УТВЕРЖДЕНО

Приказом
Первого Заместителя Председателя Правления
АКБ «Алмазэргиэнбанк» АО
Ф.А. Ноговицыным
от «01» сентября 2022 года № 957

ТИПОВАЯ ФОРМА

Раздел 10 Условий предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ –Бизнес»

Раздел 10Правил 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.

PUSH-сообщение – сообщение, используемое для передачи информации на мобильные устройства под управлением операционных систем iOS, Android OS (по технологиям Apple Push Notification Service и Google Cloud Messaging).

PayControl – программный комплекс, выполняющий функции по взаимодействию с мобильными приложениями, включая регистрацию мобильных устройств Владельцев ключей

УНЭП, отправку ЭД и электронных сообщений. **АБС** - Автоматизированная банковская система комплекс программного и технического обеспечения, направленный на автоматизацию деятельности Банка.

Администратор информационной безопасности – работник Банка, к должностным обязанностям 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 целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, нарушения доступности информации и обеспечения невозможности отказа от совершенных действий.

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

Информационная безопасность – состояние информации, информационных ресурсов и информационных систем, при которых с требуемой вероятностью 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 однозначную аутентификацию Клиента.

Модуль «Расчетный центр Корпорации» (далее –модуль РЦК) – модуль Системы «Клиент-Банк», при использовании которого Уполномоченному лицу Контролирующей организации предоставляется возможность получения информации о движении денежных средств по счетам Клиента и/или Подконтрольных организаций, открытым в Банке – мониторинга, акцепта (бюджетирования), управления счетами.

Мобильное устройство – смартфоны, мобильные телефоны, планшеты и прочие устройства, имеющие доступ к информационно-телекоммуникационной сети «Интернет» (далее - «Интернет»), на которых установлено Мобильное приложение PayControl и которые привязаны к номеру телефона, указанному Клиентом в Заявлении.

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, имитирующих клавиатурный 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 и

подтверждающему реквизиты получателя средств и/или реквизиты плательщика, если он использовался при совершении операции.

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

Удостоверяющий центр (УЦ) – организация, осуществляющая функции по созданию и выдаче Сертификатов ЭП, а также иные функции, предусмотренные законодательством Российской Федерации, аккредитованная в соответствии с требованиями Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи»

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.

УКЭП (усиленная квалифицированная электронная подпись) – электронный аналог подписи от руки. Документ с лектронный аналог подписи от руки. Документ с квалифицированной подписью равнозначен собственноручно подписанному квалифицированной подписью равнозначен собственноручно подписанному

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 электронной форме 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. Для клиентов Банка, присоединившихся к настоящим Условиям ранее 01.06.2022 года, некоторые функции ДБО «АЭБ –бизнес» могут быть недоступны в связи с техническими особенностями Системы. Указанные Клиенты имеют право обратиться в Банк в целях повторного присоединения к настоящим Условиям.

1.4. Заключение Договора 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. Модуль РЦК подключается заключением между Банком и Клиентом двустороннего договора (Приложение №5 к настоящим Условиям)

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

1.8. Стороны обязуются обеспечить допуск к работе в Системе только уполномоченным лицам Клиента в соответствии с Заявлением о присоединении к Условиям.

1.9. 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.

1.10. 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.

1.11. 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.

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

1.13. Стороны признают используемые в Системе средства криптографической защиты информации и используемые Банком и Клиентом ПЭП/PayControl/УНЭП/УКЭП достаточными для защиты ЭД от несанкционированного доступа, а также подтверждения их авторства и подлинности.

1.14. 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.

1.15. 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. Инкассовые поручения в рублях РФ;

2.1.3. Платежное требование;

2.1.4. Запрос на отзыв платежного поручения;

2.1.5. Запрос на отзыв инкассового поручения;

2.1.6. Сообщение свободного формата;

2.1.7. Заявление на выпуск корпоративных карт, их блокировок и установление лимитов;

2.1.8. Заявление на подключение эквайринга;

2.1.9. Заявление на открытие депозита;

2.1.10. Заявление на подключение зарплатного проекта;

2.1.11. Заявление на получение кредита;

2.1.12. Запрос на справку;

2.1.13. Анкета-заявление на кредит Заявление на инкассацию;

2.1.14. Заявление на подключение программы лояльности «Свои»;

2.1.15. Документы по операциям с иностранной валютой (формирование заявок покупки / продажи валюты, обязательной продажи; валютные переводы, в том числе перевод с транзитного счета на валютный; платежи в иностранной валюте; уведомление о поступлении валюты на транзитный счет)

2.1.16. Заявление о постановке на учет контракта / кредитного договора в иностранной валюте, заявление о внесении изменений по контракту / кредитному договору в иностранной валюте , заявление о снятии с учета контракта / кредитного договора в иностранной валюте;

2.1.17. Документы, связанные с расширенным банковским сопровождением контрактов;

2.1.18. Заявление (оферта) на подключение к услуге «Онлайн-зачисления на торговый эквайринг»;

2.1.19. Заявление (оферта) на подключение к услуге «Открытие дополнительного счета»;

2.1.20. Заявление (оферта) на подключение к услуге «Открытие отдельного (обособленного) банковского счета»;

2.1.21. Заявление (оферта) на подключение к услуге «Подключение к пакету РКО»;

2.1.22. Заявление (оферта) на подключение к услуге «QR - эквайринг (подключение)»;

2.1.23. Заявление (оферта) на подключение к услуге «Торговый эквайринг (подключение)»;

2.1.24. Заявление (оферта) на подключение к услуге «Инкассация»;

2.1.25. Заявления на присоединения к иным услугам Банка и его партнеров;

2.1.26. Письма и обращения.

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. Инкассовое поручение в валюте РФ - – заполняется в порядке, определенном в экранной форме подсистемы «Клиент»;

2.2.3. Запрос на отзыв платежного поручения - заполняется в порядке, определенном в документации подсистемы «Клиент»;

2.2.4. Запрос на выписку по счету - заполняется в порядке, определенном в документации подсистемы «Клиент»;

2.2.5. Сообщение свободного формата может включать любой текст (например, согласие на акцепт) и любой прикрепленный файл;

2.2.6. Валютный перевод – заполняется в порядке, определенном в документации подсистемы «Клиент»;

2.2.7. Покупка валюты – заполняется в порядке, определенном в документации подсистемы «Клиент»;

2.2.8. Продажа валюты – заполняется в порядке, определенном в документации подсистемы «Клиент».

2.2.9. Заявление на выпуск корпоративных карт – заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями

2.2.10. Заявление на подключение эквайринга – заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями

2.2.11. Заявление на открытие депозита – заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями

2.2.12. Заявление на подключение зарплатного проекта – заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями

2.2.13. Заявление на кредит – заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями

2.2.14. Заявление на инкассацию – заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями

2.2.15. Заявление на подключение программы лояльности «Свои» - заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями;

2.2.16. Заявление (оферта) на подключение к услуге «Онлайн-зачисления на торговый эквайринг» - заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями;

2.2.17. Заявление (оферта) на подключение к услуге «Открытие дополнительного счета» - заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями;

2.2.18. Заявление (оферта) на подключение к услуге «Открытие отдельного (обособленного) банковского счета» - заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями;

2.2.19. Заявление (оферта) на подключение к услуге «Подключение к пакету РКО» - заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями;

2.2.20. Заявление (оферта) на подключение к услуге «QR - эквайринг (подключение)» - заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями;

2.2.21. Заявление (оферта) на подключение к услуге «Торговый эквайринг (подключение)» - заполняется в формате электронных бланков документов, в соответствии с банковскими требованиями»;

2.2.22. Заявление (оферта) на подключение к услуге «Инкассация»;

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.).

2.3.5. При подключении Клиента в качестве Партнера в рамках программы лояльности «СВОИ» - счета на возмещение выплаченного Банком кешбэка, предоставлять информацию о выплаченных Держателям суммах кешбэка с каждой оплаченной покупки по установленной форме.

2.3.6. Сведения о валютных операциях ,

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.

2.5. Иные документы, сведения и информация, оформление которых возможно с использованием Системы «АЭБ-Бизнес»:

- подписание двухсторонних договоров с Банком с использованием аналогово собственноручной подписи

- взаимодействие с Банком в рамках осуществления зарплатного проекта (зарплатный договор, реестр на присоединение физического лица к зарплатному договору , ведомость зачисления на карты сотрудников).

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, только для Рутокена (Банк вправе разместить указанные драйвера 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.

3.3.1.4. Код активации и QR-код для PayControl.

3.3.2. Требования к программно-техническим средствам при использовании электронного ключа:

3.3.2.1. Персональный компьютер с операционной системой, поддерживаемой браузерами из списка: InternetExplorer 11 и выше; Firefox актуальной версии; Safari9 и выше;

Opera и GoogleChrome актуальной версии. Задание для СИБ или в УИТ (УИР), обновить данные

3.3.2.2. Канал доступа в Интернет;

3.3.2.3. Свободный USB порт.

3.3.2.4. Драйвера для электронного ключа Рутокен.

3.3.2.5. На Мобильном устройстве должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности): операционная система (iOs, Android), антивирусное программное обеспечение (если операционная система подвержена вирусным атакам).

3.3.2.6. Мобильное устройство не должно быть подвергнуто операциям взлома операционной системы (jail-break, rooting).

3.3.2.7. Клиент должен использовать процедуру доступа к Мобильному устройству путем ввода пароля, либо биометрических данных.

3.3.2.8. Мобильное приложение PayControl, установленное с официальных сервисов AppStore и Google Play.

