УТВЕРЖДЕНО
Правление
АКБ «Кросна-Банк» (ОАО)
Протокол
№ 24 от «17» октября 2014 года

РЕГЛАМЕНТ

банковского обслуживания с применением системы «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ «Кросна-Банк» (ОАО)

г. Москва

2014

ОГЛАВЛЕНИЕ

ЧАСТЬ 1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. СТАТУС РЕГЛАМЕНТА

1.1.1. Настоящий “Регламент банковского обслуживания с применением системы «Электронный Банк-Клиент» АКБ “Кросна-Банк” (ОАО) (далее по тексту – Регламент) определяет условия, на которых АКБ «Кросна-Банк» (ОАО) (далее по тексту – Банк) осуществляет банковское обслуживание с применением системы «Электронный Банк-Клиент».

1.1.2. Опубликование настоящего Регламента, включая размещение в помещениях Банка и на сайте Банка http://www.crosnabank.ru, должно рассматриваться всеми заинтересованными лицами как публичное предложение (оферта) со стороны Банка заключить соглашение о банковском обслуживании с применением системы «Электронный Банк-Клиент» (далее по тексту – Соглашение), существенные условия которого зафиксированы в настоящем Регламенте.

1.1.3. Настоящее предложение адресовано исключительно заключившим с Банком договор банковского счета юридическим и физическим лицам, индивидуальным предпринимателям, физическим лицам, занимающимся в установленном законодательством Российской Федерации порядке частной практикой.

1.1.4. Заключение Соглашения с Банком о банковском обслуживании с применением системы «Электронный Банк-Клиент» производится путем совершения письменного акцепта условий настоящего Регламента на условиях, предусмотренных для договора присоединения в соответствии со ст. 428 Гражданского Кодекса Российской Федерации, т.е. без каких–либо изъятий, условий или оговорок, за исключением тех изъятий, условий или оговорок, которые изложены в тексте самого Регламента, а также бланке Заявления, посредством выбора которых Клиент имеет возможность зафиксировать условия акцепта Регламента. Акцепт Регламента должен быть произведен путем направления Банку 2 (Двух) экземпляров «Заявления на банковское обслуживание с применением системы «Электронный Банк-Клиент»», форма которого предусмотрена Приложениями № 1, № 2, № 3 к Регламенту (далее по тексту - Заявление).

1.1.5. Акцепт Регламента будет считаться совершенным с даты регистрации Заявления в Банке. Банк присваивает каждому Заявлению Клиента номер, который является номером Соглашения. Факт регистрации Заявления подтверждается подписью руководителя, его заместителя или иного уполномоченного лица Банка, и печатью Банка на Заявлении, второй экземпляр которого передается Клиенту.

С даты присоединения к настоящему Регламенту действие Соглашения распространяется на все Счета Клиента, открытые в Банке на дату присоединения, а также на Счета, которые будут открыты в Банке в будущем.

1.1.6. С даты регистрации Заявления, все договоры на банковское обслуживание через электронные системы банковского обслуживания, ранее заключенные между Банком и Клиентом, утрачивают силу, если иное не оговорено соглашением Сторон.

1.1.7. Настоящий Регламент вступает в силу с 27 октября 2014 года.

1.1.8. Стороны устанавливают переходный период для правоотношений возникших, между Банком и Клиентом до вступления в силу настоящего Регламента и вытекающих из Регламента банковского обслуживания с применением системы «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ «Кросна-Банк» (ОАО) в редакции от 11.08.10 (далее - старая редакция Регламента):

1.1.8.1. к правоотношениям Сторон применяются следующие положения старого Регламента: п.п. 1.1- 1.4, часть II, за исключением п. 2.5, п. 2.6, часть IV. Остальные положения старого Регламента утрачивают силу с даты вступления в силу настоящего Регламента.

1.1.8.2. к правоотношениям сторон применяются следующие положения Регламента: п.п. 1.4-1.6, часть III, часть IV.

1.1.8.3. После окончания срока действия Закрытого ключа ЭЦП, сгенированного в период действия старой редакции Регламента, положения старой редакции Регламента утрачивают силу полностью и Клиент обязуется подать в Банк Заявление в соответствии с п.1.1. Регламента. Обслуживание Клиента в Системе приостанавливается до оформления отношений в соответствии с требованиями настоящего Регламента.

Если Клиент в течение 1 календарного месяца с даты окончания срока действия Закрытого ключа ЭЦП, сгенерированного в период действия старой редакции Регламента, не подаст в Банк Заявление, то правоотношения Банка и Клиента, вытекающие из Регламента, прекращаются.

1.1.8.4. Клиент вправе до истечения срока действия Закрытого ключа ЭЦП в любой момент прекратить применение старой редакции Регламента путем присоединения к настоящему Регламенту.

1.1.8. Присоединение к настоящему Регламенту на иных условиях не допускается.

1.2. СВЕДЕНИЯ О БАНКЕ

Полное наименование:

АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «КРОСНА-БАНК» (ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО)

Сокращенное наименование:

АКБ «Кросна-Банк» (ОАО)

Сведения о регистрации:

Устав зарегистрирован Центральным банком России 08 декабря 1993 г. за № 2607

Основной государственный регистрационный номер:

1027739175859

Место нахождения:

Россия, 123557 г. Москва, Пресненский Вал, д.27

Почтовый адрес:

Россия, 123557 г. Москва, Пресненский Вал, д.27

1.3. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.3.1. Применяемые в тексте настоящего Регламента следующие термины используются в их нижеприведенных значениях:

Автоматизированное рабочее место (АРМ) Клиента – программно-аппаратный комплекс, обеспечивающий работу Клиента с Системой.

Акт признания открытого ключа ЭАСП — документ на бумажном носителе по форме Приложения № 4 к Регламенту, включающий в себя сведения об Открытом ключе ЭАСП, Владельце ЭАСП, Клиенте и подтверждающий принадлежность Владельцу ЭАСП и Клиенту Открытого ключа ЭАСП и авторства ЭД, содержащего ЭАСП и успешно прошедшего Проверку подлинности ЭД.

Владелец ЭАСП — лицо, составившее Акт признания открытого ключа ЭАСП и зарегистрированное в Системе как владелец ЭАСП.

Закрытый ключ ЭАСП — уникальная последовательность символов, известная только Владельцу ЭАСП, и предназначенная для создания ЭАСП с использованием СКЗИ.

Клиент — юридическое или физическое лицо, или индивидуальный предприниматель, или физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой, присоединившееся к настоящему Регламенту.

Ключевой носитель — электронный носитель информации, хранящий Закрытый ключ ЭАСП

Ключи ЭАСП — Открытый ключ ЭАСП и Закрытый ключ ЭАСП, изготавливаемые одновременно. Каждому Закрытому ключу ЭАСП соответствует только одни единственный Открытый ключ ЭАСП и наоборот.

Ключ доступа – криптографический ключ, предназначенный исключительно для аутентификации Клиента при входе в Систему и не предназначенный для создания ЭАСП с использованием СКЗИ и обмена ЭД.

Кодовое слово Клиента — индивидуальное слово, предназначенное для аутентификации Клиента при обращении его в Банк по телефону.

Компрометация закрытого ключа ЭАСП — событие, в результате которого Закрытый ключ ЭАСП может стать доступными лицам, не имеющим полномочий доступа к нему, в том числе утрата Закрытого ключа ЭАСП и (или) его использование без согласия Владельца ЭАСП.

Компрометация Ключа доступа – событие, в результате которого Ключ доступа может стать доступным лицам, не имеющим полномочий доступа к нему, в том числе утрата Ключа доступа.

Логин — уникальный идентификатор учетной записи Клиента, предназначенный для входа Клиента в Систему.

Новость(и) – электронное сообщение в разделе «Новости банка» Системы, направленное Банком Клиенту с целью уведомления и информирования в рамках Регламента. Новости не являются ЭД.

Открытый ключ ЭАСП — уникальная последовательность символов, соответствующая Закрытому ключу ЭАСП, известная Сторонам и предназначенная для проверки с использованием СКЗИ подлинности ЭД, содержащего ЭАСП, и удостоверяющая факт составления и подписания ЭД от имени Клиента или Банка. Информация об Открытом ключе не является конфиденциальной.

Одноразовый пароль — Пароль для входа в Систему, подлежащий обязательной смене Клиентом при первом входе в Систему.

Пароль для входа в Систему — комбинация из 10 символов, которая предназначена для аутентификации Клиента при авторизации в Системе.

Подтверждение подлинности ЭД — положительный результат Проверки подлинности ЭД.

Проверка подлинности ЭД — криптографическая функция СКЗИ, использующая ЭД и Открытый ключ ЭАСП в качестве аргументов и возвращающая положительный или отрицательный результат проверки соответствия ЭАСП в ЭД Открытому ключу ЭАСП и отсутствия искажений в ЭД, подписанном данной ЭАСП.

Расчетный ЭД — распоряжение Клиента, содержащее информацию, позволяющую осуществить перевод денежных средств в рамках применяемых форм безналичных расчетов, подписанное ЭАСП.

Система «Электронный Банк-Клиент» (Система) — это система дистанционного банковского обслуживания АКБ «Кросна-Банк» (ОАО) с использованием программного продукта: «Система дистанционного банковского обслуживания “BS-Client v.3”», разработанного ООО «Банк’с Софт Системс», посредством Интернет или удаленного коммутируемого доступа (с помощью модема).

Средство криптографической защиты информации (СКЗИ) — программный продукт «КриптоПро CSP 3.6». Официальная WEB-страница продукта: http://www.cryptopro.ru/products/csp/.

Средство проверки ЭАСП — эталонное программное средство проверки ЭАСП включает в себя СКЗИ и программный продукт «КриптоАРМ» компании ООО «Цифровые технологии». Официальная WEB-страница продукта: http://www.trusted.ru/products/cryptoarm/. Рекомендация разработчика СКЗИ: http://www.cryptopro.ru/products/partner/crypto-arm/.

Счет — расчетные и иные счета, открытые Клиенту в Банке на основании договора банковского счета, заключенного между Клиентом и Банком.

Статус документа – отображение стадии обработки документа в Системе.

Тарифы Банка — утвержденные тарифы Банка за банковское обслуживание Клиента, в том числе с использованием Системы.

