключей ЭП, непреднамеренного уничтожения ключей УНЭП и выхода из строя. Кроме того, Клиент обязан произвести смену принадлежащих ему ключей УНЭП по требованию Банка.

При смене ключей УНЭП Клиент уплачивает Банку соответствующее комиссионное вознаграждение в соответствии с Тарифами.

11.6. Все операции по счету, совершаемые с использованием Системы с соблюдением требований настоящих Условий и приложений к Условиям, осуществляются Банком в общем порядке до момента поступления от Клиента уведомления об утрате/компрометации/подозрении на компрометацию ключа УНЭП или о том, что операция совершена без согласия Клиента.

11.7. Стороны обязаны соблюдать принципы и правила обработки персональных данных субъектов, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также осуществлять защиту обрабатываемых персональных данных в соответствии со статьей 19 указанного Федерального закона».

12. ИЗМЕНЕНИЕ ПРАВИЛ

12.1. В целях повышения качества обслуживания Клиента в Системе, повышения безопасности проводимых операций с использованием Системы Банк вправе вносить изменения в настоящие Условия и/или Тарифы. Банк уведомляет Клиента об изменении Условий и/или Тарифов не позднее, чем за 10 (Десять) календарных дней до даты введения в действие новой редакции Условий любым из следующих способов:

- путем размещения указанной информации на веб-сайте Банка в сети Интернет по адресу: www.albank.ru;
- путем размещения указанной информации на информационных стендах Банка;

12.2. В течение 10 (десяти) календарных дней со дня вступления в силу новой редакции Условий Клиент обязан письменно уведомить Банк о согласии на новые условия либо о расторжении Договора. Непредставление Клиентом письменного уведомления рассматривается Банком как согласие на новые условия Договора.

13. СРОК ДЕЙСТВИЯ ДОГОВОРА

13.1. Договор вступает в силу с даты подачи Клиентом в Банк Заявления о присоединении

13.2. Договор может быть расторгнут досрочно любой из Сторон в одностороннем порядке. В случае если Стороной инициатором расторжения является Клиент, то онпредставляет в Банк письменное заявление с указанием предполагаемой даты расторжения Договора. В случае если Стороной инициатором расторжения является Банк, то оннаправляет Клиенту соответствующее уведомление с указанием предполагаемой датырасторжения Договора, но не менее чем за 15 календарных дней до даты такогорасторжения.

13.3. Существующие на дату расторжения Договора обязательства Сторон, в том числе в части расчетов за уже оказанные услуги, сохраняют свою силу до момента их полного исполнения.

13.4. Договор прекращает свое действие с даты расторжения либо прекращения договора банковского счета. В случае использования Клиентом Системы в отношении нескольких счетов, открытых в Банке, действие Договора в отношении действующих счетов Клиента сохраняется.

13.5. Банк вправе расторгнуть Договор в одностороннем порядке в любое время, в том числе, но не исключительно, в случаях если:

- несогласия Клиента с изменениями Тарифов и(или) Условиями в новой редакции.
- нарушения Клиентом требований к использованию Системы и обеспечению безопасности при использовании Системы, если данное нарушение повлекло ущерб для Банка или в случае двукратного нарушения указанных требований и условий, независимо от последствий нарушения.
- невыполнения Клиентом требований настоящих Условий, а также в случае задержки оплаты услуг Банка согласно п. 9.4.Условий.
- изменения законодательства Российской Федерации, существенно изменяющего права и обязанности Сторон.
- Банк вправе в одностороннем порядке расторгнуть настоящий Договор в случае принятия в течение календарного года двух и более решений об отказе в выполнении распоряжения Клиента о совершении операции на основаниип.8.4.7. настоящего Договора и в других случаях, предусмотренных законодательством РФ.

13.6. Расторжение Договора не влияет на действительность и порядок действия электронных документов, сформированных с использованием Системы, до даты расторжения Договора.

13.7. Расторжение Договора не прекращает обязательства Сторон, возникшие до момента расторжения. Указанные обязательства сохраняют свое действие до момента их полного исполнения соответствующей Стороной Договора.