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 доступа Ответственным сотрудникам 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 или PUSH-уведомлений. При каждом подписании документа/сообщения в Системе, Система запрашивает одноразовый пароль, который Уполномоченное лицо Клиента получает на мобильный телефон посредством SMS-сообщения или PUSH-уведомления. SMS-сообщение или PUSH-уведомление с одноразовым паролем содержит основные реквизиты подписываемого документа/сообщения, которые Клиент обязан проверять.

- с использованием УНЭП, формируемой клиентом и хранимом на устройстве «Электронный ключ».

- с использованием PayControl. На Мобильное устройство Клиента поступает PUSH-сообщение о необходимости подписания документа/сообщения. Уполномоченное лицо Клиента обязано проверять основные реквизиты документа/сообщения в мобильном приложении АЭБ-Бизнес или PayControl.

- с использованием УКЭП.

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;
- своевременное извещение Банка в случае утраты/смены Мобильного устройства, SIM-карты.
- 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;
- запросы на регистрацию сертификатов ключей УКЭП;
- отзывает существующие сертификаты ключей УНЭП;
- отзывает существующие сертификаты ключей УКЭП;
- блокирует учетные записи/сертификаты ключей ПЭП/УНЭП/УКЭП клиентов в Системе;
- участвует в процедуре проверки ПЭП/УНЭП/УКЭП 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/УКЭП 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, на присутствие 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/УКЭП 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/УКЭП и отправка ЭД в Банк с использованием Системы. В зависимости от принятой Клиентом технологии, если используется вторая ЭП второго Уполномоченного лица, Клиент подписывает ЭД и второй своей ПЭП/УНЭП. ПЭП/УНЭП/УКЭП подтверждает авторство отправленного по Системе документа и гарантирует его целостность, так как любое изменение в документе после его подписания сделает ПЭП/УНЭП/УКЭП недействительным.

5.5. Основанием для принятия к исполнению Банком переданного Клиентом по Системе платежного документа является аутентификация соединения Клиента, а также наличие и корректность необходимого количества ПЭП/УНЭП/УКЭП, 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 ЭД служат:

-отрицательный результат проверки подлинности ПЭП/УНЭП/УКЭП;

-отсутствие ПЭП/УНЭП/УКЭП 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 Системы в 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/УКЭП.

6.2. Ответственному сотруднику 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. Ответственный сотрудник Клиента может самостоятельно изготовить (привязать) действующий УКЭП ключ 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).

6.5. 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.

6.6. Клиент признаёт метод шифрования информации и ЭП, используемую для передачи документов между Банком и Клиентом.

6.7. 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.

6.8. 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.

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

6.10. 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.

6.11. 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).

6.12. 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.

6.13. 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.

6.14. Стороны признают:

- в соответствии с настоящими Условиями Сторонами может использоваться простая электронная подпись (ПЭП) и/или усиленная неквалифицированная электронная подпись (УНЭП) и/или усиленная квалифицированная электронная подпись (УКЭП)

- 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 УНЭП ЭД 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 Системе ЭД, 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 и осуществлять платежи только в пределах этого остатка. Настоящий пункт не применяется при наличии дополнительного соглашения к договору банковского счета о кредитовании счета путем предоставления кредита в форме «овердрафт».

8.2.4. Обеспечивать защиту клиентского модуля Системы от несанкционированного 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» АО размещенного на официальном сайте Банка www.albank.ru.

8.2.6. При уведомлении Банком о необходимости смены программного обеспечения осуществить все необходимые действия для своевременного получения и установки новой версии 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 акцептом Клиента Банку на списание причитающегося ему вознаграждения и иных сумм по настоящему Договору, который предоставлен без ограничения по количеству расчетных документов Банка, выставляемых в соответствии с условиями настоящего Договора, а также без ограничения по сумме 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 вопросам эксплуатации Системы (функционирование Системы ДБО, использование средств защиты и передачи/приема информации, технология обработки информации). Контакты и режим работы служб Банка, задействованных в подключении и сопровождении Клиента при обслуживании 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 Системе ЭД Клиента, признанные равнозначными документу на бумажном носителе, подписанному собственноручной подписью, оформленные и подписанные (заверенные) Клиентом в соответствии с Условиями, а также осуществлять обработку и исполнение таких ЭД Клиента в строгом соответствии с установленными нормами, техническими требованиями, стандартами, нормативными актами Банка России и нормативными документами Банка.

8.3.6. Обеспечивать защиту банковского модуля Системы от несанкционированного 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 основании заранее данного акцепта с формированием расчетных документов (в том числе банковского ордера) плату за осуществление дистанционного банковского обслуживания Клиента в соответствии 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 использованием Системы путем формирования и направления Клиенту выписки по счету с использованием 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 Договору Стороны 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 Системы без 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» АО размещенного 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, УНЭП или УКЭП 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, мобильного устройства 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 Системы и 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 или УКЭП и сертификатов ключей проверки УНЭП или УКЭП осуществляются в соответствии с настоящими Условиями.

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

При смене ключей УНЭП или УКЭП 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 УКЭП 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 5 (пять) 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 он представляет в Банк письменное заявление с указанием предполагаемой даты расторжения Договора. В случае если Стороной инициатором расторжения является Банк, то он направляет Клиенту соответствующее уведомление с указанием предполагаемой даты расторжения Договора, но не менее чем за 15 календарных дней до даты такого расторжения.

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 ключ (e-token) ❒Электронный ключ (Pay Control) ❒ Электронный ключ (УКЭП)
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 ключ (e-token) ❒Электронный ключ (Pay Control) ❒ Электронный ключ (УКЭП)

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

5. **Прошу направить Логин и Пароль от Системы на номер телефона**
+7_____

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 ЭП (сертификата) для обмена сообщениями

Настоящим Актом признаётся ключ шифрования, принадлежащий уполномоченному представителю:

ФИО владельца сертификата: _____

Организация _____

Дата начала срока действия сертификата _____

Дата окончания срока действия сертификата _____

Ключ ЭП создан с использованием СКЗИ _____

Идентификатор ключа _____

Серийный номер сертификата _____

Местонахождение _____

Хранилище ключевой информации _____

Момент генерации ключа _____

_____

Достоверность приведенных данных подтверждаем

Владелец сертификата _____

_____ / _____ /

Руководитель компании (первая подпись согласно карточке образцов подписей) _____

_____ / _____ /

От Банка
_____/_____/
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.*

Приложение № 5
К Условиям предоставления услуг с использованием системы дистанционного банковского обслуживания «АЭБ Бизнес»

СОГЛАШЕНИЕ О ПРЕДОСТАВЛЕНИИ УСЛУГИ «РАСЧЕТНЫЙ ЦЕНТР КОРПОРАЦИИ»

г. Якутск «___» _____ 20__ г.

Акционерный Коммерческий Банк «Алмазэргиэнбанк» Акционерное общество, именуемый в дальнейшем **«БАНК»**, в лице Председателя Правления Банка Долгунова Николай Николаевича, действующей на основании Устава, с одной стороны, и _____(полное официальное наименование юридического лица) именуемое в дальнейшем «Контролирующая организация»/«Клиент», в лице _____

_____

(должность, фамилия, имя, отчество)

действующего на основании _____

с другой стороны, вместе именуемые «Стороны», заключили настоящее соглашение (далее по тексту – Соглашение) о нижеследующем:

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированное рабочее место «Расчетный Центр Корпорации» / АРМ РЦК – составная часть Системы РЦК, которая устанавливается на рабочем месте Контролирующей организации и является рабочим местом Контролирующей организации в Системе РЦК.

Банк - Акционерный Коммерческий Банк «Алмазэргиэнбанк» Акционерное общество, АКБ «Алмазэргиэнбанк» АО (ОГРН 1031403918138, Генеральная лицензия Банка России №2602, адрес местонахождения: 677000, Российская Федерация, Республика Саха (Якутия), г. Якутск, пр. Ленина, д. 1).

Бюджет – смета расходов, которая утверждается строго на определенный период времени. В Системе РЦК представляет собой набор строк из Классификатора (утвержденный соответствующим уполномоченным сотрудником или органом Контролирующей организации перечень аналитических признаков, в разрезе которых происходит учет, планирование, мониторинг и контроль финансовых показателей), выделенный Контролирующей организацией по каждому Счету Подконтрольной организации с указанием следующих параметров:

- лимит / отсутствие лимита;
- период планирования;
- механизм акцептования.

Договор о предоставлении услуг с использованием Системы ДБО – соглашение между Банком и Клиентом, определяющее порядок предоставления Банком услуг по подключению и обслуживанию Клиента в Системе ДБО, заключенное путем подачи Клиентом в Банк заявления о присоединении в порядке, предусмотренном Правилами комплексного банковского обслуживания юридических лиц, индивидуальных предпринимателей, а также физических лиц, занимающихся в установленном законодательством порядке частной практикой, в АКБ АЛМАЗЭРГИЭНБАНК АО.

Заявление – заявление на предоставление/изменение услуги по форме Приложения №1 к настоящему Соглашению, оформляемое Контролирующей организацией с целью выбора соответствующей Услуги и впоследствии ее оказания.

Идентификация - совокупность мероприятий Банка по установлению определенных законодательством Российской Федерации сведений о Клиентах, их Представителях, Выгодоприобретателях, Бенефициарных владельцах, по подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий.

Классификатор – это параметр, который определяется Контролирующей организацией для ведения Бюджета и анализа поступившего платежного поручения.

Контролирующая организация – юридическое лицо, осуществляющее функции мониторинга и контроля движения денежных средств, акцепта/отказа от акцепта платежных поручений по счетам своих Подконтрольных организаций в порядке, определенном настоящим Соглашением.

Логин – имя Уполномоченного лица Контролирующей организации в Системе РЦК, а именно - уникальная последовательность цифр, символов или латинских букв (строчных), определяемая Уполномоченным лицом самостоятельно, которая необходима для его аутентификации в Системе РЦК.