Токен — ключевой носитель с защитой Закрытого ключа ЭАСП или Ключа доступа от несанкционированного доступа.

Удаленный помощник — программное средство удаленного доступа через Интернет к «рабочему столу» Windows АРМ Клиента с целью оказания технической поддержки Клиенту.

Электронный аналог собственноручной подписи (ЭАСП) — неотъемлемый реквизит ЭД, обеспечивающий защиту ЭД от подделки и искажений, полученный в результате криптографического преобразования ЭД с помощью СКЗИ и Закрытого ключа ЭАСП, и позволяющий однозначно установить с помощью Открытого ключа ЭП и СКЗИ факт того, что ЭД документ был создан обладателем Закрытого ключа ЭАСП, а также установить подлинность и отсутствие искажений информации в ЭД.

Электронный документ (ЭД) – набор данных в Системе, подписанный ЭАСП, имеющий в Системе визуальное отображение, возможность преобразования в бумажный документ путем печати на принтер, а также возможность сохранения в виде файла на стороне Клиента и/или Банка. Электронный документ включает в себя понятие Расчетный ЭД.

Иные термины, специально не определенные настоящим Регламентом, используются в значениях, установленных действующим законодательством Российской Федерации.

1.5. БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ

1.5.1. Стороны признают, что ЭД, подписанный ЭАСП, подготовленный и переданный с помощью Системы, соответствующий требованиям действующего законодательства и банковским правилам,

признается ЭД, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и порождает аналогичные ему права и обязанности Сторон.

1.5.2. Стороны признают, что используемые ими подсистемы обработки, хранения, защиты и передачи информации достаточны для обеспечения надежной, эффективной и безопасной работы.

1.5.3. Стороны принимают к использованию для осуществления передачи ЭД в Системе средства криптографической защиты информации, сертифицированные уполномоченным федеральным органом исполнительной власти Российской Федерации.

1.5.4. Стороны признают, что используемые в Системе средства криптографической защиты информации, которые обеспечивают шифрование, контроль целостности ЭАСП, достаточны для защиты информации от несанкционированного доступа, подтверждения подлинности и авторства ЭД, а также разбора конфликтных ситуаций по ним.

1.5.5. Закрытый ключ ЭАСП, Ключ доступа, пароли, Кодовое слово Клиента, а также материалы разбора конфликтных ситуаций являются конфиденциальной информацией и не подлежат разглашению Банком и Клиентом ни при каких обстоятельствах, за исключением случаев, установленных действующим законодательством и/или Регламентом.

1.5.6. Банк обязуется ограничить круг своих сотрудников, допущенных к сведениям о Клиенте, таким образом, чтобы их число не превышало необходимое для выполнения обязательств, предусмотренных настоящим Регламентом.

1.5.7. Клиент согласен, что в случаях, установленных действующим законодательством и нормативными актами Банка России, Банк вправе раскрывать информацию об операциях, счетах и реквизитах Клиента, а так же прочую информацию о Клиенте.

1.5.8. Клиент обязуется не передавать третьим лицам без письменного согласия Банка любые сведения, которые станут ему известны в связи исполнением положений настоящего Регламента, если только такое разглашение прямо не связано с необходимостью защиты собственных интересов в установленном законодательством порядке.

1.5.9. В целях соблюдения безопасности и конфиденциальности Банк и Клиент обязуются нести обязанности, предусмотренные настоящим Регламентом и действующим законодательством.

1.5.10. Клиент подтверждает, что до присоединения к настоящему Регламенту проинформирован Банком, в том числе путем ознакомления с информацией, размещенной на сайте Банка http://www.crosnabank.ru:

- о случаях повышенного риска использования как Системы, ЭАСП, так и любого электронного средства платежа, в том числе о риске передачи ЭД неуполномоченным лицом или злоумышленником путем несанкционированного доступа к АРМ Клиента или хищения Ключевого носителя, Закрытого ключа ЭАСП, Ключа доступа, Логина, паролей.

- об условиях использования Системы, Ключевого носителя, Закрытого ключа ЭАСП, Ключа доступа, Логина, паролей;

- об ограничениях способов и мест использования Системы, Ключевого носителя, Закрытого ключа ЭАСП, Ключа доступа, Логина, паролей.

1.5.11. Клиент обязуется принимать все необходимые меры по обеспечению:

- конфиденциальности Закрытого ключа ЭАСП, Пароля для входа в Систему, Кодового слова, Ключа доступа;

- доступа к Системе и Ключевым носителям исключительно уполномоченных Клиентом лиц;

- учета копий дистрибутива СКЗИ, находящегося на дистрибутивном диске АРМ Клиента.

1.5.12. Рекомендации по обеспечению безопасного использования Системы приведены в Приложении № 6 к Регламенту.

1.5.13. Файлы, прикрепленные к направляемым в Банк ЭД, проходят антивирусный контроль. В случае обнаружения вредоносного вложения Банк блокирует работу Клиента с ЭД, которые допускают прикрепление файлов, до устранения Клиентом заражения АРМ Клиента вредоносным кодом. Порядок взаимодействия Сторон в случае обнаружения Банком вредоносного кода содержится в части II настоящего Регламента. Список ЭД, которые допускают прикрепление файлов, перечислены в Приложении 5 к Регламенту.

1.6. УВЕДОМЛЕНИЯ И ИНФОРМИРОВАНИЕ.

1.6.1. Документы по форме приложений к настоящему Регламенту составляются только на бумажном носителе, если иное не предусмотрено настоящим Регламентом.

1.6.2. Банк с помощью Новостей, которые предоставляются Клиенту при входе в Систему, информирует Клиента о событиях в Системе, новостях, непредвиденных ситуациях, иных случаях и ситуациях, предусмотренных настоящим Регламентом.

1.6.3. Для направления Сторонами сообщений друг другу применяются составленные в произвольной форме уведомления, которые передаются с использованием произвольных документов или путем предоставления оригинальных документов на бумажных носителях, включая пересылку документов по почте заказным письмом с уведомлением о вручении.

1.6.4. Банк рекомендует во всех случаях указывать в тексте очередного уведомления, что оно является дубликатом, если оно дублирует ранее направленное тем же способом уведомление или повторяет уведомление направленное иным способом.

1.6.5. В случае отсутствия указания Клиента, что какое-либо уведомление, является дублирующим, Банк рассматривает и исполняет его как независимое от ранее полученных уведомлений.

1.6.6. Банк информирует Клиента о совершении каждой операции в Системе следующим способом:

- отображение актуального статуса ЭД;

- предоставление выписок по счету Клиента в соответствующем разделе Системы;

- «SMS-оповещение» и «E-mail - оповещение» Клиента о проведенных операциях по Счету Клиента. Услуга предоставляется платно в соответствии с Тарифами Банка.

1.6.7. Банк фиксирует направление Клиенту и получение от Клиента ЭД, уведомления, Новости, а также хранит соответствующую информацию не менее 3-х лет.

1.6.8. Клиент обязуется в Системе:

- контролировать статус ЭД;

- проверять и запрашивать выписки по Счетам;

- проверять поступление новостей и уведомлений от Банка;

- регулярно (не реже 1 раза в рабочий день) знакомиться с новостями в Системе.

1.6.9. Клиент вправе с помощью АРМ Клиента запросить выписку по Счету за период не более 3 (трех) рабочих дней

1.7. СРОКИ ПО РЕГЛАМЕНТУ

1.7.1. ЭД, оформляемые и передаваемые Клиентом с использованием Системы, принимаются Банком круглосуточно, за исключением времени технологических перерывов, указанных в Приложении № 8 к Регламенту.

1.7.2. Стороны признают, что безотзывность перевода денежных средств, наступает с момента списания денежных средств со Счета Клиента.

1.7.3. Банк принимает к исполнению заявление Клиента на отмену ЭД только в том случае, если у Банка имеется возможность отменить его исполнение. Отмена ЭД осуществляется Банком после получения Банком от Клиента заявления на отзыв с использованием Системы с полным указанием реквизитов отзываемого документа. В случае невозможности отозвать документ, Банк направляет об этом Клиенту сообщение в форме произвольного документа.

1.7.4. Стороны устанавливают, что все Новости и ЭД, передаваемые Банком в Системе, считаются доведенными до сведения Клиента не позднее следующего рабочего дня с даты их направления Клиенту (включая день направления).

1.7.5. Срок хранения ЭД равен сроку хранения аналогичного бумажного документа, установленному действующим законодательством.

1.7.6. Сроки исполнения обязательств по ЭД не являются предметом настоящего договора, при этом сроки исполнения Расчетных ЭД установлены действующим законодательством и договором банковского счета или иного договора, заключенного между Банком и Клиентом.

1.8. ЭЛЕКТРОННЫЙ АНАЛОГ СОБСТВЕННОРУЧНОЙ ПОДПИСИ И КЛЮЧИ ЭАСП.

1.8.1. Распоряжение денежными средствами, находящимися на Счете Клиента с использованием ЭАСП осуществляется Владельцем ЭАСП, которым могут быть:

- Клиент-физическое лицо;

- Клиент-индивидуальный предприниматель;

- Клиент-физическое лицо, занимающееся в установленном законодательством Российской Федерации порядке частной практикой;

- Единоличный исполнительный орган Клиента, действующий на основании учредительного документа;

- уполномоченное лицо, указанное в карточке с образцами подписей и оттиска печати Клиента, действующее на основании доверенности от имени Клиента физического лица или индивидуального предпринимателя, а также физического лица, занимающегося в установленном законодательством Российской Федерации порядке частной практикой;

- уполномоченный сотрудник Клиента-юридического лица, указанный в карточке с образцами подписи и оттиска печати Клиента, в должностные обязанности которого входит совершение таких действий.

1.8.2. Количество Владельцев ЭАСП и сочетание подписей Владельцев ЭАСП Клиент определяет самостоятельно на основании карточки с образцами подписей и оттиска печати Клиента и Соглашения **о** количестве подписей в Карточке с образцами подписей и оттиска печати и их сочетании в распоряжениях Клиента (при наличии такого соглашения). Клиент вправе оформить в качестве Владельцев ЭАСП как всех лиц, указанных в карточке, так и часть из них, при условии соблюдения Соглашения о количестве подписей в Карточке с образцами подписей и оттиска печати и их сочетании в распоряжениях Клиента.