13.8. Споры по Договору Стороны разрешают путем переговоров с учетом взаимных интересов. Если в результате переговоров Стороны не приходят к согласию, спор передается на рассмотрение в Арбитражный суд РС (Я) в соответствии с действующим законодательством РФ.

Приложение № 1
К Условиям предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес»

ЗАЯВЛЕНИЕ (ОФЕРТА) О ПРИСОЕДИНЕНИИК УСЛОВИЯМ ПРЕДОСТАВЛЕНИЯ УСЛУГ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ «АЭБ БИЗНЕС»

❒**ПЕРВОНАЧАЛЬНОЕ**

❒**КОРРЕКТИРУЮЩЕЕ** **№ ДБО** _____

1. СВЕДЕНИЯ О КЛИЕНТЕ

Наименование заявителя (далее – Клиент):_____

(указывается полное наименование в соответствии с учредительными документами)

_____

Адрес местонахождения (юридический адрес):_____

_____

(адрес юридического лица, указанный в ЕГРЮЛ; адрес места жительства (места пребывания) индивидуального предпринимателя или физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой)

Контактный телефон Клиента: _____

Адрес электронной почты Клиента (e-mail): | | | | | | | | | | | | | | | | | | | | |

Клиент является по законодательству Российской Федерации ☐ резидентом ☐ нерезидентом

ИНН/КИО	
КПП	
ОГРН/ОГРНИП	

2. ПОДПИСЬ КЛИЕНТА

Клиент в лице_____,

(указывается фамилия, имя, отчество, должность руководителя (уполномоченного представителя) Клиента/ статус физического лица, осуществляющего предпринимательскую деятельность/занимающегося частной практикой)

действующего/ей на основании _____

(указывается наименование документа – Устав, Доверенность, иной соответствующий документ)

выражает согласие, что подписание настоящего Заявления является подтверждением того, что Клиент:

1. ознакомился и согласен с действующими «Условиями предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес» и Тарифами, размещенными на официальном сайте Банка в сети интернет по адресу: http://www.albank.ru;
2. **Просит выдать Электронные ключи для работы с системой «АЭБ Бизнес»** в количестве: _____ шт.
3. **Просит ❒ предоставить доступ**

❒ удалить доступ для работы в системе следующим сотрудникам

❒ изменить текущую учетную запись

1. ФИО (полностью)	
Должность	
Подпись сотрудника	
Срок полномочий	с _____ по _____
Номер телефона	+ 7									
Право подписи	❒Единственная подпись ❒Вторая подпись ❒Первая подпись ❒Без права подписи
Вариант защиты Системы	❒SMS пароли ❒ Электронный кдюч
2. ФИО (полностью)	
Должность	

Подпись сотрудника	
Срок полномочий	с _____ по _____
Номер телефона	+ 7 ☐☐☐☐☐☐☐☐☐☐
Право подписи	❒Единственная подпись ❒Вторая подпись ❒Первая подпись ❒Без права подписи
Вариант защиты Системы	❒SMS пароли ❒ Электронный кдюч

4. **Плату за услуги Банка просит списывать со счета №** ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

М.П. Клиента _____ _____ 20___ г. _____/ _____/

дата *подпись* *Фамилия И.О.*

3. ОТМЕТКИ БАНКА

АКБ «Алмазэргиэнбанк» АО, 677000, Республика Саха (Якутия), г. Якутск, пр. Ленина, 1

ОГРН 1031403918138 **ИНН** 1435138944 **БИК** 049805770**Корр.счет**30101810300000000770 **в Отделении-НБ РС(Я)**

Заявление принял, идентификацию Клиента осуществил:

___ _____ 20__ г. _____ _____/ _____/

дата *должность сотрудника, принявшего Заявление* *подпись* *Фамилия И.О.*

Приложение № 2
К Условиям предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес»

АКТ
признания открытого ключа (сертификата) для обмена сообщениями

___ 20___ г.

Настоящим Актом признаётся открытый ключ шифрования, принадлежащий уполномоченному представителю организации