Мониторинг – прямой доступ Контролирующей организации ко всем (или выбранной части) платежным операциям Подконтрольных организаций в режиме реального времени, т.е. мониторинг всех платежных поручений Подконтрольных организаций, оперативная информация о платежах, контроль за движением денежных средств.

Подконтрольная организация – юридическое лицо, индивидуальный предприниматель, филиал Контролирующей организации, имеющие расчетный(-ые) счет(-а) в Банке, подключенные к Системе ДБО и предоставившие Контролирующей организации право контроля и управления денежными средствами, находящимися на их счетах в порядке, определенном настоящим Соглашением.

Сайт – официальный интернет-сайт Банка www.albank.ru.

Система «АЭБ Бизнес» – система электронного документооборота между Банком и Клиентом, предназначенная для клиентов микро и малого бизнеса, не требующая установки специализированного программного обеспечения на рабочее место Клиента, работа Клиента производится посредством браузера.

Система «Расчетный Центр Корпорации» / Система РЦК – информационная система, предназначенная для осуществления Контролирующей организацией контроля управления денежными средствами, находящимися на счетах Подконтрольных организаций.

Справочник подтвержденных контрагентов – справочник с реквизитами контрагентов, используемый для проверки исполнения Бюджета по контрагенту.

Счета Подконтрольных организаций – расчетные счета, открытые в Банке Подконтрольными организациями в валюте Российской Федерации и перечисленные в Заявлении.

Тарифы – Тарифы АКБ «Алмазэргиэнбанк» АО для корпоративных клиентов, включают устанавливаемые Банком ставки комиссионного вознаграждения, взимаемого с Клиента за оказание услуг Банка при осуществлении расчетов, а также иные условия, которые устанавливаются в Тарифах. Тарифы Банка размещены на официальном сайте Банка в сети интернет по адресу www.albank.ru и информационных стендах Банка по месту обслуживания Клиента.

Уполномоченное лицо Контролирующей организации – работник Контролирующей организации, уполномоченный распоряжаться денежными средствами и совершать иные действия, предусмотренные настоящим Соглашением, используя ЭП, а также работник Контролирующей организации, наделенный полномочиями по подготовке документов в Системе РЦК.

Услуга – услуга под названием «Расчетный Центр Корпорации», которая оказывается Банком Контролирующей организации в соответствии с условиями настоящего Соглашения. Выбор варианта Услуги из перечня, приведенного в п. 1.2 настоящего Соглашения, осуществляется Контролирующей организацией самостоятельно посредством оформления Заявления.

Электронный документ – электронный образ документа (платежного или иного), представленный в согласованном Сторонами формате, определяемом программными средствами создания документа. Электронный документ передается между Сторонами в составе файла, подписанного ЭП. В состав файла может входить несколько электронных документов. Если файл имеет корректную ЭП, то каждый электронный документ, входящий в файл, считается подписанным ЭП.

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. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. В соответствии с условиями настоящего Соглашения Банк обязуется оказать Контролирующей организации Услугу, указанную в п. 1.2. настоящего Договора, а Контролирующая организация обязуется оплатить данную Услугу в соответствии с тарифами Банка, размещенными на Сайте Банка.

1.2. В рамках оказываемой по настоящему Соглашению Услуги Банк предоставляет Контролирующей организации возможность по ее выбору осуществления следующих действий в отношении Счетов Подконтрольных организаций:

1.2.1. получение Контролирующей организацией информации по Счетам Подконтрольных организаций;

1.2.2. осуществление дополнительного акцепта/отказа от акцепта Контролирующей организацией электронных платежных поручений Подконтрольных организаций;

1.2.3. осуществление контроля над расходными операциями Подконтрольных организаций по Счетам Подконтрольных организаций, согласно п. 2.1.6 настоящего Соглашения, путем ведения Бюджета/сметы расходов.

1.3. Услуга предоставляется с использованием Системы РЦК в порядке, установленном настоящим Соглашением.

1.4. Выбор варианта Услуги, указанного в п. 1.2 настоящего Соглашения, осуществляется Контролирующей организацией посредством оформления Заявления.

2. УСЛОВИЯ И ПОРЯДОК ОКАЗАНИЯ УСЛУГИ

2.1. Услуга оказывается Контролирующей организации при наличии в совокупности следующих условий:

2.1.1. Подконтрольные организации заключили с Банком договоры банковского счета в валюте Российской Федерации по всем расчетным счетам, указанным в Заявлении.

2.1.2. Подконтрольные организации заключили с Банком Договор о предоставлении услуг с использованием Системы ДБО по всем Счетам, указанным в Заявлении.

2.1.3. Подконтрольными организациями, указанными в Заявлении, в зависимости от выбранной Контролирующей организацией функциональной возможности в соответствии с п. 1.2 настоящего Соглашения заключены дополнительные соглашения к договору банковского счета (Приложение 2а, 2б, 2в к настоящему Соглашению). В случае прекращения действия указанных дополнительных соглашений Банк в одностороннем порядке прекращает оказание Услуги Контролирующей организации. В случае прекращения оказания Банком Услуги Контролирующей организации прекращают действие все указанные дополнительные соглашения к договору банковского счета, заключенные между Банком и Подконтрольной организацией.

2.1.4. Контролирующая организация имеет необходимые программно-технические средства, отвечающие требованиям настоящего Соглашения.

2.1.5. Услуга оказывается в отношении распоряжений о переводе денежных средств, составляемых Подконтрольными организациями в электронном виде.

2.1.6. Оказание Услуги, указанной в п. 1.2.2, п. 1.2.3 настоящего Соглашения, с использованием АРМ РЦК возможно только при наличии у Уполномоченных лиц Контролирующей организации действующих ключей ЭП, зарегистрированных и используемых в соответствии с настоящим Соглашением, и наличии в Банке документов, подтверждающих полномочия Уполномоченных лиц Контролирующей организации на работу в Системе РЦК.

2.1.7. В случае если Контролирующая организация не имеет открытого счета в Банке, то Контролирующая организация предоставляет в Банк комплект документов для идентификации в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Документы должны быть предоставлены в Банк до заключения настоящего Соглашения и оказания Услуги. В случае не предоставления Контролирующей организацией Банку комплекта документов в соответствии с настоящим пунктом либо ненадлежащего предоставления (не в полном объеме), Банк вправе отказать Контролирующей организации в заключении настоящего Соглашения и оказании Услуги.

В случае если после заключения настоящего Соглашения и в процессе оказания Услуги возникнет необходимость (в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма или по требованию Банка в иных случаях) предоставления Контролирующей организацией Банку дополнительных документов к указанному комплекту документов и в случае не предоставления Контролирующей организацией Банку необходимых документов в соответствии с настоящим пунктом либо ненадлежащего предоставления (не в полном объеме), Банк вправе отказать Контролирующей организации в оказании Услуги и расторгнуть настоящее Соглашение в одностороннем порядке по

истечению 30 (Тридцати) календарных дней с момента такого отказа либо ненадлежащего предоставления.

2.2. Оказание Услуги реализуется на базе специального программного обеспечения АРМ РЦК, установка которого производится на рабочее место Контролирующей организации, которое должно соответствовать техническим требованиям Банка, указанным в Приложении №3 к настоящему Соглашению.

2.3. Контролирующая организация самостоятельно и за свой счет приобретает программно-технические средства, предусмотренные в Приложении №3 к настоящему Соглашению, обеспечивает подключение к сети Интернет, а также обеспечивает защиту собственных вычислительных средств и электронных ключей от несанкционированного доступа и вредоносного программного обеспечения.

2.4. Контролирующая организация соглашается с оказанием Услуги через сеть Интернет. Контролирующая организация осознает, что сеть Интернет не является безопасным каналом связи, и соглашается нести все риски, связанные с подключением его вычислительных средств к сети Интернет, возможным нарушением конфиденциальности и целостности информации при работе через сеть Интернет. Стороны также признают, что выход из строя АРМ РЦК, установленного у Контролирующей организации, в результате вмешательства третьих лиц через сеть Интернет рассматривается как выход из строя по вине Контролирующей организации.

2.5. Банк осуществляет оказание Услуги/прекращение оказания Услуги на основании настроек, указанных Контролирующей организацией в Заявлении.

2.6. Стороны признают используемую ими по настоящему Соглашению систему защиты информации, которая обеспечивает контроль целостности и аутентификацию посредством шифрования и ЭП, достаточной для защиты от несанкционированного доступа, а также для подтверждения авторства и подлинности Электронных документов. Обмен открытыми ключами ЭП оформляется документом «Сведения об открытом ключе абонента» (по форме, определенной в интерфейсе Системы РЦК). ЭП используются Сторонами с даты, указанной в Сведениях об открытом ключе абонента. Датой ввода в действие открытого ключа ЭП считается дата регистрации открытого ключа в Центре регистрации ключей Банка.

2.7. Подтверждение операций в АРМ РЦК осуществляется с использованием ЭП.

2.8. Контролирующая организация самостоятельно формирует свои ключи ЭП в АРМ РЦК.

2.9. При выборе Контролирующей организацией Услуг в рамках п. 1.2.1 настоящего Соглашения:

2.9.1. Банк предоставляет Контролирующей организации в лице Уполномоченных лиц Контролирующей организации информацию по Счетам Подконтрольных организаций.

2.9.2. Информация по Счетам Подконтрольных организаций предоставляется Контролирующей организации в виде Электронных документов, передаваемых с использованием Системы ДБО, без последующего представления на бумажном носителе.

2.9.3. Уполномоченным лицам Контролирующей организации предоставляется доступ к Счетам Подконтрольных организаций с правом просмотра за движением денежных средств по данным счетам, 5 просмотра распоряжений Подконтрольных организаций о переводе денежных средств, но без права дополнительного акцепта/отказа от акцепта.