1.8.2.1. Сведения о сотруднике/лице, уполномоченном распоряжаться денежными средствами с использованием ЭАСП указываются Клиентом в Заявлении при присоединении к настоящему Регламенту.

Сведения о новом уполномоченном сотруднике/лице, уполномоченном распоряжаться денежными средствами с использованием ЭАСП, и/или смене такого сотрудника/лица предоставляются Клиентом Банку в письменном виде по форме Приложения № 7 к Регламенту.

В указанных документах Клиент-юридическое лицо отражает порядок сочетания подписей (статус) Владельца(ев) ЭАСП:

– одна ИЛИ

– две подписи (с указанием Владельца ЭАСП с которым сочетается подпись).

Выбирая статус «одна» Клиент-юридическое лицо признает, что ЭД должен быть подписан одной ЭАСП, принадлежащей любому Владельцу ЭАСП.

Выбирая статус «две подписи» Клиент-юридическое лицо признает, что ЭД должен быть подписан одновременно двумя ЭАСП, принадлежащими двум Владельцам ЭАСП в порядке, определенном настоящим Регламентом.

Владельцы ЭАСП Клиентов индивидуальных предпринимателей, физических лиц и физических лиц, занимающихся в установленном порядке частной практикой имеют статус «одна» по умолчанию. Сведения об изменении сочетания ЭАСП подписей лиц, наделенных правом подписи, необходимых для подписания документов, содержащих распоряжение Клиента предоставляются Клиентом Банку в письменном виде по форме Приложения № 7 к Регламенту. Сведения по указанной форме могут быть представлены в отношении одного, двух и более Владельцев ЭАСП.

1.8.3. В целях выполнения требований действующего законодательства Клиент должен выполнить все необходимые действия, предъявить и предоставить все документы, необходимые для установления личности лица (лиц), наделенных правом распоряжаться денежными средствами, находящимися на Счете с использованием ЭАСП.

1.8.4. Ключи ЭАСП изготавливаются Клиентом самостоятельно. Одновременно с генерацией Закрытого Ключа ЭАСП автоматически формируется Открытый Ключ ЭАСП.

1.8.5. Акт признания Открытого ключа ЭАСП распечатывается из Системы и подписывается Владельцем ЭАСП и заверяется подписью уполномоченного лица и печатью Клиента (при наличии печати).

1.8.6. Акт признания открытого ключа ЭАСП составляется по форме Приложения № 4 к Регламенту в 1-м экземпляре, передается Клиентом в Банк в срок не позднее 3 (трех) календарных месяцев с даты генерации

Закрытого ключа ЭАСП и хранится в Банке не менее 6 лет с даты его подписания, уполномоченным лицом Банка. Дата подписания Акта признания открытого ключа уполномоченным лицом Банка является датой начала действия Открытого ключа ЭАСП.

1.8.7. Клиент вправе получить копию Акта признания открытого ключа, заверенную Банком.

1.8.8. Срок действия Закрытого ключа ЭАСП – один год с момента его генерации, после чего использование Закрытого ключа ЭАСП для подписи ЭД запрещается

1.8.9. После смены Закрытого ключа ЭАСП и начала работы в Системе с использованием нового Закрытого Ключа ЭАСП старый Закрытый ключ ЭАСП подлежит уничтожению Клиентом средствами СКЗИ в соответствии с Руководством по уничтожению Закрытого ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

1.8.10. В целях обеспечения непрерывного доступа в Систему Клиенту рекомендуется иметь резервную копию Закрытого ключа ЭАСП на случай выхода из строя Ключевого носителя, а также зарегистрировать в Банке дополнительные ЭАСП и Владельцев ЭАСП на случай непредвиденного прекращения действия или компрометации Закрытого ключа ЭАСП.

1.9. КЛЮЧ ДОСТУПА.

1.9.1. Для аутентификации Клиента при входе в Систему Клиент вправе использовать Ключ доступа, позволяющий работать в Системе, но не предназначенный для создания ЭАСП с использованием СКЗИ и обмена ЭД.

1.9.2. К изготовлению, формированию, смене, сроку действия Ключа доступа применяются положения настоящего Регламента о Закрытом и Открытом ключах ЭАСП, за исключением положений о распоряжении денежными средствами, находящимися на Счете Клиента.

1.9.3. Сведения о сотруднике/лице, уполномоченном использовать Ключ доступа указываются Клиентом в Заявлении при присоединении к настоящему Регламенту.

Сведения о новом уполномоченном сотруднике/лице, уполномоченном использовать Ключ доступа, и/или смене такого сотрудника/лица предоставляются Клиентом Банку в письменном виде по форме Приложения № 7а к Регламенту.

1.9.4. В целях выполнения требований действующего законодательства Клиент должен выполнить все необходимые действия, предъявить и предоставить все документы, необходимые для установления личности лица (лиц), уполномоченных использовать Ключ доступа. Идентификация представителя Клиента проводится в соответствии сдействующим законодательством и внутренними документами Банка. Перечень документов и сведений, необходимых для идентификации Клиента, устанавливается законодательством Российской Федерации и «Правилами внутреннего контроля в Банке в целях противодействия и легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"[1].

1.9.5. Ключи доступа изготавливаются Клиентом самостоятельно по аналогии с изготовлением Ключей ЭАСП.

1.9.6. Акт признания Открытого ключа распечатывается из Системы и подписывается Владельцем Ключа доступа и заверяется подписью уполномоченного лица и печатью Клиента (при наличии печати) с обязательным указанием в особых отметках о примени режима Ключа доступа.

1.9.7. Акт признания открытого ключа составляется по форме Приложения № 4 к Регламенту в 1-м экземпляре, передается Клиентом в Банк в срок не позднее 3 (трех) календарных месяцев с даты генерации Ключа доступа и хранится в Банке не менее 6 лет с даты его подписания, уполномоченным лицом Банка. Дата подписания Акта признания открытого ключа уполномоченным лицом Банка является датой начала действия Ключа доступа.

1.9.8. Клиент вправе получить копию Акта признания открытого ключа, заверенную Банком.

1.9.9. Срок действия Ключа доступа – один год с момента его генерации, после чего использование Ключа доступа запрещается.

[1] Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию доходов, полученных преступным путем, и финансированию терроризма»; Положение Банка России № 262-П от 19.08.2004 "Об идентификации кредитными организациями клиентов и выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" и т.д.

1.9.10. После смены Ключа доступа и начала работы в Системе с использованием нового Ключа доступа старый Ключ доступа подлежит уничтожению Клиентом средствами СКЗИ в соответствии с Руководством по уничтожению Закрытого ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

1.9.11. В целях обеспечения непрерывного доступа в Систему Клиенту рекомендуется иметь резервную копию Ключа доступа на случай выхода из строя Ключевого носителя.

ЧАСТЬ II. ОСНОВНЫЕ УСЛОВИЯ РАБОТЫ С СИСТЕМОЙ

2.1. ПОДКЛЮЧЕНИЕ И НАЧАЛО РАБОТЫ В СИСТЕМЕ

2.1.1. Клиент за свой счет подготавливает компьютер для установки АРМ Клиента, соответствующий требованиям, изложенным в Приложении № 8 к Регламенту.

2.1.2. После присоединения Клиента к настоящему Регламенту Банк передает Клиенту по описи, составленной по форме Приложения № 9 к Регламенту, дистрибутивный диск АРМ Клиента и конверт с паролями, Кодовым словом, а также на основании Заявления Клиента токен и/или код активации СКЗИ.

2.1.3. Клиент самостоятельно и/или с помощью технической поддержки Банка по телефону или в форме выезда специалиста к Клиенту производит установку и настройку программного обеспечения АРМ Клиента в соответствии с Руководством по подключению к Системе, которое находится на дистрибутивном диске АРМ Клиента, и изготавливает Ключи ЭАСП и при необходимости Ключи доступа.

2.1.5. Клиент передает в Банк на бумажном носителе Акт признания открытого ключа ЭАСП Клиента. Начало работы в Системе определяется датой начала действия Открытого ключа ЭАСП Клиента, указанной Банком в Акте признания Открытого ключа.

2.1.6. Вход Клиента в Систему производится с использованием Логина, Пароля для входа в Систему и Закрытого ключа ЭАСП или Ключа доступа.

2.1.7. Логин может быть изменен Банком по письменному заявлению Клиента.

2.1.8. Пароль для входа в Систему может быть изменен Клиентом самостоятельно в любое время в меню «Сервис→Безопасность» АРМ Клиента.

2.1.9. При неправильном вводе Пароля для входа в Систему 3 (три) раза подряд доступ Клиента в Систему блокируется и Клиент обязан обратиться в Службу технической поддержки Банка для разблокировки.

2.2. ВНЕСЕНИЕ ИЗМЕНЕНИЙ В НАСТРОЙКИ АРМ КЛИЕНТА

2.2.1. Клиент по Системе в форме произвольного ЭД направляет заявку на изменение настроек АРМ Клиента.

2.2.2. Специалист Службы технической поддержки Банка направляет Клиенту сообщение по Системе в форме произвольного документа с информацией о произведенных изменениях в настройках или об отказе во внесении изменений.

2.3. СМЕНА КЛЮЧЕЙ ЭАСП \КЛЮЧА ДОСТУПА КЛИЕНТА

2.3.1.ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ ЭАСП

2.3.1.1. В соответствии с планом смены Закрытого Ключа ЭАСП Банк за 30 (Тридцать) календарных дней до истечения срока действия Закрытого Ключа ЭАСП направляет Клиенту по Системе сообщение в форме произвольного документа о необходимости произвести плановую смену Закрытого Ключа ЭАСП.

2.3.1.2. В случае невозможности проведения Клиентом смены Закрытого Ключа ЭАСП в течение последних 30 (Тридцати) календарных дней срока действия Закрытого ключа ЭАСП, в целях обеспечения непрерывной работы в Системе Клиенту рекомендуется произвести заблаговременную внеплановую смену Закрытого Ключа ЭАСП.

2.3.1.3. Клиент осуществляет смену Закрытого Ключа ЭАСП в соответствии с Руководством по плановой смене Ключей ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.3.1.4. После создания нового Закрытого ключа Клиент передает в Банк на бумажном носителе Акт признания открытого ключа ЭАСП Клиента.