Наименование организации: _____

Юридический адрес: _____

Телефон: _____

Фамилия, имя, отчество владельца ключей: _____

Должность: _____

Удостоверение личности: _____

_____

Личная подпись владельца ключа _____

Параметры ключа:

Алгоритм: ГОСТ Р 34.10-2001 (1.2.643.2.2.19), Параметры:

Начало срока действия:

Окончание срока действия:

Текст открытого ключа:

Дополнительные поля открытого ключа (сертификата):

Серийный номер ключа: **********

Имя владельца ключей:

Дополнительная информация о владельце ключа:

Код страны: RU

Город:

Организация:

Параметры издателя (центра сертификации):

Имя: aebank-ISIMPLE-CA4

Данные об издателе:

Ключ зарегистрирован и может использоваться для обмена сообщениями.
Группа подписи - Единственная.

БАНК	**КЛИЕНТ**
АКБ «АЛМАЗЭРГИЭНБАНК» АО	_____
_____ / _____ /	_____ / _____ /
М.П.	М.П.

Приложение № 3
К Условиям предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес»

Правила информационной безопасности при работе в системе дистанционного банковского обслуживания АКБ «Алмазэргиэнбанк» АО

Правила информационной безопасности при работе в системе дистанционного банковского обслуживания (далее – Правила) составлены в соответствии с требованиями Законодательства Российской Федерации, Стандартом Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» и другими нормативными документами Банка России, а также Политикой информационной безопасности АКБ «Алмазэргиэнбанк» АО (далее – Банк) и являются обязательными к исполнению Клиентами, заключившими Договор на подключение к системам дистанционного банковского обслуживания (далее – ДБО).

1. Общие положения

1.1. Настоящие Правила являются обязательным **Приложением к «Условиям предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес».**

1.2. Настоящие Правила определяют Защитные меры по обработке Рисков нарушения Информационной безопасности при использовании Клиентами Системы ДБО. При этом Клиент обязан учитывать то, что:

- Сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- Существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- Существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из сети Интернет;
- Гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
- Меры по нейтрализации Злоумышленных действий могут быть эффективными только в течение первых часов после Инцидента;
- Расследованием Злоумышленных действий и поиском Злоумышленников занимаются правоохранительные органы. В целях проведения расследования пострадавшая сторона должна предоставить в распоряжение следственных органов компьютер, который использовался для доступа в Систему, для проведения экспертизы.

1.3. Термины и определения, используемые в настоящем документе:

- **Злоумышленник** - лицо, которое совершает или совершило заранее обдуманное действие с осознанием его опасных последствий или не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.
- **Злоумышленные действия** – любые действия, совершаемые Злоумышленником в Системе.
- **Угроза** - опасность, предполагающая возможность потерь (ущерба).

- **Риск** - мера, учитывающая вероятность реализации Угрозы и величину потерь (ущерба) от реализации этой Угрозы.
- **Информационная безопасность** - безопасность, связанная с Угрозами в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.
- **Защитная мера** - сложившаяся практика, процедура или механизм, которые используются для уменьшения Риска нарушения Информационной безопасности в Системе.
- **Инцидент** - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию Угрозы Информационной безопасности
- **Риск нарушения информационной безопасности** - Риск, связанный с Угрозой Информационной безопасности.
- **Обработка риска нарушения информационной безопасности** - процесс выбора и осуществления Защитных мер, снижающих Риск нарушения Информационной безопасности, или мер по переносу, принятию или уходу от Риска.

2. Ограничение ответственности Банка

2.1. В связи с тем, что для доступа к услугам дистанционного обслуживания, предоставляемым Банком через Систему, Клиент использует технические и программные средства, не принадлежащие Банку, Банк не несет ответственности за любые, в том числе Злоумышленные, действия третьих лиц в отношении и/или с использованием технических и программных средств, когда-либо использовавшихся Клиентом.

2.2. За пользование нелицензированным программным обеспечением Клиент несет уголовную ответственность в соответствии со статьей 146 УК РФ.

2.3. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы ДБО. Содержимое журнала Системы ДБО используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования Злоумышленных действий.