2.10. При выборе Контролирующей организацией Услуги в рамках п. 1.2.2, п. 1.2.3 настоящего Соглашения:

2.10.1. Формирование (ввод или импорт из автоматизированной системы Контролирующей организации и его подразделений) платежного поручения Подконтрольными организациями осуществляется в Системе ДБО.

2.10.2. Подписание ЭП платежного поручения Подконтрольной организации осуществляется в Системе ДБО, что подтверждается соответствующими статусами в Системе ДБО.

2.10.3. После успешного подписания платежного поручения в Системе ДБО ЭП, оно направляется в АРМ РЦК и становится доступным для дальнейшей его обработки.

2.10.4. При оказании Услуги в соответствии с п. 1.2.2, п. 1.2.3 настоящего Соглашения Контролирующей организацией производится автоматический акцепт/отказ от акцепта или предоставляется право ручного акцепта/отказа от акцепта. В данном случае под ручным акцептом Контролирующей организации понимается визирование/подписание платежного поручения Подконтрольной организации в Системе РЦК ЭП Уполномоченного лица для его исполнения Банком, то есть Контролирующая организация визирует платежное поручение своей ЭП и платежное поручение направляется в Банк для исполнения. В Системе РЦК визирование платежного поручения производится не более чем 2 (Двумя) Уполномоченными лицами Контролирующей организации, при

многоуровневом визировании (акцепте) – не более 5 (Пятью) Уполномоченными лицами Контролирующей организации. Под автоматическим акцептом понимается акцепт, совершаемый в Системе РЦК без проставления ЭП Уполномоченным лицом Контролирующей организации. При ручном отказе в АРМ РЦК платежное поручение не исполняется Банком. Под ручным отказом понимается действие, при котором Контролирующая организация отказывает в исполнении платежного поручения и такой документ не подлежит направлению в Банк для исполнения. Под автоматическим отказом от акцепта понимается отказ от акцепта, совершаемый в Системе РЦК без проставления ЭП Уполномоченным лицом Контролирующей организации. При ручном или автоматическом акцепте в АРМ РЦК платежное поручение выгружается на обработку в Банк. Контролирующая организация самостоятельно формирует путем ввода в АРМ РЦК или загрузки из автоматизированных систем Контролирующей организации значения лимитов по строкам Бюджета в разрезе периодов планирования.

2.10.5. Автоматический акцепт/отказ от акцепта в рамках оказания Услуги в соответствии с п. 1.2.2, п. 1.2.3 настоящего Соглашения должен быть предоставлен Контролирующей организацией Банку не позднее следующего рабочего дня со дня поступления для акцепта платежного поручения.

2.10.6. Ручной акцепт/отказ от акцепта в рамках оказания Услуги в соответствии с п. 1.2.2, п. 1.2.3 настоящего Соглашения должен быть предоставлен Контролирующей организацией Банку в течение 3 (Трех) рабочих дней со дня поступления на рассмотрение платежного поручения.

2.10.7. В случае не поступления от Контролирующей организации акцепта/отказа от акцепта, платежное поручение Подконтрольной организации не направляется в Банк и не подлежит исполнению.

2.10.8. Контролирующая организация самостоятельно ведет справочник контрагентов путем ввода данных по каждому контрагенту в АРМ РЦК или путем импорта файла с перечнем контрагентов определенного для РЦК CSV формата.

2.11. При выборе Контролирующей организацией Услуги в рамках п. 1.2.3 настоящего Соглашения: 2.11.1. При использовании функциональных возможностей, описанных в п. 1.2.3 настоящего Соглашения, в Системе ДБО необходимо в справочнике КБК выбрать код статьи Бюджета, в рамках которой необходимо провести платеж.

2.11.2. При выборе Контролирующей организацией функциональных возможностей в соответствии с п. 1.2.3 настоящего Соглашения Контролирующая организация обязана обеспечить формирование лимита средств по каждой из строк Бюджета и установку лимитов по строкам Бюджета в АРМ РЦК в соответствии с установленными в Системе РЦК правилами, не позднее дня, предшествующего первому дню периода планирования.

2.11.3. В зависимости от настроек, предварительно выполненных в Системе РЦК в соответствии с п. 1.2.3 настоящего Соглашения, платежное поручение проходит (не проходит) проверку на соответствие статье Бюджета и на остаток лимита по строке Бюджета.

2.12. Подробное описание Услуги в рамках п. 1.2.2, п. 1.2.3 настоящего Соглашения, оказываемых Банком, представлено в Руководстве пользователя к Системе РЦК.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Взаимные обязанности Сторон.

3.1.1. Каждая Сторона обязана за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые для работы в Системе РЦК в соответствии с настоящим Соглашением.

3.1.2. Стороны обязуются не разглашать третьим лицам, за исключением случаев, предусмотренных действующим законодательством Российской Федерации или дополнительным соглашением Сторон, конкретные способы защиты информации, реализованные в используемой по настоящему Соглашению Системе РЦК.

3.1.3. Стороны обязуются сохранять в тайне применяемые в системе защиты информации секретные ключи. Смена ключей производится каждый раз при изменении состава лиц, работающих с системой защиты информации в Системе РЦК, а также в случаях компрометации ключа одной из Сторон.

3.1.4. Каждая из Сторон обязуется немедленно, не позднее следующего рабочего дня, информировать другую Сторону обо всех случаях компрометации секретных ключей, их утраты, хищения, несанкционированного использования, а также повреждения программно-технических средств подсистем обработки, хранения, защиты и передачи информации. При этом работа в Системе

РЦК приостанавливается и возобновляется только после проведения внеплановой смены ключей и других согласованных действий по поддержанию Системы РЦК в рабочем состоянии.

3.1.5. Стороны, после введения программно-технических средств в эксплуатацию, генерации ключей системы защиты информации оформляют Сведения об открытом ключе абонента передачи и ввода в действие открытого ключа ЭП (по форме, определенной в интерфейсе Системы РЦК).

3.2. Контролирующая организация обязана:

3.2.1. Производить оплату Банку всех комиссий, вознаграждений и расходов, вызванных подключением, установкой, обслуживанием Системы РЦК в порядке, предусмотренном п. 5.2 настоящего Соглашения.

3.2.2. Обеспечить заключение Подконтрольными организациями дополнительных соглашений к договорам банковского счета, указанных в п. 2.1.3 настоящего Соглашения.

3.2.3. Получить от Банка после подписания настоящего Соглашения указанные в Приложении №1 программно-технические средства.

3.2.4. В течение 10 (Десяти) рабочих дней с момента заключения настоящего Соглашения ввести в эксплуатацию программно-технические средства в соответствии с требованиями, указанными в Приложении №3 к настоящему Соглашению, для обеспечения работы в АРМ РЦК. Банк вправе отказаться от выполнения своих обязательств по настоящему Соглашению, расторгнув его в одностороннем порядке, в случае несоблюдения Контролирующей организацией указанного срока.

3.2.5. В Заявлении указать Уполномоченных лиц, а также необходимую информацию, в том числе Логин, для первичной регистрации Уполномоченных лиц в Системе РЦК.

3.2.6. Своевременно, но не позднее следующего рабочего дня, уведомить Банк о наступлении обстоятельств, влекущих изменение настоящего Соглашения.

3.2.7. При расторжении настоящего Соглашения или прекращении его действия по иным основаниям прекратить использование АРМ РЦК и не передавать его третьим лицам.

3.2.8. Соблюдать требования правил информационной безопасности, изложенных в «Инструкции Клиента по обеспечению информационной безопасности», опубликованной на Сайте Банка.

3.2.9. Исключить возможность заражения компьютера с установленной Системой ДБО программными вирусами и другими вредоносными программами.

3.2.10. Обеспечить доступ сотрудников Банка для осмотра оборудования Контролирующей организации, на котором установлена Система ДБО, в случае возникновения спора между Сторонами, связанных с исполнением настоящего Соглашения.

3.2.11. Направить в случае утраты/выхода из строя/несанкционированного использования (без согласия Контролирующей организации)/ блокировки ЭП/смены уполномоченного лица письменное уведомление Банку для блокировки электронного ключа, используемого при проведении расчетных операций в электронной форме.

3.2.12. Производить плановую перегенерацию ключей ЭП до истечения одного года с даты последней генерации ключей ЭП, а также выполнять процедуру перегенерации при проведении внеплановой замены ключей ЭП, смене лиц, уполномоченных работать в Системе РЦК.

3.2.13. Контролирующая организация обязуется уведомить Банк о прекращении действия полномочий Уполномоченных лиц и запретить им подписывать и отправлять в Банк электронные платежные поручения.

3.2.14. Контролирующая организация обязуется своевременно, но не позднее следующего рабочего дня, уведомить Банк в случае изменения состава Уполномоченных лиц, имеющих право подписи или изменения их прав доступа, предоставив в Банк Заявление на изменение Услуги по форме Приложения №1 к настоящему Соглашению.

3.2.15. Не разглашать и не передавать другим лицам (обеспечить конфиденциальность) информацию, связанную с использованием Системы РЦК, за исключением случаев, предусмотренных действующим законодательством Российской Федерации и условиями настоящего Соглашения.

3.2.16. При установлении возможности нарушения безопасности Системы РЦК, выявлении фактов или признаков таких нарушений, немедленно приостановить использование Системы РЦК и оповестить Банк любым доступным способом.

3.2.17. Не допускать тиражирования и передачи третьим лицам программного обеспечения, поставляемого Банком по настоящему Соглашению.

3.2.18. Довести до сведения Подконтрольной организации содержание и условия настоящего Соглашения.