2.3.1.5. Начало работы в Системе с использованием нового Закрытого Ключа ЭАСП определяется датой начала действия нового Открытого ключа ЭАСП Клиента, указанной Банком в Акте признания Открытого ключа.

2.3.1.6. Если Клиент до истечения срока действия Закрытого ключа ЭАСП не сменил Закрытый Ключ ЭАСП и не предоставил в Банк Акт признания открытого ключа ЭАСП, то доступ Клиента в Систему с использованием старого Закрытого ключа ЭАСП блокируется и может быть осуществлен Клиентом исключительно для выполнения процедур по смене Закрытого Ключа ЭАСП и по обращению в Службу технической поддержки Банка.

2.3.1.7. После истечения срока действия Закрытого ключа ЭАСП Клиент уничтожает его средствами СКЗИ в соответствии с руководством по уничтожению Закрытого ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.3.2.ВНЕПЛАНОВАЯ СМЕНА КЛЮЧЕЙ ЭАСП

2.3.2.1. В случае необходимости Клиент осуществляет внеплановую смену Закрытого Ключа ЭАСП в соответствии с Руководством по внеплановой смене Ключей ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.3.2.2. После создания нового Закрытого ключа Клиент передает в Банк на бумажном носителе Акт признания открытого ключа ЭАСП Клиента.

2.3.2.3. Начало работы в Системе с использованием нового Закрытого Ключа ЭАСП определяется датой начала действия нового Открытого ключа ЭАСП Клиента, указанной Банком в Акте признания Открытого ключа.

2.3.2.4. Банк блокирует старый Закрытый ключ ЭАСП Клиента с даты начала действия нового Открытого ключа

2.3.2.5. После начала успешной работы с новым Закрытым ключом ЭАСП Клиент уничтожает старый Закрытый ключ ЭАСП средствами СКЗИ в соответствии с руководством по уничтожению Закрытого ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.3.3.ВЫХОД ИЗ СТРОЯ КЛЮЧЕВОГО НОСИТЕЛЯ

2.3.3.1. В случае выхода из строя Ключевого носителя Клиент обращается в Службу технической поддержки Банка.

2.3.3.2. Служба технической поддержки Банка предоставляет Клиенту возможность самостоятельно изготовить новый Закрытый ключ ЭАСП.

2.3.3.3. Клиент изготавливает новый Закрытый ключ ЭАСП в соответствии с Руководством по изготовлению нового Ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.3.3.4. После создания нового Закрытого ключа ЭАСП Клиент передает в Банк на бумажном носителе Акт признания открытого ключа ЭАСП Клиента.

2.3.3.5. Начало работы в Системе с использованием нового Закрытого Ключа ЭАСП определяется датой начала действия нового Открытого ключа ЭАСП Клиента, указанной Банком в Акте признания Открытого ключа.

2.3.3.6. Клиент производит физическое уничтожение вышедшего из строя Ключевого носителя.

2.3.3.7. Банк блокирует Закрытый ключ ЭАСП Клиента, оставшийся на вышедшем из строя Ключевом носителе.

2.3.4.КОМПРОМЕТАЦИЯ КЛЮЧА ЭАСП

2.3.4.1. При обнаружении факта или подозрении о компрометации Закрытого ключа ЭАСП Клиент обязан немедленно по телефону: (495) 913-77-59 оповестить Банк о компрометации Ключа ЭАСП с использованием Кодового слова Клиента.

2.3.4.2. Банк блокирует скомпрометированный Закрытый Ключ ЭАСП с момента получения информации по телефону и направляет Клиенту с использованием Системы сообщение в форме произвольного документа о блокировании Закрытого ключа ЭАСП. Клиент направляет в Банк соответствующее письменное уведомление по форме Приложения № 10 к Регламенту о факте компрометации или отсутствии факта компрометации Закрытого ключа ЭАСП. Если в Банк поступит письменное уведомление об отсутствии факта компрометации Закрытого ключа ЭАСП, то Банк возобновляет работу Закрытого ключа ЭАСП.

2.3.4.3. Банк предоставляет Клиенту техническую возможность самостоятельно изготовить новый Закрытый Ключ ЭАСП.

2.3.4.4. Клиент изготавливает новый Закрытый ключ ЭАСП в соответствии с Руководством по изготовлению нового Ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.3.4.5. После создания нового Закрытого ключа ЭАСП Клиент передает в Банк на бумажном носителе Акт признания открытого ключа ЭАСП Клиента.

2.3.4.6. Начало работы в Системе с использованием нового Закрытого Ключа ЭАСП определяется датой начала действия нового Открытого ключа ЭАСП Клиента, указанной Банком в Акте признания Открытого ключа.

2.3.4.7. Клиент уничтожает скомпрометированный Закрытый ключ ЭАСП средствами СКЗИ в соответствии с Руководством по уничтожению Закрытого ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.3.5.СМЕНА КЛЮЧА ДОСТУПА

2.3.5.1. В соответствии с планом смены Ключа доступа Банк за 30 (Тридцать) календарных дней до истечения срока действия Ключа доступа направляет Клиенту по Системе сообщение в форме произвольного документа о необходимости произвести плановую смену Ключа доступа.

В случае невозможности проведения Клиентом смены Ключа доступа в течение последних 30 (Тридцати) календарных дней срока действия Ключа доступа, в целях обеспечения непрерывной работы в Системе Клиенту рекомендуется произвести заблаговременную внеплановую смену Ключа доступа.

Клиент осуществляет смену Ключа доступа по аналогии со сменой Закрытого Ключа ЭАСП.

Банк блокирует старый Ключ доступа с даты начала действия нового Ключа доступа.

После начала успешной работы с новым Ключом доступа Клиент уничтожает старый Ключ доступа средствами СКЗИ по аналогии с уничтожением Закрытого ключа ЭАСП.

2.3.5.2. В случае выхода из строя Ключевого носителя Клиент обращается в Службу технической поддержки Банка.

Служба технической поддержки Банка предоставляет Клиенту возможность самостоятельно изготовить новый Ключ доступа.

Клиент изготавливает новый Ключ доступа по аналогии с изготовлением нового Закрытого Ключа ЭАСП.

Клиент производит физическое уничтожение вышедшего из строя Ключевого носителя.

Банк блокирует Ключ доступа, оставшийся на вышедшем из строя Ключевом носителе.

2.3.5.3. При обнаружении факта или подозрении о компрометации Ключа доступа Клиент обязан немедленно по телефону: (495) 913-77-59 оповестить Банк о компрометации Ключа доступа с использованием Кодового слова Клиента.

Банк блокирует скомпрометированный Ключ доступа с момента получения информации по телефону и направляет Клиенту с использованием Системы сообщение в форме произвольного документа о блокировании Ключа доступа. Клиент направляет в Банк соответствующее письменное уведомление по форме Приложения № 10 к Регламенту о факте компрометации или отсутствии факта компрометации Ключа доступа. Если в Банк поступит письменное уведомление об отсутствии факта компрометации Ключа доступа, то Банк возобновляет работу Ключа доступа.

Банк предоставляет Клиенту техническую возможность самостоятельно изготовить новый Ключ доступа.

Клиент изготавливает новый Ключ доступа по аналогии с изготовлением нового Закрытого Ключа ЭАСП.

Клиент уничтожает скомпрометированный Ключ доступа средствами СКЗИ по аналогии с уничтожением Закрытого ключа ЭАСП.

2.3.5.4. При смене Ключа доступа Акт признания Открытого ключа распечатывается из Системы и подписывается Владельцем Ключа доступа и заверяется подписью уполномоченного лица и печатью Клиента (при наличии печати) с обязательным указанием в особых отметках о примени режима Ключа доступа.

Акт признания открытого ключа составляется по форме Приложения № 4 к Регламенту в 1-м экземпляре, передается Клиентом в Банк в срок не позднее 3 (трех) календарных месяцев с даты генерации Ключа доступа и хранится в Банке не менее 6 лет с даты его подписания, уполномоченным лицом Банка. Дата подписания Акта признания открытого ключа уполномоченным лицом Банка является датой начала действия Ключа доступа.

Клиент вправе получить копию Акта признания открытого ключа, заверенную Банком.

2.4. НАЧАЛО РАБОТЫ В СИСТЕМЕ С ИСПОЛЬЗОВАНИЕМ НОВОГО КЛЮЧА ДОСТУПА ОПРЕДЕЛЯЕТСЯ ДАТОЙ ИЗГОТОВЛЕНИЯ НОВОГО КЛЮЧА ДОСТУПА. 2.4.СМЕНА КЛЮЧЕЙ ЭАСП БАНКА.

2.4.1. Банк уведомляет Клиента по Системе путем направления сообщения в виде Новости о смене Ключей ЭАСП Банка с указанием электронной ссылки для получения копии Акта признания нового открытого ключа ЭАСП Банка. Заверенную копию Акта признания открытого ключа ЭАСП Банка Клиент может получить в Банке на основании письменного запроса.

2.5. РЕГИСТРАЦИЯ НОВЫХ ЭАСП И ВЛАДЕЛЬЦЕВ ЭАСП

2.5.1. Клиент передает по Системе сообщение в форме произвольного ЭД с просьбой о регистрации новых ЭАСП и Владельцев ЭАСП.

2.5.2. Служба технической поддержки Банка предоставляет Клиенту возможность самостоятельно изготовить новый Закрытый ключ ЭАСП.

2.5.3. Клиент изготавливает новый Закрытый ключ ЭАСП в соответствии с Руководством по изготовлению нового Ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.5.4. Клиент предоставляет в Банк Акт признания открытого ключа ЭАСП Клиента.

2.5.5. В целях выполнения требований действующего законодательства Клиент должен выполнить все необходимые действия, предъявить и предоставить все документы, необходимые для установления личности лица (лиц), наделенных правом распоряжаться денежными средствами, находящимися на Счете с использованием ЭАСП.

2.5.6. Начало работы в Системе с использованием нового Закрытого Ключа ЭАСП определяется датой начала действия нового Открытого ключа ЭАСП Клиента, указанной Банком в Акте признания Открытого ключа.