3. Защитные меры

3.1. Не сообщайте никому, в том числе сотрудникам банка, логины и пароли доступа к ресурсам Банка. Не сообщайте посторонним лицам, в том числе через сеть интернет, историю операций, контактные и учетные данные, так как эти данные могут быть использованы Злоумышленниками для получения доступа к Вашим счетам.

3.2. Не записывайте логин и пароль и не храните их в местах где к ним могут получить доступ посторонние люди.

3.3. Не используйте функцию запоминания логина и пароля в браузерах.

3.4. Не используйте одинаковые логин и пароль для доступа к различным системам.

3.5. Всегда явным образом завершайте сеанс работы с Системой, используя пункт меню «Выход».

3.6. Не рекомендуется использовать чужой компьютер для доступа к Системе ДБО, в случае если доступ к Системе ДБО необходимо осуществить с использованием постороннего компьютера, не рекомендуется сохранять на нем идентификационные данные и другую информацию, а после завершения всех операций нужно убедиться, что идентификационные данные и другая информация не сохранились. После возвращения к штатному персональному компьютеру обязательно смените логин и пароль.

3.7. Если Вы получили на электронную почту письмо с просьбой обновить или предоставить какую-либо информацию со ссылкой на какой-либо сайт или телефон (в том числе – сайт Банка), перезвоните в Службу технической поддержки Банка и сообщите о письме. Банк никогда не просит передать данные для входа в ДБО. Обновление данных осуществляется

только сотрудником Банка в присутствии представителя Клиента, предъявившего документ, удостоверяющего личность. Не открывайте ссылки, указанные в сомнительном письме, в котором Вас просят указать конфиденциальные данные. Не звоните по телефонам, указанным в подобных письмах и не отвечайте на них.

3.8. Не открывайте приложения к письмам от незнакомых отправителей, так как в них могут быть вирусы (вредоносное программное обеспечение), способные украсть ваши идентификационные данные для входа в Систему и ключи ЭП.

3.9. Регулярно, производите смену Пароля.

3.10. При составлении пароля используйте прописные и строчные буквы, цифры, а также различные символы, например: ! / { } [ ] <>. Настоятельно рекомендуется использовать специализированные программы-генераторы паролей.

3.11. Не используйте в качестве пароля имена, памятные даты, номера телефонов.

3.12. Не позволяйте третьим лицам производить за Вас генерацию ключей ЭП.

3.13. Присоединяйте ключевой носитель ЭП к компьютеру непосредственно перед началом работы с Системой ДБО. По окончании работы извлекайте ключевой носитель из компьютера.

3.14. Используйте лицензированное программное обеспечение. ПОМНИТЕ: помимо того, что Вы несете уголовную ответственность за пользование нелицензированным программным обеспечением в соответствии со статьей 146 УК РФ, использование подобного программного обеспечения равноценно предоставлению посторонним лицам доступа на Ваш компьютер.

3.15. Регулярно (не реже раза в неделю) проводите проверку на наличие обновлений операционной системы и программного обеспечения, установленного на компьютере, и обновляйте антивирусные базы. В случае обнаружения вирусов (вредоносного программного обеспечения) на компьютере, после его удаления незамедлительно смените логин и пароль в Системе и произведите замену ключей ЭП.

3.16. Четко регламентируйте порядок использования компьютера, с которого осуществляется взаимодействие с Системой, в том числе список лиц и порядок доступа к компьютеру. Не рекомендуется использовать указанный компьютер для доступа к посторонним сайтам.

3.17. Не устанавливайте на компьютере, который используется для взаимодействия с Системой, постороннее программное обеспечение, например, программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Доказано, что подобные программы передают информацию о содержимом просматриваемых страниц посторонним лицам.

3.18. Не запускайте на своем компьютере программы, полученные из незаслуживающих доверияисточников.

3.19. Используйте межсетевой экран (брандмауэр, firewall), блокирующий передачу нежелательной информации.

3.20. Настройте браузер на использование протокола защищенной связи TLS. Использование протоколов семейства SSL не обеспечивает надлежащей защиты.