3.2.19. До осуществления операций в Системе РЦК ознакомиться с Руководством пользователя, размещенном в Системе РЦК.

3.2.20. Обеспечить предоставление в Банк лицом, указанным в преамбуле настоящего Соглашения, лицом, подписавшим Заявление (уполномоченным представителем Клиента), действующих от имени Контролирующей организации, Уполномоченным лицом Контролирующей организации Согласия субъекта на обработку персональных данных по форме Приложения №5 к настоящему Соглашению до заключения настоящего Соглашения и оказания Услуги.

3.3. Банк обязан:

3.3.1. Надлежащим образом оказывать Контролирующей организации Услугу в соответствии с настоящим Соглашением.

3.3.2. В соответствии с Заявлением на изменение Услуги по форме Приложения №1 к настоящему Соглашению, вносить соответствующие изменения в параметры работы Системы РЦК при наличии технической возможности.

3.3.3. Исполнять акцептованные и оформленные должным образом электронные платежные поручения Подконтрольных организаций в соответствии с настоящим Соглашением.

3.3.4. Организовать работу по предоставлению информации по Счетам Подконтрольных организаций в срок не позднее 3 (Трех) рабочих дней с момента ввода Контролирующей организацией в эксплуатацию программно-технических средств для обеспечения работы в АРМ РЦК.

3.3.5. По мере необходимости осуществлять консультирование и поддержку Контролирующей организации по вопросам эксплуатации АРМ РЦК.

3.3.6. Организовать внутренний режим функционирования входящих в Систему РЦК рабочих мест Банка таким образом, чтобы исключить возможность использования Системы РЦК и ключей ЭП лицами, не имеющими допуска к работе с Системой РЦК.

3.4. Банк вправе:

3.4.1. Списывать комиссию за оказываемую Банком по настоящему Соглашению Услугу в соответствии с тарифами Банка, в порядке, установленном п. 5.2 настоящего Соглашения.

3.4.2. При неисполнении или ненадлежащем исполнении Контролирующей организацией своих обязательств по оплате Услуг Банк имеет право в одностороннем порядке расторгнуть настоящее Соглашение в порядке, предусмотренном п. 6.3 настоящего Соглашения.

3.4.3. Производить замену программного обеспечения Системы РЦК без согласия Контролирующей организации. Банк обязан уведомить об этом Контролирующую организацию не менее чем за 7 (Семь) рабочих дней до даты замены, а Контролирующая организация обязана в соответствующий срок получить у Банка или приобрести за свой счет и ввести в эксплуатацию необходимые программные средства.

3.4.4. Отказать Контролирующей организации в оказании Услуги в случае нарушений со стороны Контролирующей организации условий настоящего Соглашения, в том числе в случае несоблюдения условий оказания Услуги в соответствии с п. 2.1 настоящего Соглашения.

3.4.5. Вносить в одностороннем порядке изменения в установленные тарифы Банка с последующим уведомлением Контролирующей организации в течение 7 (Семи) рабочих дней. Извещение Контролирующей организации о внесенных изменениях осуществляется путем направления электронного сообщения по Системе ДБО и/или путем размещения соответствующей информации на Сайте Банка.

3.4.6. Под изменением тарифов понимается изменение размера тарифов, сроков взимания комиссионного вознаграждения, а также введение тарифов за иные услуги и операции.

3.4.7. Раскрывать содержание и условия настоящего Соглашения Подконтрольной организации.

3.4.8. Хранить и обрабатывать, в том числе, автоматизировано, любую информацию, относящейся к персональным данным Клиента/Представителя Клиента, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, предоставленных Банку в связи с заключением настоящего договора в целях исполнения договорных обязательств, а также разработки Банком новых продуктов и услуг и информировании Клиента об этих продуктах и услугах, и в целях участия в опросах/анкетировании, проводимых Банком для изучения и исследования мнения клиентов о качестве обслуживания и услугах Банка.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

4.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

4.2. В случае нарушения настоящего Соглашения ответственность за последствия несет Сторона, которая допустила эти нарушения.

4.3. В случае возникновения обстоятельств непреодолимой силы, к которым относятся стихийные бедствия, аварии, пожары, массовые беспорядки, забастовки, революции, военные действия, противоправные действия Клиента, вступление в силу законодательных актов, правительственных постановлений и распоряжений государственных органов, прямо или косвенно запрещающих или препятствующих осуществлению Сторонами своих функций по Соглашению и иных обстоятельств, не зависящих от волеизъявления Сторон, Стороны по настоящему Соглашению освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств.

4.4. Банк не несет ответственность за:

4.4.1. любые задержки, сбои, прерывания и потери, возникшие вследствие неисправности Системы РЦК, не контролируемые Банком;

4.4.2. ущерб, возникший вследствие принятия к исполнению электронных платежных поручений с недействительной или скомпрометированной ЭП Контролирующей организации, поступившей до получения от Контролирующей организации информации о признании ее недействительной или о ее компрометации;

4.4.3. правомерность и правильность надлежащим образом оформленного Контролирующей организацией дополнительного акцепта/отказа от акцепта платежа, а также за убытки, понесенные Контролирующей организацией, Подконтрольными организациями вследствие отказов и несвоевременных действий лиц, в пользу которых осуществляется расчетная операция;

4.4.4. ущерб, возникший вследствие:

- неправильного заполнения электронного платежного поручения в Системе РЦК;
- разглашения Контролирующей организацией собственного пароля и/или передачи третьим лицам ключа ЭП, используемых для доступа подписания документов в Системе РЦК;
- несанкционированного доступа неуполномоченных лиц к АРМ РЦК, установленному у Контролирующей организации, и ключам ЭП Контролирующей организации;
- нарушения Контролирующей организацией правил информационной безопасности, изложенных в «Инструкции Клиента по обеспечению информационной безопасности», опубликованной на Сайте Банка.

4.5. Банк не несет ответственность за убытки Контролирующей организации, возникшие вследствие несвоевременного контроля Контролирующей организацией за действиями либо бездействием Контролирующей организации в Системе РЦК, вследствие некорректного или несвоевременного использования функциональных возможностей Системы РЦК.

4.6. Каждая Сторона несет полную ответственность за сохранение в тайне содержания своих ключей ЭП, а также за действия своего персонала.

4.7. Банк не несет ответственность за неработоспособность оборудования и программных средств Контролирующей организации и третьих лиц, повлекшую за собой невозможность доступа Контролирующей организации к Системе РЦК, и возникшие в результате этого задержки в осуществлении операций Контролирующей организацией, а также за возможное уничтожение (в полном или частичном объеме) информации, содержащейся на вычислительных средствах Контролирующей организации, подключенных к сети Интернет для обеспечения оказания Услуги по настоящему Соглашению.

5. ПОРЯДОК ОПЛАТЫ УСЛУГИ

5.1. Контролирующая организация самостоятельно и за свой счет приобретает программно-технические средства, предусмотренные в Приложении №3 к настоящему Соглашению.

5.2. Контролирующая организация оплачивает все расходы, комиссии и вознаграждения, вызванные подключением, установкой и обслуживанием Системы РЦК, согласно действующим тарифам Банка. Списание расходов, комиссий и вознаграждений производится в порядке, указанном в п. 6 Приложения №1 к настоящему Соглашению.

5.3. Плата за организацию доступа к Системе РЦК перечисляется Контролирующей организацией в день подписания настоящего Соглашения в соответствии с тарифами Банка. Плата за выдачу электронного ключа перечисляется Контролирующей организацией в день подписания

настоящего Соглашения в соответствии с тарифами Банка. Ежемесячная плата за предоставление Услуги с использованием Системы РЦК перечисляется Контролирующей организацией в последний рабочий день месяца в соответствии с тарифами Банка.

6. СРОК ДЕЙСТВИЯ СОГЛАШЕНИЯ И ДРУГИЕ УСЛОВИЯ

6.1. Настоящее Соглашение вступает в силу (в части работ по подключению Контролирующей организации к Системе РЦК) с момента подписания настоящего Соглашения обеими Сторонами и действует до момента расторжения настоящего Соглашения при условии соблюдения Контролирующей организацией условий оказания Услуги, указанных в п. 2.1 настоящего Соглашения. Настоящее Соглашение в полном объеме вступает в силу с даты ввода в действие открытого ключа ЭП Клиента.

6.2. Каждая из Сторон может расторгнуть настоящее Соглашение в одностороннем порядке, направив уведомление о прекращении оказания услуги РЦК и расторжении настоящего Соглашения не позднее, чем за 30 (Тридцать) календарных дней до момента расторжения. Настоящее Соглашение считается расторгнутым по истечении 30 (Тридцати) календарных дней с даты предоставления/направления Стороной такого уведомления другой Стороне. Отключение от Системы РЦК производится Банком в последний день истечения срока для расторжения настоящего Соглашения.

6.3. При неисполнении или ненадлежащем исполнении Контролирующей организацией своих обязательств по оплате Услуги Банк имеет право приостановить оказание Услуги на срок до 1 (Одного) календарного месяца с момента возникновения задолженности, а в случае неоплаты Контролирующей организацией своей задолженности по истечении указанного срока – расторгнуть настоящее Соглашение в одностороннем порядке. Настоящее Соглашение считается расторгнутым с даты, указанной Банком в уведомлении о расторжении настоящего Соглашения.