2.6 АННУЛИРОВАНИЕ ЗАРЕГИСТРИРОВАННЫХ ЭАСП И ВЛАДЕЛЬЦЕВ ЭАСП

2.6.1. Клиент передает по Системе сообщение в форме произвольного ЭД с просьбой об аннулировании регистрации ЭАСП и Владельцев ЭАСП.

2.6.2. Банк блокирует аннулируемый Закрытый ключ ЭАСП Клиента.

2.6.3. Клиент уничтожает аннулированные Закрытые ключи ЭАСП средствами СКЗИ в соответствии с Руководством по уничтожению Закрытого ключа ЭАСП, которое находится на дистрибутивном диске АРМ Клиента.

2.7. ОБНАРУЖЕНИЕ БАНКОМ ВРЕДОНОСНОГО КОДА В ФАЙЛЕ, ПРИКРЕПЛЕННОМ К ЭД КЛИЕНТА.

2.7.1. В случае обнаружения Банком вредоносного кода в файле, прикрепленном к ЭД Клиента, который допускает прикрепление файлов, Банк блокирует работу Клиента с таким ЭД. Список ЭД, которые допускают прикрепление файлов, перечислены в Приложении 6 Регламенту.

2.7.2. О факте обнаружения Банком вредоносного кода в файле, прикрепленном к ЭД Клиента, Банк уведомляет Клиента по Системе путем отправки сообщения в форме произвольного документа.

2.7.3. Специалист Службы технической поддержки Банка связывается с Клиентом по телефону с разъяснениями причин блокировки и рекомендациями по устранению вирусного заражения.

2.7.4. Клиент самостоятельно принимает меры по обезвреживанию и удалению вредоносного кода с АРМ Клиента.

2.7.5. Клиент сообщает в Службу технической поддержки Банка об отсутствии вредоносного кода.

2.7.6. Банк разблокирует работу Клиента с ЭД, которые допускают прикрепление файлов.

2.8. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

2.8.1. Банк оказывает Клиенту услуги технической консультации и удаленной помощи на АРМ Клиента без выезда специалиста Банка к Клиенту в рамках Регламента.

2.8.2. Банк предоставляет Клиенту услугу выезда специалиста Банка к месту установки АРМ Клиента для оказания технической помощи на месте в пределах г.Москвы и Московской области (до 20 км. от МКАД).

2.8.4. Служба технической поддержки Банка работает по рабочим дням с 9:00 до 18:00 (по пятницам до 17:00). Телефон службы – (495)913-77-59, e-mail: 9137759@crosnabank.ru.

2.8.5 При обращении в Службу технической поддержки Банка по телефону с целью приостановки или возобновления работы в Системе после любой произошедшей приостановки, блокировки входа в Систему, в целях блокировки или разблокировки Закрытого ключа ЭАСП, сброса Пароля для входа в Систему, переустановки или дополнительной установки АРМ Клиента, а также в других случаях, по просьбе специалиста Службы технической поддержки Банка Клиент обязан в целях аутентификации назвать Кодовое слово Клиента.

2.8.6. Служба технической поддержки Банка при возникновении такой необходимости и при наличии работающего подключения к интернету оказывает Клиенту удаленную помощь с использованием Удаленного помощника Windows для чего Клиенту высылается ссылка для загрузки настроечной программы.

2.8.7. Кодовое слово Клиента по письменному заявлению Клиента может быть заменено на новое. В этом случае Банк передает Клиенту по описи, примерная форма которой приведена в Приложении 9 к Регламенту, новый конверт с паролями, после чего Клиент должен уничтожить ранее выданный конверт.

2.8.8. Факт оказания услуг, оплачиваемых в соответствии с Тарифами Банка, подтверждается оформлением двустороннего Акта выполненных работ по форме, приведенной в Приложении 11 к Регламенту.

ЧАСТЬ III. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. ОБЯЗАННОСТИ

3.1.1. БАНК ОБЯЗУЕТСЯ

3.1.1.1. Выдать Клиенту дистрибутивный диск АРМ Клиента, конверт с паролями, а также токен и код активации СКЗИ, если они запрошены Клиентом в Заявлении.

3.1.1.2. Предоставлять Клиенту для установки актуальные версии программное обеспечение.

3.1.1.3. Консультировать Клиента по вопросам установки и эксплуатации Системы в порядке, установленном Регламентом.

3.1.1.4. Своевременно информировать Клиента об изменениях в порядке приема/передачи ЭД по Системе.

3.1.1.5. Не корректировать реквизиты ЭД Клиента.

3.1.1.6. Информировать Клиента о причинах неисполнения ЭД.

3.1.1.7. Ежедневно готовить для Клиента выписки по счету (счетам), независимо от наличия операций по нему (ним), вести и хранить Электронные журналы учета отправленных/принятых ЭД. Журналы должны храниться в соответствии с порядком и сроками, установленными для расчетных документов.

3.1.1.8. В случае получения от Клиента сообщения о компрометации Закрытого ключа ЭАСП Клиента немедленно приостановить обслуживание Клиента в Системе с применением скомпрометированного Закрытого ключа ЭАСП в порядке, установленном настоящим Регламентом.

3.1.1.9. Предоставлять Клиенту документы и информацию, которые связаны с использованием Клиентом ЭАСП по письменному заявлению Клиента.

3.1.1.10.Банк обязан рассматривать заявления Клиента, а также предоставлять Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в срок не более 30 дней со дня получения таких заявлений, а также не более 60 дней со дня получения заявлений в случае использования ЭАСП для осуществления трансграничного перевода денежных средств.

3.1.1.11.Нести иные обязанности, предусмотренные настоящим Регламентом и действующим законодательством.

3.1.2. КЛИЕНТ ОБЯЗУЕТСЯ

3.1.2.1. Приобрести за свой счет оборудование, отвечающие требованиям, предъявляемым Банком к АРМ Клиента, изложенным в Регламенте, а также поддерживать АРМ Клиента в рабочем состоянии.

3.1.2.2. Установить на АРМ Клиента программное обеспечение, предоставленное Банком.

3.1.2.3. Использовать при проведении обмена ЭД Систему только на исправном и проверенном на отсутствие компьютерных вирусов персональном компьютере и направлять в Банк ЭД, не содержащие компьютерных вирусов и/или иных вредоносных программ.

3.1.2.4. Использовать установленные на АРМ Клиента программные средства, предоставленные Банком, только для обмена ЭД и информацией в Системе с Банком в целях, установленных Регламентом, без права передачи третьим лицам или копирования.

3.1.2.5. Подписывать и предавать Банку в установленные Регламентом сроки Акты признания открытого ключа ЭАСП Клиента.

3.1.2.6. Обеспечивать конфиденциальность Закрытого ключа ЭАСП, Ключа доступа, Логина, паролей, Кодового слова.

3.1.2.7. Обеспечивать доступ к Системе и Ключевым носителям исключительно уполномоченных Клиентом лиц.

3.1.2.8. Осуществлять ввод расчетно-денежных документов и контроль введенной информации на соответствие ее первичным платежным документам и формирование записей в ЭД, соблюдая порядок подготовки документов и обеспечивая заполнение форм в соответствии с действующим законодательством и действующими банковскими правилами.

3.1.2.9. Контролировать правильность реквизитов получателя платежа на своих Расчетных ЭД.

3.1.2.10.Осуществлять регулярные (не реже одного раза в рабочий день) сеансы связи с Банком для получения возможных уведомлений, служебных сообщений, новостей и своевременно реагировать на них. Вся информация, переданная Банком по Системе, считается доведенной до сведения Клиента по истечении 1 (Одного) банковского дня с даты ее размещения на сервере Банка.

3.1.2.11.Оплачивать услуги Банка по настоящему Регламенту в соответствии с Тарифами Банка.

3.1.2.12.Предоставлять Банку все необходимые документы и информацию об осуществлении операций в установленные законодательством Российской Федерации сроки в случаях, предусмотренных действующим законодательством.

3.1.2.13.Проводить плановую смену Закрытого Ключа ЭАСП и Ключа доступа.

3.1.2.14.Не передавать третьим лицам коды активации СКЗИ, использовать СКЗИ только в составе АРМ Клиента и удалить СКЗИ в случаях отказа от Регламента или от АРМ Клиента.

3.1.2.15.Представить и передать Банку оформленные в соответствии с действующим законодательством документы, материалы и информацию, необходимые для подключения к Системе.

3.1.2.16.Следовать рекомендациям, перечисленным в Приложении № 5 к настоящему Регламенту.

3.1.2.17.По требованию Банка, в указанные им сроки, произвести замену (смену версии) программного обеспечения АРМ Клиента.

3.1.2.18.По уведомлению Банка, в указанные им сроки, произвести смену Ключей ЭАСП Клиента и Ключа доступа.

3.1.2.19.Немедленно сообщать Банку об исключении Владельцев ЭАСП из числа лиц, которые имеют право доступа к Системе, в том числе в связи с его увольнением, переводом на другой участок работы, а также об изменении их полномочий в целях ограничения использования соответствующих ЭАСП.

3.1.2.20.Уничтожить Закрытый ключ ЭАСП и Ключ доступа не позднее 1 (Одного) месяца со дня истечения срока или прекращения его действия.

3.1.2.21.Извещать Банк о всех случаях компрометации Закрытого ключа ЭАСП/Ключа доступа, в том числе обо всех случаях утраты, хищения, несанкционированного использования ключевого носителя.

3.1.2.22.В случае отказа от Регламента и прекращения использования Системы удалить программное обеспечение Системы с компьютера, уничтожить дистрибутивный диск и конверт с паролями, включая коды активации СКЗИ.

3.1.2.23.Предоставлять возможность лицам, уполномоченным Банком и членам Экспертной комиссии при рассмотрении споров в порядке, установленном настоящим Регламентом, осуществлять контроль на АРМ Клиента за соблюдением мер безопасности, установленных Регламентом и эксплуатационной документацией на используемые программные средства защиты информации.

3.1.2.24.Предоставлять членам Экспертной комиссии доступ к АРМ Клиента при рассмотрении споров в порядке, установленном настоящим Регламентом.

3.1.2.25.В целях выполнения требований действующего законодательства выполнять все необходимые действия, предъявить и предоставить все документы, необходимые для установления личности лица (лиц), наделенных правом подписывать документы, предусмотренные настоящим Регламентом, распоряжаться денежными средствами, находящимися на счете Клиента с использованием ЭАСП.