3.21. Не храните незашифрованные идентификационные данные на жестком диске, так как эти данные могут быть похищены Злоумышленником и использованы для получения доступа к Вашим счетам.

3.22. Перед вводом своего логина и пароля убедитесь, что Вы установили соединение с легальным сайтом. Проверьте правильность указания адреса сайта, наличие сертификата безопасности. В случае обнаружения подозрительных web-сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официального сайта АКБ «Алмазэргиэнбанк» АО, просьба сообщить об этом по электронной почте sib@albank.ru.

3.23. Настройте механизм информирования о входе в Систему и совершаемых операциях на электронную почту или СМС. Регулярно проверяйте входящие сообщения, а также журнал

операций Системы. Поддерживайте свою контактную информацию в Системе в актуальном состоянии для того, чтобы в случае необходимости с Вами можно было оперативно связаться.

3.24. Не передавайте мобильное устройство третьим лицам, а также храните в недоступном для третьих лиц месте мобильное устройство, на которое поступают СМС-сообщения на ваш мобильный номер оператора связи для подтверждения операций в Системе.

3.25. Не устанавливайте непроверенные мобильные приложения, в частности с неизвестных источников, на мобильное устройство, на которое поступают СМС-сообщения на ваш мобильный номер оператора связи для подтверждения операций в Системе.

3.26. Установите антивирусное приложение на мобильное устройство, на которое поступают СМС-сообщения на ваш мобильный номер оператора связи для подтверждения операций в Системе.

3.27. Обязательно уведомляйте Банк перед сменой номера мобильного оператора связи, на которое поступают СМС-сообщения для подтверждения операций в Системе.

3.28. В случае обнаружения подозрительных действий, совершенных от Вашего имени в Системе, незамедлительно смените логин и пароль, сообщите об инциденте в Службу технической поддержки и произведите смену ключей ЭП.

3.29. В случае обнаружения несанкционированных действий со средствами, находящимися на Ваших счетах, необходимо в максимально короткий срок отозвать сертификат ЭП и оформить заявление на имя Председателя Правления Банка в свободной форме, содержащее максимально подробное описание инцидента, для инициирования расследования. Для проведения расследования необходимо по согласованию со службой информационной безопасности передать в Банк файлы протоколов, подтверждающие установку обновлений операционной системы персонального компьютера и антивирусного программного обеспечения, и в течение 5 (пяти) рабочих дней представить в Службу информационной безопасности Банка для снятия копий документы, подтверждающие факт законного приобретения операционной системы и антивирусного программного обеспечения, а также копию договора об оказании услуг по предоставлению доступа в сеть интернет или иного удостоверяющего факт заключения подобного договора документа (квитанция, чек, счет и тому подобные) и иные документы, которые Клиент сочтет необходимыми для рассмотрения претензии по существу. В случае невозможности представления необходимых файлов и документов об этом делается соответствующая запись на заявлении с указанием причины. Необоснованный отказ в предоставлении требуемых документов может являться основанием для отказа в удовлетворении заявленных Клиентом требований. Решение об обращении в правоохранительные органы Клиент принимает самостоятельно.

Приложения

1. «Памятка для клиентов о действиях в случае обнаружения несанкционированного списания»

Дополнение к Приложению № 3
к «Правилам информационной безопасности
при работе в системе дистанционного
банковского обслуживания «АЭБ Бизнес»

ПАМЯТКА ДЛЯ КЛИЕНТОВ
о действиях в случае обнаружения несанкционированного списания

В случае обнаружения несанкционированного списания со счета Банк рекомендует Клиенту осуществить следующие действия:

1. Максимально оперативно представить письменное заявление в Банк, заверенное печатью и подписью руководителя, по возможности, на бланке организации о факте несанкционированного списания с указанием даты, суммы платежа, других известных Клиенту обстоятельств, а также с просьбой об оказании содействия в возврате несанкционированно списанных денежных средств. Указанное заявление необходимо представить в Банк на бумажном носителе в срок не позднее 2-х рабочих дней с даты устного обращения в Банк.