6.4. Любое требование (запрос и т.д.), любой документ, направляемые Банком в соответствии с условиями настоящего Соглашения, считаются полученными Контролирующей организацией, если они были направлены Контролирующей организации заказным письмом с уведомлением о вручении посредством почтовой связи по адресу, указанному в настоящем Соглашении, либо вручены под роспись Контролирующей организации с указанием должности, фамилии, имени, отчества полномочного представителя Контролирующей организации, даты получения и проставлением подписи, либо иным способом, включая, но, не ограничиваясь по электронной почте, факсу, телексу, телефонограммой, позволяющим определить момент получения такого требования (запроса и т.д.), документа Банка:

- в случае направления требования (запроса и т.д.), документа - через 5 (Пять) рабочих дней с даты его отправления, указанной на почтовом штемпеле;
- в случае вручения требования (запроса и т.д.), документа под роспись - в день передачи документа нарочно;
- в случае направления требования (запроса и т.д.), документа иным способом - на следующий рабочий день после его направления.

6.5. Контролирующая организация и Банк согласны с тем, что настоящее Соглашение в части неразглашения паролей и ключей системы защиты информации действительно в течение 1 (Одного) календарного года после расторжения настоящего Соглашения.

6.6. Настоящее Соглашение может быть изменено и дополнено по взаимному согласию Сторон, за исключением случаев, предусмотренных настоящим Соглашением. Все изменения или дополнения к настоящему Соглашению считаются действительными, если они выполнены в письменной форме и подписаны полномочными представителями Сторон.

6.7. Неотъемлемой частью настоящего Соглашения являются:

Приложение №1 – Заявление на предоставление/изменение услуги «Расчетный Центр Корпорации».

Приложение №2а – Дополнительное соглашение к договору банковского счета (о предоставлении информации по счету третьему лицу).

Приложение №2б – Дополнительное соглашение к договору банковского счета (о дополнительном акцепте расчетных документов Подконтрольной организации).

Приложение №2в – Дополнительное соглашение к договору банковского счета (о дополнительном акцепте расчетных документов Подконтрольной организации в рамках бюджета/сметы расходов).

Приложение №3 – Требования к программно-техническим средствам Системы РЦК.

Приложение №4 – Порядок подключения Контролирующей организации к автоматизированному рабочему месту (АРМ) Системы РЦК.

Приложение №5 – Согласие субъекта на обработку его персональных данных.

6.8. Настоящее Соглашение составлено в 2 (Двух) экземплярах, каждое из которых имеет одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

6.9. Срок хранения настоящего Соглашения и приложений к нему составляет не менее 5 (Пяти) лет.

7. РАЗРЕШЕНИЕ СПОРОВ И КОНФЛИКТНЫХ СИТУАЦИЙ

7.1. Все разногласия и конфликтные ситуации, возникающие в рамках настоящего Соглашения, разрешаются с учетом взаимных интересов путем переговоров в порядке, установленном настоящим Соглашением.

7.2. При возникновении разногласий и споров в связи с обменом Электронными документами с помощью Системы РЦК с целью установления фактических обстоятельств, послуживших основанием для их возникновения, а также для проверки целостности и подтверждения авторства Электронного документа, Стороны обязаны собрать экспертную комиссию и провести техническую экспертизу.

7.3. Экспертная комиссия состоит в количестве не менее 3 (Трех) человек, ее членами являются представители Банка и Контролирующей организации. Персональный состав экспертной комиссии отражается в акте работы экспертной комиссии, который утверждается руководством Банка и Контролирующей организации и заверяется их печатями. Для консультации могут привлекаться независимые эксперты.

7.4. В случае если экспертной комиссией не достигнуто соглашение по разрешению спора или конфликтной ситуации, любой спор, разногласие или претензия, вытекающие из или в связи с настоящим Соглашением, либо его нарушением, прекращением или недействительностью, а также незаключенностью подлежат разрешению в соответствии с действующим законодательством Российской Федерации.

8. АДРЕСА И РЕКВИЗИТЫ СТОРОН

Банк: АКБ АЛМАЗЭРГИЭНБАНК АО, 677000, г. Якутск, пр. Ленина, 1, корреспондентский счет в рублях 30101810300000000770 в ГРКЦ НБ РС (Я), БИК 049805770, ИНН 1435138944,
телефакс: (4112)34-22-22.
Контролирующая организация: _____
Место нахождения: _____
Телефоны:
_____
Адрес электронной почты: _____
Банк: АКБ АЛМАЗЭРГИЭНБАНК АО

Клиент: _____

Банк АКБ АЛМАЗЭРГИЭНБАНК АО _____ /_____/	Клиент _____ _____/_____/

Приложение №1
к Соглашению о предоставлении Услуги
«Расчетный Центр Корпорации» от «___» _____ 20__ г. № _____

ЗАЯВЛЕНИЕ
на предоставление/изменение услуги «Расчетный Центр Корпорации» (РЦК)
«___» _____ 20__ г.

❒на подключение ❒на изменение условий

1. Наименование Контролирующей организации (далее – Клиент):

_____

(полное официальное наименование юридического лица)

ИНН/ КПП:_____ ОГРН: _____
Местонахождение Клиента _____

(адрес местонахождения юридического лица)

2. Прошу организовать предоставление доступа к Системе «Расчетный Центр Корпорации» (РЦК) на условиях, предусмотренных Соглашением о предоставлении Услуги «Расчетный Центр Корпорации» № _____ от «___» _____ 20__ г. (далее – Соглашение) по следующим счетам:

№ п/п	Наименование	ИНН	КПП	Номер счета	Подразделение банка	Наименование услуги		
						Мониторинг	Контроль и акцепт	Контроль и акцепт в рамках бюджета
1						❒	❒	❒
2						❒	❒	❒

3. Перечень уполномоченных лиц и прав пользователей «Расчетный Центр Корпорации» (РЦК):

№ п/п	ФИО (полностью) пользователя	Должность пользователя	Паспортные данные (серия, номер, где и когда выдан)	Подпись пользователя	Услуга в части	Настройки	Область видимости	Телефон мобильный	Адрес электронной почты
1					☑Мониторинг ❒Контроль и акцепт				

					❒Контроль и акцепт в рамках бюджета				
2					☑Мониторинг ❒Контроль и акцепт ❒Контроль и акцепт в рамках бюджета				

Выше перечисленные устройства (программно-технические средства) для работы в Системе РЦК в количестве _____ шт. получил представитель Клиента: _____

(должность, Фамилия, Имя, Отчество представителя (указываются полностью)

_____,

действующий на основании _____

(наименование документа – Устав, Доверенность (указываются номер доверенности и дата ее совершения), иной соответствующий документ)

«___» _____ 20__ г. _____

Подпись

4. Настоящим Клиент предоставляет Банку право производить списание денежных средств в счет оплаты организации доступа к Системе РЦК, за выдачу электронного ключа, в счет оплаты ежемесячной платы за предоставление Услуги с использованием Системы РЦК, а также иных расходов, комиссий и вознаграждений, вызванных подключением, установкой и обслуживанием Системы РЦК, согласно действующим тарифам Банка, со Счета Клиента. В случае отсутствия счета клиента выставлять счета на оплату.

Плату за услугу Банка по соглашению просим :

❒списывать со счета Клиента_____, открытом в АКБ Алмазэргиэнбанк АО

❒выставлять счета на оплату.

Настоящим Клиент подтверждает, что ознакомился с тарифами и условиями настоящего Соглашения, понимает текст данных условий, выражает свое согласие с ними и обязуется их исполнять.

Подпись клиента:

С условиями предоставления услуги согласен _____

(должность, Фамилия, Имя, Отчество представителя (указываются полностью)

_____,
действующий на основании _____
(наименование документа – Устав, Доверенность (указываются номер доверенности и дата ее совершения), иной соответствующий документ)

«___» _____ 20__ г. _____
Подпись

ОТМЕТКИ БАНКА:
АКБ АЛМАЗЭРГИЭНБАНК АО, 677000, г. Якутск, пр. Ленина, 1, корреспондентский счет в рублях 30101810300000000770 в ГРКЦ НБ РС (Я), БИК 049805770, ИНН 1435138944, КПП 143501001
Заявление принял и проверил

_____ _____ _____ «___» _____ 20__ г.
Должность *подпись* *ФИО* *дата*

действия	**дата**	**Ответственный сотрудник банка**
Проверку полномочий лица, подписавшего заявление, произвел		_____/ _____/ *Должность, ФИО сотрудника* *подпись*
Полномочия лиц, имеющих право на заключение договора/распоряжение счетом, проверил, программно-технические устройства для работы в Системе РЦК (электронный(-ые) ключ(-и)) выдал		_____/ _____/ *Должность, ФИО сотрудника* *подпись*
Присвоен тарифный план _____		_____/ _____/ *Должность, ФИО сотрудника* *подпись*

Приложение №2а
к Соглашению о предоставлении Услуги «Расчетный Центр Корпорации»
от «___» _____ 20__ г. № _____

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ
к договору банковского счета № _____ от «___» _____ 20__ г.

Акционерный коммерческий банк «АЛМАЗЭРГИЭНБАНК» (АО), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, далее совместно именуемые «Стороны», заключили настоящее дополнительное соглашение к договору банковского счета № _____ от «___» _____ 20__ г. (далее – Договор) о нижеследующем:

1. Банк вправе предоставлять _____ *(указываются полное официальное наименование юридического лица и ИНН, с которым заключено Соглашение на предоставление услуги РЦК и в рамках которого будет предоставляться информация по счету подконтрольной организации)* информацию о счете и операциях по нему. Настоящим Клиент предоставляет Банку безусловное согласие на предоставление _____ *(указываются полное официальное наименование юридического лица и ИНН, с которым заключено Соглашение на предоставление услуги РЦК и в рамках которого будет предоставляться информация по счету подконтрольной организации)* информации по счету № _____, *(указывается номер счета клиента*) предусмотренной настоящим пунктом, без ограничений по способу и частоте предоставления.

2. До заключения настоящего дополнительного соглашения обеспечить предоставление лицом, указанным в преамбуле настоящего дополнительного соглашения, действующим от имени Клиента, согласия Банку на обработку персональных данных. Согласие предоставляется по форме Банка.