3.1.2.26.Сообщать Банку о любых изменениях, произошедших в сведениях и документах ранее предоставленных в Банк, а также обо всех других изменениях, имеющих существенное значение для полного и своевременного исполнения обязательств по настоящему договору, не позднее 48 часов с даты их изменения.

3.1.2.27.Одновременно с сообщением об изменении сведений, предусмотренных настоящим пунктом, Клиент должен предоставить в Банк удостоверенные в установленном порядке копии соответствующих документов.

3.1.2.28.Нести иные обязанности, предусмотренные настоящим Регламентом и действующим законодательством.

3.1.3. СТОРОНЫ ВЗАИМНО ОБЯЗУЮТСЯ

3.1.3.1. При обмене ЭД с использованием Системы руководствоваться правилами и требованиями, установленными Центральным банком Российской Федерации, действующим законодательством, применяемыми в банковской практике правилами, обычаями делового оборота и условиями настоящего Регламента.

3.1.3.2. За собственный счет поддерживать в рабочем состоянии компьютер с установленным АРМ Клиента.

3.1.3.3. Организовать внутренний режим функционирования рабочего места таким образом, чтобы исключить возможность использования Системы лицами, не имеющими допуска к работе с ней, а также исключить возможность использования ключей ЭАСП не уполномоченными лицами.

3.1.3.4. Приостановление или прекращение использования Клиентом электронного средства платежа не прекращает обязательств Клиента и Банка по переводу денежных средств, возникших до момента приостановления или прекращения указанного использования.

3.1.3.5. Нести иные обязанности, предусмотренные настоящим Регламентом и действующим законодательством.

3.2. ПРАВА

3.2.1. БАНК ИМЕЕТ ПРАВО

3.2.1.1. Не принять ЭД, в том числе Расчетный ЭД, к исполнению, если подлинность ЭД не подтверждена, если ЭД оформлен ненадлежащим образом, в случае несоответствия операции законодательству РФ, в случаях непредставления клиентом в Банк документов и информации об осуществляемой операции в порядке, определенном законодательством, в иных случаях, предусмотренных условиями договора банковского счета или иного договора, заключенного между Банком и Клиентом, а также если Клиент не осуществил плановую/внеплановую смену Ключей ЭАСП.

3.2.1.2. Запрашивать у Клиента документы и иную информацию в соответствии с законодательством РФ, получать необходимые разъяснения, справки, документы и сведения по вопросам, касающимся проводимых Клиентом операций.

3.2.1.3. Контролировать полноту заполнения реквизитов в ЭД Клиента. Некорректно оформленные ЭД Клиента к исполнению Банком не принимаются.

3.2.1.4. Оформлять бумажные копии принятых к исполнению ЭД Клиента и заверять их в соответствии с банковскими правилами проведения расчетных операций.

3.2.1.5. Ограничивать и приостанавливать использование Системы для приема ЭД, в случаях ненадлежащего исполнения Клиентом своих обязательств по Регламенту, а также по договору банковского счета или иного договора, с предварительным уведомлением Клиента не менее чем за 3 (три) рабочих дня, а по требованию уполномоченных государственных органов в случаях и в порядке, предусмотренных законодательством Российской Федерации.

3.2.1.6. Осуществлять замену/обновление программного обеспечения Системы без предварительного согласия Клиента. О замене/обновлении программного обеспечения Системы Банк уведомляет Клиента не менее чем за 30 (Тридцать) календарных дней путем направления сообщения в виде Новости.

3.2.1.7. В одностороннем порядке изменять Регламент и тарифы Банка.

3.2.1.8. Временно, до выяснения обстоятельств, прекратить обслуживание Клиента через Систему с использованием Закрытого ключа ЭАСП/Ключа доступа в случае наличия у Банка обоснованного подозрения о Компрометации Закрытого ключа ЭАСП/Ключа доступа, в том числе, если Банку стало известно о прекращении полномочий Владельца ЭАСП. В этом случае Банк прикладывает все усилия для скорейшего оповещения Клиента о временном прекращении обслуживания и разрешения возникшей ситуации.

3.2.1.9. При наличии сомнений в подлинности Расчетного ЭД направить запрос Клиенту (письменный, устный) о подтверждении его подлинности и исполнить такой Расчетный ЭД не ранее дня получения от Клиента соответствующего подтверждения. Сомнения могут быть вызваны, в том числе, в связи с поступлением в Банк Расчетного ЭД:

- сформированного в послеоперационное время (если иное не установлено отдельным договором между Банком и Клиентом);
- предусматривающего списание денежных средств на текущий счет (счет вклада (депозита)) физического лица в случае, если такое перечисление производится впервые и т.д.

3.2.1.10. Временно приостановить доступ Клиента к Системе в случаях выявления фактов допуска Клиентом к Системе неуполномоченных третьих лиц, временно блокировать доступ Клиента к Системе в случае поступления информации о зачислении на Счет денежных средств, списанных в результате несанкционированного доступа к счетам других клиентов (в том числе в других банках), а также любого несанкционированного доступа к Счету.

3.2.1.11. Временно приостановить доступ Клиента к Системе в рамках мероприятий, предусмотренных Законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (Федеральный закон от 07.08.2001 № 115-ФЗ).

3.2.1.12. В любой момент приостановить обслуживание Клиента через Систему в случае нарушения или неисполнения Клиентом требований настоящего Регламента.

3.2.1.13. Временно прекращать обслуживание Клиента через Систему в случае неоплаты услуги за использование Системы в течение 1 (одного) месяца. Возобновление обслуживания по Системе осуществляется не позднее 3 (трех) рабочих дней после поступления в Банк соответствующей оплаты.

3.2.1.14. В одностороннем порядке отключить Клиента от Системы по истечении 5-месячного срока от даты появления задолженности по оплате услуг за использование Системы.

3.2.1.15. Приостановить обслуживание Клиента через Систему для выполнения неотложных, аварийных и регламентных работ, связанных с обслуживанием Системы, с уведомлением Клиента о сроках проведения этих работ.

3.2.2. КЛИЕНТ ИМЕЕТ ПРАВО

3.2.2.1. Требовать от Банка предоставления информации о причинах неисполнения ЭД и проверки платежных документов по проведенным на основании полученных по Системе ЭД операциям, не позднее 10 (Десяти) банковских дней после предоставления Банком выписки.

3.2.2.2. Получать от Банка необходимую информацию и консультационные услуги по вопросам использования Системы, а также в случае неисправности в Системе в соответствии с условиями настоящего Регламента и Тарифами Банка запрашивать выезд специалиста Банка к Клиенту. Банк вправе самостоятельно по Заявке Клиента установить на АРМ Клиента специальное программное обеспечение, предоставленное Банком.

3.2.2.3. Получать от Банка необходимые подтверждения выполненных операций.

3.2.2.4. Клиент имеет право направить отзыв своего ЭД с помощью Системы.

3.2.2.5. Требовать от Банка выдачи на руки заверенной копии Акта признания открытого ключа ЭАСП Банка на бумажном носителе.

ЧАСТЬ IV. ПРОЧИЕ УСЛОВИЯ

4.1. ВОЗНАГРАЖДЕНИЕ БАНКА И ОПЛАТА РАСХОДОВ.

4.1.1. Клиент за свой счет приобретает программно-технические средства в соответствии с Приложением № 8 к Регламенту.

4.1.2. В случае переустановки/дополнительной установки программного обеспечения Системы и т.п., Клиент в указанный Банком срок приобретает программное обеспечение за свой счет.

4.1.3. Услуги Банка по настоящему Регламенту оплачиваются Клиентом в соответствии с Тарифами Банка.

4.1.4. Тарифы могут изменяться Банком в одностороннем порядке, при этом Клиент признает право Банка не только на одностороннее изменение стоимости действующих услуг, но и на введение новых платных услуг. Новые тарифы доводятся до сведения Клиента путем публичного размещения информации в операционном зале Банка по месту его нахождения. Информация о новых тарифах размещается не менее чем за 10 (Десять) календарных дней до даты их введения. Новые тарифы действуют с даты, установленной в решении уполномоченного органа Банка об их утверждении.

4.1.5. Комиссионное вознаграждение Банка за услуги по настоящему Регламенту (далее «комиссии Банка» или «комиссионное вознаграждение») списываются Банком со Счета Клиента в безакцептном порядке в соответствии с Тарифами Банка. Клиент обязан обеспечивать на своем Счете наличие денежных средств в размере, достаточном для оплаты комиссионного вознаграждения в соответствии с Тарифами Банка.

4.1.6. При необходимости пересчета комиссионного вознаграждения из одной валюты в другую валюту применяются курсы данных валют к рублю, установленные Банком России на дату списания комиссии.

4.1.7. Банк вправе отказать Клиенту в оказании услуг по настоящему Регламенту, а также в проведении операции по Счету с использованием Системы, при недостаточности средств для оплаты комиссионного вознаграждения, взимаемого Банком в соответствии с действующими Тарифами.

4.2.ИЗМЕНЕНИЕ И ДОПОЛНЕНИЕ РЕГЛАМЕНТА

4.2.1. Внесение изменений и дополнений в настоящий Регламент производится Банком самостоятельно в одностороннем порядке.

4.2.2. Для вступления в силу изменений и дополнений в Регламент, Банк соблюдает обязательную процедуру по предварительному раскрытию информации.

4.2.3. Предварительное раскрытие информации осуществляется Банком не позднее, чем за 10 (Десять) календарных дней до вступления в силу изменений или дополнений.

4.2.4. В случае если вносимые изменения связаны с приведением Регламента в соответствие с требованиями законодательства, то предварительное раскрытие информации осуществляется Банком не позднее, чем за 1 (Один) календарный день до вступления в силу изменений или дополнений

4.2.5. Любые изменения и дополнения в Регламенте с момента вступления в силу с соблюдением процедур настоящего раздела равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений в силу. В случае несогласия с изменениями или дополнениями, внесенными в Регламент Банком, Клиент имеет право до вступления в силу таких изменений или дополнений отказаться от Регламента в порядке, предусмотренном настоящим Регламентом.