2. Не использовать компьютеры, которые эксплуатировались для работы в Системе. Их необходимо отключить от сети. С высокой долей вероятности они заражены специализированным вредоносным программным обеспечением, поэтому этот шаг позволит предотвратить последующие инциденты, а также сохранить доказательства для проведения технической экспертизы.

3. Произвести смену ключей шифрования и ключей ЭП, используемых для работы с Системой в соответствии с действующим Договором. **До момента смены ключей работа в Системе будет прекращена в связи с компрометацией действующих средств доступа.**

4. В случае подтверждения операций СМС-сообщениями – заблокируйте мобильное устройство и вытащите SIM-карту, а также попросите выписку СМС-сообщений у мобильного оператора связи и заблокируйте SIM-карту, предварительно уведомив Банк.

5. По факту несанкционированного доступа к компьютерной информации обратиться с заявлением в правоохранительные органы о возбуждении уголовного дела по статьям 272 и 273 УК РФ в связи с созданием, использованием и распространением неустановленными лицами вредоносных компьютерных программ, повлекшим неправомерный доступ неустановленных лиц к Вашей компьютерной информации, что, в свою очередь, привело к несанкционированному Клиентом переводу денежных средств Клиента.

6. С копией указанного заявления с приложением копии талона правоохранительного органа о приеме заявления, обратиться в Арбитражный суд с исковым заявлением в отношение банка-получателя о возврате неосновательного обогащения с ходатайством об аресте похищенной суммы денежных средств на счете получателя в банке получателя и раскрытии персональных данных получателя в целях привлечения его в качестве соответчика (гл. 60 ГК РФ) Если известны полные реквизиты получателя – физического лица, указанный иск подается в суд общей юрисдикции.

7. Копии вышеуказанных обращений в правоохранительные органы и суд с отметками о приеме необходимо предоставить в Банк для того, чтобы Банк мог оказать содействие в возврате несанкционированно списанных средств.

Указанные действия произвести в течение 2-х рабочих дней с даты обнаружения несанкционированного списания в целях оперативного противодействия дальнейшему переводу и обналичиванию денежных средств.

Приложение № 4
К Условиям предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес»

ЗАЯВЛЕНИЕО РАСТОРЖЕНИИ ДОГОВОРАНА ПРЕДОСТАВЛЕНИЕ УСЛУГ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ«АЭБ БИЗНЕС»

1. СВЕДЕНИЯ О КЛИЕНТЕ

Наименование заявителя (далее – Клиент):_____
(указывается полное наименование в соответствии с учредительными документами)
_____

Адрес местонахождения (юридический адрес):_____
_____

(адрес юридического лица, указанный в ЕГРЮЛ; адрес места жительства (места пребывания) индивидуального предпринимателя или физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой)

Почтовый адрес_____
Контактный телефон Клиента: _____
Адрес электронной почты Клиента (e-mail): ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Номер расчетного счета ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Номер договора ДБО №_____ от _____

Клиент является по законодательству Российской Федерации ☐ резидентом ☐ нерезидентом

ИНН/КИО	
КПП	
ОГРН/ОГРНИП	

Настоящим Клиент в лице (уполномоченного представителя Клиента)_____
(должность, фамилия, имя, отчество уполномоченного представителя Клиента)
_____,

действующего (ей)на основании _____
(наименование документа – Устав, Доверенность, иной соответствующий документ)

просит расторгнуть договор на предоставление услуг с использованием системы дистанционного банковского обслуживания « АЭБ-Бизнес» с _____20___ г.

_____ _____ /_____/
Дата *подпись* *Фамилия, И.О.*

М.П. Клиента

2. ЗАПОЛНЯЕТСЯ БАНКОМ

Заявление принял, идентификацию Клиента осуществил, полномочия Клиента/представителя Клиента проверил:

❒Сертификаты ключей проверки электронной подписи отозваны

❒ Отсутствуют

_____ _____ 20___ г. _____ _____/ _____/
дата *Должность сотрудника принявшего Заявлениеподпись* *Фамилия, И.О.*