3. Остальные условия Договора, не затронутые настоящим дополнительным соглашением и не противоречащие ему, остаются неизменными, и Стороны подтверждают по ним свои обязательства.

4. Настоящее дополнительное соглашение составлено в ___ (_____) экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

5. Настоящее дополнительное соглашение является неотъемлемой частью Договора и вступает в силу с момента подписания Сторонами.

6. Настоящее дополнительное соглашение прекращает свое действие с момента прекращения Банком оказания Контролирующей организации услуги «Расчетный Центр Корпорации».

ЮРИДИЧЕСКИЕ АДРЕСА И ПОДПИСИ СТОРОН

Банк: АКБ АЛМАЗЭРГИЭНБАНК АО, 677000, г. Якутск, пр. Ленина, 1, корреспондентский счет в рублях 30101810300000000770 в ГРКЦ НБ РС (Я), БИК 049805770, ИНН 1435138944, телефакс: (4112)34-22-22.

Контролирующая организация: _____

Место нахождения: _____

Телефоны:

_____

Адрес электронной почты:

_____

Клиент: _____

Банк АКБ АЛМАЗЭРГИЭНБАНК АО _____ /_____/	Клиент _____ _____/_____/

Примечание (не включается в текст документа): Текст или отдельные слова документа, либо текст примечаний, сносок, выделенные курсивом и желтым цветом, являются комментариями к заполнению документа и в текст документа не включаются.

Приложение №2б
к Соглашению о предоставлении Услуги «Расчетный Центр Корпорации»
от «___» _____ 20__ г. № _____

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ
к договору банковского счета № _____ от «___» _____ 20__ г.

Акционерный коммерческий банк «АЛМАЗЭРГИЭНБАНК» (АО), именуемый в дальнейшем «Банк», в лице _____, действующего на основании _____, с одной стороны, и _____, *(полное официальное наименование юридического лица)* именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, далее совместно именуемые «Стороны», заключили настоящее дополнительное соглашение к договору банковского счета № _____ от «___» _____ 20__ г. (далее – Договор) о нижеследующем:: 1. Банк вправе предоставлять _____ *(указываются полное официальное наименование юридического лица и ИНН, с которым заключено Соглашение на предоставление услуги РЦК и в рамках которого будет предоставляться информация по счету подконтрольной организации)* информацию о счете и операциях по нему. Настоящим Клиент предоставляет Банку безусловное согласие на предоставление _____ *(указываются полное официальное наименование юридического лица и ИНН, с которым заключено Соглашение на предоставление услуги РЦК и в рамках которого будет предоставляться информация по счету подконтрольной организации)* информации, предусмотренной настоящим пунктом, без ограничений по способу и частоте предоставления.

2. Руководствуясь статьей 845 Гражданского кодекса РФ, Стороны договорились о необходимости получения Банком согласительной (акцептующей) подписи _____ *(полное наименование и ИНН Контролирующей организации)* на распоряжениях Клиента о списании денежных средств со счета Клиента, предусмотренной условиями соглашения на предоставление услуги «Расчетный центр корпорации» (РЦК) № _____ от «___» _____ 20__ г. (далее – Соглашение), а также о выполнении иных условий, содержащихся в указанном Соглашении.

3. Настоящим Клиент поручает Банку принимать к исполнению расчетные документы только при условии соблюдения требований, установленных п. 1 и п. 2 настоящего дополнительного соглашения, а также соблюдения иных условий Соглашения. Расчетные документы, не соответствующие таким требованиям, Банком не принимаются и не исполняются.

3.1. Предусмотренный настоящим дополнительным соглашением порядок исполнения расчетных документов Клиента в электронном виде по счету не распространяется на распоряжения Клиента по платежам в бюджет различных уровней, фонды, а также на списание денежных средств со счета без распоряжения Клиента в случаях, определенных действующим законодательством Российской Федерации.

4. Условия, установленные Соглашением, обязательны для исполнения Сторонами настоящего дополнительного соглашения, и имеют приоритет в части регулирования процедуры исполнения распоряжений Клиента, по сравнению с тем как такая процедура определена в Договоре.
5. Настоящим дополнительным соглашением Клиент поручает Банку принимать к исполнению распоряжения Клиента посредством электронной Системы ДБО только с учетом условий Соглашения. 6. Условия, предусмотренные настоящим дополнительным соглашением, а также Соглашением, применяются в отношении расчетных операций, осуществляемых посредством электронной Системы ДБО.
7. Клиент обязуется передавать в Банк расчетные документы только в электронном виде, посредством Системы ДБО, используемой в соответствии с Договором о предоставлении услуг с использованием Системы ДБО либо Соглашением/договором на подключение и обслуживание электронной Системы «АЭБ-Бизнес», заключенным между Банком и Клиентом. Банк не принимает распоряжения Клиента, составленные на бумажных носителях.
8. Настоящим Клиент предоставляет Банку право раскрытия сведений по счету № _____
_____
(полное наименование Контролирующей организации и ИНН)
9. До заключения настоящего дополнительного соглашения обеспечить предоставление лицом, указанным в преамбуле настоящего дополнительного соглашения, действующим от имени Клиента, согласия Банку на обработку персональных данных. Согласие предоставляется по форме Банка.
10. Остальные условия Договора, не затронутые настоящим дополнительным соглашением и не противоречащие ему, остаются неизменными, и Стороны подтверждают по ним свои обязательства.
11. Настоящее дополнительное соглашение составлено в ___ (_____) экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.
12. Настоящее дополнительное соглашение является неотъемлемой частью Договора и вступает в силу с момента подписания Сторонами.
13. Настоящее дополнительное соглашение прекращает свое действие с момента прекращения Банком оказания Контролирующей организации услуги «Расчетный Центр Корпорации».

Банк: АКБ АЛМАЗЭРГИЭНБАНК АО, 677000, г. Якутск, пр. Ленина, 1, корреспондентский счет в рублях 30101810300000000770 в ГРКЦ НБ РС (Я), БИК 049805770, ИНН 1435138944, телефакс: (4112)34-22-22.
Контролирующая организация: _____
Место нахождения: _____
Телефоны:
_____
Адрес электронной почты:
_____

Клиент: _____

Банк АКБ АЛМАЗЭРГИЭНБАНК АО _____ /_____/	Клиент _____ _____/_____/

Приложение №2в
Соглашению о предоставлении Услуги «Расчетный Центр Корпорации»
от «___» _____ 20__ г. № _____

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ
к договору банковского счета № _____ от «___» _____ 20__ г.

Акционерный коммерческий банк «Алмазэргиэнбанк» (акционерное общество), именуемый в дальнейшем «Банк», в лице _____,
(должность, фамилия, имя, отчество)
действующего на основании _____, с одной стороны, и
_____, *(полное официальное наименование юридического лица)*
именуемое в дальнейшем «Клиент», в лице _____
_____,
(должность, фамилия, имя, отчество)
действующего на основании _____, с другой стороны, далее совместно именуемые «Стороны», заключили настоящее дополнительное соглашение к договору банковского счета № _____ от «___» _____ 20__ г. (далее – Договор) о нижеследующем:

1. Банк вправе предоставлять _____ *(указываются полное официальное наименование юридического лица и ИНН, с которым заключено Соглашение на предоставление услуги РЦК и в рамках которого будет предоставляться информация по счету подконтрольной организации)* информацию о счете и операциях по нему.

Настоящим Клиент предоставляет Банку безусловное согласие на предоставление _____ *(указываются полное официальное наименование юридического лица и ИНН, с которым заключено Соглашение на предоставление услуги РЦК и в рамках которого будет предоставляться информация по счету подконтрольной организации)* информации, предусмотренной настоящим пунктом, без ограничений по способу и частоте предоставления.

2. Руководствуясь статьей 845 Гражданского кодекса РФ, Стороны договорились о необходимости получения Банком согласительной (акцептующей) подписи _____ *(полное наименование и ИНН Контролирующей организации)* (далее – Контролирующая организация) на распоряжениях Клиента о списании денежных средств со счета Клиента, предусмотренной условиями соглашения на предоставление услуги «Расчетный центр корпорации» (РЦК) № _____ от «___» _____ 20__ г. (далее – Соглашение), а также о выполнении иных условий, содержащихся в указанном Соглашении.

3. Настоящим Клиент поручает Банку принимать к исполнению расчетные документы только при условии соблюдения требований, установленных п. 1 и п. 2 настоящего дополнительного соглашения, а также соблюдения иных условий Соглашения. Расчетные документы, не соответствующие таким требованиям, Банком не принимаются и не исполняются.

3.1. Предусмотренный настоящим дополнительным соглашением порядок исполнения расчетных документов Клиента в электронном виде по счету не распространяется на распоряжения Клиента по платежам в бюджет различных уровней, фонды, а также на списание денежных средств со счета без распоряжения Клиента, в случаях, определенных действующим законодательством Российской Федерации.

4. Условия, установленные Соглашением, обязательны для исполнения Сторонами настоящего дополнительного соглашения и имеют приоритет в части регулирования процедуры исполнения распоряжений Клиента, по сравнению с тем, как такая процедура определена в Договоре.

5. Настоящим дополнительным соглашением Клиент поручает Банку принимать к исполнению распоряжения Клиента посредством электронной Системы ДБО только с учетом условий Соглашения.