4.2.6. Предварительное раскрытие информации осуществляется Банком путем обязательной публикацией полного текста изменений/новой редакции на информационных стендах в Банке и/или на сайте Банка «www.crosnabank.ru» в сети Интернет.

4.2.7. С целью обеспечения гарантированного ознакомления всех лиц, присоединившихся к Регламенту до вступления в силу изменений или дополнений, настоящим Регламентом установлена обязанность для Клиента:

- не реже 1 (Одного) раза в календарный месяц обращаться в Банк за сведениями об изменениях, произведенных в Регламенте и Тарифах Банка;

- не реже 1 (Одного) раза в неделю знакомиться с информацией на сайте Банка «www.crosnabank.ru» в сети Интернет;

- в сроки, установленные настоящим Регламентом, соединяться с Системой.

4.3.ОТВЕТСТВЕННОСТЬ СТОРОН.

4.3.1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение положений Регламента в соответствии с настоящим Регламентом и законодательством Российской Федерации.

4.3.2. Стороны несут ответственность за содержание любого ЭД, подписанного их ЭАСП.

4.3.3. Клиент самостоятельно несет все риски, связанные с невыполнением рекомендаций, установленных в Приложении № 5 Регламента.

4.3.4. Банк несет ответственность за несоблюдение сроков проведения расчетных операций по счету Клиента на основании надлежащим образом оформленных и своевременно доставленных ЭД Клиента в соответствии с действующим законодательством и условиями соответствующих договоров.

4.3.5. Банк не несет ответственность перед Клиентом:

- за убытки, понесенные Клиентом, в случае компрометации Закрытого ключа ЭАСП/Ключа доступа Клиента, если Клиент не известил о Банк о компрометации;

- за убытки, понесенные Клиентом, в случае блокирования работы Клиента в Системе на основании телефонного сообщения о компрометации Закрытого ключа ЭАСП/Ключа доступа с использованием Кодового слова Клиента;

- за убытки, понесенные Клиентом, в случае направления в Банк ЭД, в том числе РД, подписанного ЭАСП Владельца, полномочия которого прекращены (истечение срока полномочий, увольнение, смерть и т.п) если Банк не был своевременно уведомлен о таком прекращении;

- за последствия исполнения ЭД, выданных неуполномоченными лицами, в тех случаях, когда с использованием предусмотренных банковскими правилами и Регламентом процедур Банк не мог установить факта передачи ЭД неуполномоченными лицами;

- за принятие к исполнению подложных и недостоверных ЭД, если Проверка подлинности ЭД не смогла установить их недостоверность или подложность;

- за ошибочное перечисление (неперечисление) денежных средств, связанное с неправильным указанием Клиентом в Расчетных ЭД реквизитов получателя средств;

- за неправомерность и неправильность надлежащим образом оформленного Клиентом платежа, а также за убытки, понесенные Клиентом вследствие отказов и несвоевременных действий лиц, в пользу которых осуществляется расчетная операция по поручению Клиента;

- за отсутствие доступа к Системе по независящим от него причинам;

- за убытки, причиненные действием или бездействием Банка, обоснованно полагавшегося на ЭД Клиента, а также на информацию, утерявшую свою достоверность из-за несвоевременного доведения ее Клиентом до Банка;

- за неисполнение ЭД Клиента, направленных Банку с нарушением сроков и процедур, предусмотренных настоящим Регламентом;

- за убытки, понесенные Клиентом, в случае нарушения Клиентом положений настоящего Регламента.

4.3.6. Клиент несет ответственность за все операции в Системе до момента блокирования Банком работы Клиента в Системе в связи с компрометацией Закрытого ключа ЭАСП в соответствии с Регламентом.

4.3.7. Клиент несет перед Банком ответственность за убытки, причиненные Банку по вине Клиента, в том числе за ущерб причиненный Банку:

- в результате непредставления (несвоевременного представления) Клиентом любых документов, предоставление которых Банку предусмотрено настоящим Регламентом;

- в результате любого искажения информации, содержащейся в представленных Клиентом документах,

- в результате разглашения конфиденциальной информации;

- в результате несанкционированного доступа третьих лиц к Системе, произошедшего по вине Клиента;

- в результате невыполнения Клиентом рекомендаций, установленных в Приложении № 5 Регламента;

- в иных случаях.

4.3.8. Во всех случаях ущерба, причиненного Сторонами друг другу, размер возмещаемых убытков определяется в соответствии с действующим законодательством Российской Федерации.

4.4. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

4.4.1. Банк или иная сторона, присоединившаяся к настоящему Регламенту, освобождаются от ответственности за частичное или полное неисполнение обязательств, предусмотренных настоящим Регламентом, если оно явилось следствием обстоятельств непреодолимой силы, возникших после

присоединения к настоящему Регламенту, в результате событий чрезвычайного характера, которые они не могли ни предвидеть, ни предотвратить разумными мерами. К таким обстоятельствам будут относиться, но не исключительно: военные действия, массовые беспорядки, стихийные бедствия и забастовки, неисправность коммутируемых каналов связи, неисправность Интернета, сбои в компьютерных сетях, силовых электрических сетях или системах электросвязи, решения органов государственной и местной власти и управления, делающие невозможным исполнение обязательств, предусмотренных Регламентом.

4.4.2. Сторона, для которой создалась невозможность исполнения обязательств, предусмотренных Регламентом, должна в трехдневный срок уведомить другую заинтересованную сторону о наступлении обстоятельств непреодолимой силы и об их прекращении, при этом срок выполнения обязательств по Соглашению переносится соразмерно времени, в течение которого действовали такие обстоятельства

4.4.3. Указанное обязательство будет считаться выполненным Банком, если Банк осуществит такое извещение почтой или иным способом, предусмотренным настоящим Регламентом для распространения сведений об изменении Регламента.

4.4.4. Указанное обязательство будет считаться выполненным Клиентом, если он направит соответствующее сообщение в Банк по почте, предварительно направив копию этого сообщения в Банк по факсимильной связи.

4.4.5. Неизвещение или несвоевременное извещение Клиентом о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

4.4.6. После прекращения действия обстоятельств непреодолимой силы исполнение любой Стороной своих обязательств в соответствии с Регламентом должно быть продолжено в полном объеме.

4.5. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

4.5.1. Споры по настоящему Регламенту решаются в порядке, установленном действующим законодательством по месту нахождения Банка, а с Клиентом-физическим лицом в Пресненском районном суде города Москвы.

4.5.2. При возникновении споров по вопросам установления факта отправки или целостности и подлинности ЭД Клиента или Банка, Стороны обязаны соблюсти порядок, установленный в Приложении № 12 к Регламенту.

4.5.3. При несогласии одной из Сторон с результатами рассмотрения спора в порядке, установленным в Приложении № 12 к Регламенту, такая Сторона имеет право обратиться в суд в порядке, установленном п. 4.5.1. настоящего Регламента. В таком случае материалы разбора конфликтных ситуаций, результаты рассмотрения спора могут использоваться в качестве доказательств в суде.

4.5.4. При разрешении споров Электронные журналы используются в качестве подтверждения правомерности совершения операций и могут предъявляться в качестве доказательств в суде.

4.6. ОТКАЗ ОТ РЕГЛАМЕНТА

4.6.1. Правоотношения сторон могут быть прекращены путем отказа от Регламента.

4.6.2. Клиент имеет право в любой момент отказаться от присоединения к настоящему Регламенту.

Отказ Клиента от Регламента производится путем направления Банку письменного уведомления не менее чем за 5 (Пять) календарных дней до даты прекращения. Отказ вступает в силу по истечении 5 (Пяти) календарных дней с даты получения Банком письменного уведомления.

Уведомление должно быть направлено Клиентом по адресу, указанному в пункте 1.2 Регламента.

Отказ Клиента от Регламента не влечет за собой прекращение обязательств Клиента, возникших и не исполненных до даты отказа Клиента от Регламента, в том числе не влечет освобождения от оплаты неоплаченных услуг Банка в соответствии с Тарифами Банка, а также не освобождает Клиента от ответственности за нарушение принятых на себя в рамках Регламента обязательств и возмещения причиненных убытков.

4.6.3. Банк имеет право отказаться от исполнения настоящего Регламента в одностороннем порядке.

Отказ Банка от исполнения Регламента в отношении Клиента производится путем направления последнему письменного уведомления за 5 (Пять) календарных дней до даты прекращения. Отказ вступает в силу по истечении 5 (Пяти) календарных дней с даты направления Клиенту письменного уведомления.

Отказ Банка от Регламента не влечет за собой прекращение обязательств Клиента, возникших и не исполненных до даты отказа Банка от Регламента, а также не освобождает Клиента от ответственности за нарушение принятых на себя в рамках Регламента обязательств и возмещения причиненных убытков.

4.6.4. Действие Соглашения между Банком и Клиентом в рамках настоящего Регламента прекращается с даты закрытия Счета Клиента в Банке, а в случае если Клиенту открыто в Банке несколько Счетов, то с даты закрытия последнего из таких Счетов.

Наступление даты прекращения действия Соглашения в рамках настоящего Регламента не влечет за собой прекращения обязательств Сторон, возникших и не исполненных до даты прекращения действия Соглашения в рамках настоящего Регламента, а также не освобождает Стороны от ответственности за нарушение принятых на себя в соответствии с Регламентом обязательств и возмещения причиненных убытков.