6. Условия, предусмотренные настоящим дополнительным соглашением, а также Соглашения применяются в отношении расчетных операций, осуществляемых посредством электронной Системы ДБО.
7. Клиент обязуется передавать в Банк расчетные документы только в электронном виде, посредством Системы ДБО, используемой в соответствии с Договором о предоставлении услуг с использованием Системы ДБО либо Соглашением/договором на подключение и обслуживание электронной Системы «АЭБ-БИЗНЕС», заключенным между Банком и Клиентом. Банк не принимает распоряжения Клиента, составленные на бумажных носителях.
8. Настоящим Клиент предоставляет Банку право раскрытия сведений по счету № _____
_____
_____ *(полное наименование Контролирующей организации и ИНН)*
9. Клиент подтверждает, что при составлении им расчетных документов по своему счету, Контролирующая организация, указанная в п. 1 настоящего дополнительного соглашения, устанавливает бюджет на определенный период, указанный в Системе РЦК, в рамках которого Клиент осуществляет операции.
10. Клиент уведомлен и согласен, что соответствие расчетного документа Клиента бюджету и акцепт расчетного документа Клиента/отказ от акцепта расчетного документа Клиента осуществляет Контролирующая организация в Системе РЦК в зависимости от Услуги, указанной в заявлении на предоставление услуги «Расчетный центр Корпорации» (РЦК).
11. Клиент уведомлен и согласен, что Банк не контролирует соответствие осуществленных Клиентом операций/составленных им расчетных документов установленному Контролирующей организацией бюджету.
12. До заключения настоящего дополнительного соглашения обеспечить предоставление лицом, указанным в преамбуле настоящего дополнительного соглашения, действующим от имени Клиента, согласия Банку на обработку персональных данных. Согласие предоставляется по форме Банка.
13. Остальные условия Договора, не затронутые настоящим дополнительным соглашением и не противоречащие ему, остаются неизменными, и Стороны подтверждают по ним свои обязательства. 14. Настоящее дополнительное соглашение составлено в ___ (_____) экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.
15. Настоящее дополнительное соглашение является неотъемлемой частью Договора и вступает в силу с момента подписания Сторонами.
16. Настоящее дополнительное соглашение прекращает свое действие с момента прекращения Банком оказания Контролирующей организации услуги «Расчетный Центр Корпорации».

Банк: АКБ АЛМАЗЭРГИЭНБАНК АО,
677000, г. Якутск, пр. Ленина, 1, корреспондентский счет в рублях 30101810300000000770 в ГРКЦ НБ РС (Я), БИК 049805770, ИНН 1435138944,
телефакс: (4112)34-22-22.
Контролирующая организация: _____
Место нахождения: _____
Телефоны:
_____
Адрес электронной почты:
_____

Клиент: _____

Банк АКБ АЛМАЗЭРГИЭНБАНК АО _____ /_____/	Клиент _____ _____/_____/

Приложение №3
к Соглашению о предоставлении Услуги «Расчетный Центр Корпорации»
от «___» _____ 20__ г. № _____

1. **Требования к программно-техническим средствам Системы (приобретаются Контролирующей организацией за собственный счет у третьих лиц):**

1.1. Персональный компьютер в конфигурации, достаточной для обеспечения работы операционной системы из п. 1.2;

1.2. Операционная система (ОС): MS Windows XP / 7 / 8 / 8.1 / 10 или Windows Server 2003 R2 x64 / 2008 x86, x64 / 2008 R2 / 2012 / 2012 R2;

1.3. Дополнительное ПО: Microsoft Excel 2003 или выше;

1.4. Канал доступа в Интернет;

1.5. Принтер;

1.6. Для использования функционала наложения ЭП дополнительно необходимо установить драйвер для устройства хранения закрытой части ЭП.

2. Правила эксплуатации Системы.

Для эксплуатации Системы необходим выделенный компьютер с предустановленной операционной системой семейства Microsoft Windows. Если по желанию Контролирующей организации установка Системы производится на компьютер с предустановленными программными средствами сторонних производителей, Банк не несет ответственности за работоспособность программного обеспечения сторонних производителей.

При эксплуатации Системы запрещается:

- Установка программного обеспечения сторонних фирм, а также сознательное внесение изменений в файлы программного и информационного обеспечения Системы, которые могут повлечь за собой неработоспособность Системы;
- Доступ к Системе неуполномоченных лиц.

При эксплуатации Системы Контролирующая организация обязана:

- Исключить возможность заражения компьютера с установленной Системой программными вирусами или другими вредоносными программами;
- Использовать только легальное и лицензионное программное обеспечение;
- Обеспечить техническую исправность оборудования, входящего в состав рабочего места Системы.

Необходимость резервного копирования рабочего места пользователя Системы определяет Контролирующая организация и при необходимости осуществляет его собственными силами.

Банк АКБ АЛМАЗЭРГИЭНБАНК АО _____ /_____/	Клиент _____ _____/_____/

Приложение №4
к Соглашению о предоставлении Услуги «Расчетный Центр Корпорации»
от «___» _____ 20__ г. № _____

Порядок подключения Контролирующей организации к автоматизированному рабочему месту (АРМ) Системы РЦК

1. Одновременно с соглашением на предоставление услуги «Расчетный центр корпорации» Контролирующая организация подает в Банк Заявление на предоставление/изменение услуги «Расчетный Центр Корпорации» (далее - Заявление) по форме Приложения №1 к Соглашению, в котором Контролирующая организация указывает требуемый ему функционал и состав пользователей Системы РЦК, уполномоченных выполнять соответствующие функциональные обязанности в рамках Соглашения, а также реквизиты Контролирующей организации, перечень подключаемых счетов, параметры настроек и иную относящуюся к организации работ в Системе РЦК информацию.

В случае если Контролирующая организация не имеет открытого счета в Банке, то Контролирующая организация предоставляет в Банк комплект документов для идентификации в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Документы должны быть предоставлены в Банк до заключения Соглашения и оказания Услуги. В случае не предоставления Контролирующей организацией Банку комплекта документов в соответствии с настоящим пунктом либо ненадлежащего предоставления (не в полном объеме), Банк вправе отказать Контролирующей организации в заключении Соглашения и оказании Услуги.

В случае если после заключения Соглашения и в процессе оказания Услуги возникнет необходимость (в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма или по требованию Банка) предоставления Контролирующей организацией Банку дополнительных документов к указанному комплекту документов и в случае не предоставления Контролирующей организацией Банку необходимых документов в соответствии с настоящим пунктом либо ненадлежащего предоставления (не в полном объеме), Банк вправе отказать Контролирующей организации в оказании Услуги и расторгнуть Соглашение в одностороннем порядке по истечению 30 (Тридцати) календарных дней с момента такого отказа либо ненадлежащего предоставления.

2. Сотрудник Банка проверяет полномочия пользователей Системы РЦК согласно Заявлению. Сотрудник Банка имеет право не принимать к исполнению Заявление Контролирующей организации, заполненное неразборчиво, содержащее ошибки или не полностью заполненное.

3. Банк предоставляет Контролирующей организации программное обеспечение через Систему ДБО, сопроводительную документацию через Сайт Банка.

4. Факт приема-передачи электронных ключей Стороны отражают в Приложении №1 к Соглашению.

5. Контролирующая организация самостоятельно проводит установку, переустановку и настройку переданного Банком программного обеспечения в соответствии с предоставленными инструкциями на своих аппаратных средствах, отвечающих требованиям Приложения №3.

В случае если Контролирующая организация предполагает использовать функционал акцепта платежных поручений в соответствии с п. 1.2.2 или п. 1.2.3 Соглашения необходимо:

6. По окончании работ по установке и настройке программного обеспечения Уполномоченные лица Контролирующей организации самостоятельно формируют ключи ЭП и производят распечатку Сведений об открытом ключе абонента (по форме, определенной в интерфейсе Системы РЦК) в 3 (Трех) экземплярах.

7. Контролирующая организация нарочно передает Банку распечатки Сведений об открытом ключе абонента (по форме, определенной в интерфейсе Системы РЦК), заверенные собственноручной подписью владельца сертификата ключа электронной подписи, руководителя или лица, наделенного правом подписывать договор(-ы) финансово-банковских услуг (договоры, содержащие право на распоряжение денежными средствами по счету), и оттиска печати Контролирующей организации (по 3 (Три) экземпляра для каждого ключа проверки ЭП).

Банк АКБ АЛМАЗЭРГИЭНБАНК АО _____ /_____/	Клиент _____ _____/_____/

Приложение №5
к Соглашению о предоставлении Услуги «Расчетный Центр Корпорации»
от «___» _____ 20__ г. № _____

Согласие субъекта на обработку его персональных данных

Я, _____, проживающий по адресу: _____
Паспорт серии _____, номер _____, выдан _____
__ даю АКБ АЛМАЗЭРГИЭНБАНК АО (далее – Банк), расположенному по адресу: Россия, Республика Саха (Якутия), г.Якутск, пр.Ленина,1, в соответствии с требованиями статьи 9 Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных» **согласие на обработку** (любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) **моих персональных данных** (фамилии, имени, отчества, даты и места рождения, адреса места жительства, реквизитов документа, удостоверяющего личность) с целью принятия Банком решений об установлении, изменении или прекращении правовых отношений между Банком и мною, а также информирования меня о новых продуктах и услугах Банка, об изменении продуктов и услуг Банка.

Я также даю согласие на сообщение моих персональных данных третьей стороне, а именно, в Центральный Банк Российской Федерации, государственным органам и организациям для целей обеспечения соблюдения законов, а также иным лицам в случаях, предусмотренных действующим законодательством Российской Федерации, нормативными актами Банка России в целях обеспечения указанных выше целей третьему лицу, или при привлечении третьих лиц к оказанию услуг в указанных целях.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

В случае получения моего письменного отзыва согласия на обработку персональных данных Банк прекращает обработку моих персональных данных в течение 30 (Тридцати) дней, если иное не установлено законодательством Российской Федерации.

Номер мобильного телефона: _____

Адрес электронной почты: _____

Субъект персональных данных _____ / _____/

(подпись, Фамилия, имя, отчество)

«___» _____ 20__ г.