ПРИЛОЖЕНИЯ

Приложение № 1 «Заявление юридического лица на банковское обслуживание с применением системы «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ “Кросна-Банк” (ОАО)»

Приложение № 2 «Заявление индивидуального предпринимателя на банковское обслуживание с применением системы «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ “Кросна-Банк” (ОАО)»

Приложение № 3 «Заявление физического лица на банковское обслуживание с применением системы «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ “Кросна-Банк” (ОАО)»

Приложение № 4 Акт признания открытого ключа

Приложение № 5 «ПЕРЕЧЕНЬ электронных документов»

Приложение № 6 «Рекомендации Клиенту по обеспечению безопасности использования системы «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ “Кросна-Банк” (ОАО)»

Приложения № 7 «Информационное письмо об уполномоченном сотруднике/лице и изменении сочетания *электронных аналогов собственноручной подписи* (ЭАСП), необходимых для подписания документов, содержащих распоряжение Клиента в Системе «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАОИнформационное письмо об уполномоченном сотруднике/лице»

Приложение № 7а «Информационное письмо о лице, уполномоченном использовать Ключ доступа к **с**истеме «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)»

Приложение № 8 «Требования к программно-аппаратному обеспечению для установки системы «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ “Кросна-Банк” (ОАО)»»

Приложение № 9 «Опись комплекта для подключения к Системе»

Приложение № 10 «Уведомление о компрометации закрытого ключа ЭП»

Приложение № 11 «Акт выполненных работ»

Приложение № 12 «Порядок разбора конфликтных ситуаций»

Приложение 1

Заявление юридического лица
№_____ от «___» _____ 20__ г.
на банковское обслуживание с применением Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

Заявитель
(полное наименование юридического лица)**:** _____

В лице: _____

действующего на основании _____

Место нахождения: _____

_____

Почтовый адрес: _____

_____

Телефон ответственного за взаимодействие по Системе «Электронный Банк-Клиент»: _____

ИНН: _____ ОГРН: _____ Расчетный счет: _____

Настоящим заявляю о присоединении к условиям (акцепте условий) Регламента банковского обслуживания с применением Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО) (далее — «Регламент») в порядке, предусмотренном ст. 428 Гражданского Кодекса Российской Федерации.

Все положения тарифов АКБ «Кросна-Банк» (ОАО) и Регламента разъяснены мне в полном объеме, включая правила внесения в Регламент изменений и дополнений.

Количество *электронных аналогов собственноручной подписи* (ЭАСП), необходимых для подписания электронного документа

☐ - одна подпись;

☐ - две подписи.

Прошу зарегистрировать в Системе «Электронный Банк-Клиент» ЭАСП для следующих уполномоченных лиц (Владельцев ЭАСП) и их следующие сочетания (*в пустых полях поставить прочерки):

1. Ф.И.О _____
Должность _____
Ф.И.О _____
Должность _____
2. Ф.И.О _____
Должность _____
Ф.И.О _____
Должность _____

Прошу зарегистрировать в Системе «Электронный Банк-Клиент» Ключ доступа для следующих уполномоченных лиц (Владельцев Ключа доступа) (*в пустых полях поставить прочерки; в отношении указанных лиц прилагаются все документы, необходимые для установления личности лица (лиц), уполномоченных использовать Ключ доступа, и согласие на обработку персональных данных:

1. Ф.И.О _____
2. Ф.И.О _____

Прошу предоставить дополнительные услуги в соответствии с Тарифами Банка:

☐ выезд специалиста Банка для настройки *АРМ Клиента* ☐ предоставить код активации СКЗИ КриптоПро CSP 3.6

☐ «SMS-оповещение» на телефонный номер: ☐ предоставить Токен

☐ «E-mail–оповещение» на адрес эл.почты:

(должность руководителя юридического лица) (подпись) (Ф.И.О.)

М. П. « _____ » _____ 20 _____ г.

Для служебных пометок АКБ «Кросна-Банк» (ОАО)	
Заявку принял(а): _____/_____/	
Присоединение к Регламенту согласовано «____» _____ 20____ г.	
Председатель Правления _____/_____/	М. П.

Приложение 2

Заявление индивидуального предпринимателя

№_____ от «___» _____ 20___ г.

на банковское обслуживание с применением Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

Заявитель

(Ф.И.О. полностью)**:** _____

Данные документа,
удостоверяющего личность:
(серия, номер, дата выдачи,
орган, выдавший документ) _____

Место жительства: _____

_____

Почтовый адрес: _____

_____

Телефон ответственного за взаимодействие по Системе «Электронный Банк-Клиент»: _____

ИНН: _____ ОГРНИП: _____ Расчетный счет: _____

Настоящим заявляю о присоединении к условиям (акцепте условий) Регламента банковского обслуживания с применением Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО) (далее — «Регламент») в порядке, предусмотренном ст. 428 Гражданского Кодекса Российской Федерации.

Все положения тарифов АКБ «Кросна-Банк» (ОАО) и Регламента разъяснены мне в полном объеме, включая правила внесения в Регламент изменений и дополнений.

Прошу зарегистрировать *электронные аналоги собственноручной подписи* (ЭАСП) в Системе «Электронный Банк-Клиент» для следующих уполномоченных лиц – Владельцев ЭАСП (должность, Ф.И.О.)

Прошу зарегистрировать в Системе «Электронный Банк-Клиент» Ключ доступа для следующих уполномоченных лиц (Владельцев Ключа доступа) (*в пустых полях поставить прочерки; в отношении указанных лиц прилагаются все документы, необходимые для установления личности лица (лиц), уполномоченных использовать Ключ доступа, и согласие на обработку персональных данных):

1. Ф.И.О _____
2. Ф.И.О _____

Прошу предоставить дополнительные услуги в соответствии с Тарифами Банка:

☐ предоставить код активации СКЗИ КриптоПро CSP 3.6 ☐ предоставить Токен

☐ выезд специалиста Банка для настройки *АРМ Клиента*

☐ «SMS-оповещение» на телефонный номер: _____

☐ «E-mail–оповещение» на адрес эл.почты: _____

_____ _____

(подпись) (Ф.И.О.)

М. П. « ____ » _____ 20 ____ г.

Для служебных пометок АКБ «Кросна-Банк» (ОАО)

Заявку принял(а): _____/_____/

Присоединение к Регламенту согласовано «____» _____ 20____ г.

Председатель Правления _____/_____/ М. П.

Приложение 3

Заявление физического лица

№_____ от «___» _____ 20___ г.

на банковское обслуживание с применением Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

Заявитель
(Ф.И.О. полностью)**:** _____

Данные документа,
удостоверяющего личность:
(серия, номер, дата выдачи,
орган, выдавший документ) _____

Место жительства: _____

_____

Почтовый адрес: _____

_____

Телефон ответственного за взаимодействие по Системе «Электронный Банк-Клиент»: _____

Расчетный счет: _____

Настоящим заявляю о присоединении к условиям (акцепте условий) Регламента банковского обслуживания с применением Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО) (далее — «Регламент») в порядке, предусмотренном ст. 428 Гражданского Кодекса Российской Федерации.

Все положения тарифов АКБ «Кросна-Банк» (ОАО) и Регламента разъяснены мне в полном объеме, включая правила внесения в Регламент изменений и дополнений.

Прошу зарегистрировать *электронные аналоги собственноручной подписи* (ЭАСП) в Системе «Электронный Банк-Клиент» для следующих уполномоченных лиц – Владельцев ЭАСП (Ф.И.О.)

Прошу зарегистрировать в Системе «Электронный Банк-Клиент» Ключ доступа для следующих уполномоченных лиц (Владельцев Ключа доступа) (*в пустых полях поставить прочерки; в отношении указанных лиц прилагаются все документы, необходимые для установления личности лица (лиц), уполномоченных использовать Ключ доступа, и согласие на обработку персональных данных):

1. Ф.И.О _____
2. Ф.И.О _____

Прошу предоставить дополнительные услуги в соответствии с Тарифами Банка:

☐ предоставить код активации СКЗИ КриптоПро CSP 3.6 ☐ предоставить Токен

☐ выезд специалиста Банка для настройки *АРМ Клиента*

☐ «SMS-оповещение» на телефонный номер: _____

☐ «E-mail–оповещение» на адрес эл.почты: _____

Подтверждаю, что до подписания настоящей Заявки я информирован Банком обо всех условиях обслуживания, взаимных правах и обязанностях, зафиксированных в Регламенте.

(подпись) (Ф.И.О.)

« ____ » _____ 20 ____ г.

Для служебных пометок АКБ «Кросна-Банк» (ОАО)

Заявку принял(а): _____/_____/

Присоединение к Регламенту согласовано «____» _____ 20____ г.

Председатель Правления _____/_____/ М. П.

Приложение 4

Акт
признания открытого ключа
от «____» _____ 20__ года

_____

(наименование, Ф.И.О. Клиента, ОГРН (при наличии))

Соглашения № _____ от _____

Сведения о Владельце Электронного аналога собственноручной подписи (ЭАСП):

1. Ф.И.О. _____
2. паспорт: _____
3. Должность _____

Открытый ключ ЭАСП:

ОСОБЫЕ ОТМЕТКИ **□ ДА □ НЕТ**	**применяется режим Ключа доступа в соответствии с Регламентом банковского обслуживания с применением системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО) - предназначен исключительно для аутентификации Клиента при входе в Систему «Электронный Банк-Клиент» и не предназначен для создания ЭАСП с использованием СКЗИ и обмена электронными документами ЭД.**

Сведения об Открытом ключе ЭАСП не являются конфиденциальной информацией и носят открытый характер. Настоящим подтверждаю, что с Регламентом банковского обслуживания с применением системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО) и иными документами с ним связанными ознакомлен(а).

Подпись Владельца ЭАСП

_____ (_____)
«_____»_____ 20___г.

Подпись Клиента физического лица/руководителя Клиента-юридического лица

_____ (_____)
«____» _____ 20___ г.

М.П.

Настоящий Акт составлен в 1-м подлинном экземпляре для АКБ «Кросна-Банк» ОАО.

Для служебных пометок АКБ «Кросна-Банк» (ОАО)

АКТ принял(а): _____/_____/

«____» _____ 20____ г.

Дата начала действия Открытого ключа ЭАСП «____» _____ 20____ г.

_____ _____/_____/
(должность)

М. П.

Приложение 5

Перечень электронных документов (ЭД),
используемых в Системе «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

№п.п.	Наименование ЭД	Расчетный ЭД	Прикрепление файлов
1.	Платежное поручение	да	нет
2.	Запрос на отзыв документа	нет	нет
3.	Запрос на получение выписки	нет	нет
4.	Выписка	нет	нет
5.	Произвольный документ в банк	нет	да
6.	Зарплатная ведомость	да	нет
7.	Квитанция банка	нет	нет
8.	Произвольный документ из банка*	нет	да

* - документ, переданный в виде вложения с вложенным отдельным файлом ЭАСП.

В форме произвольных документов Стороны могут обмениваться договорами, заявлениями, справками, письмами, уведомлениями, сообщениями.

Приложение 6

Рекомендации по обеспечению безопасного использования Системы

«Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

1. Общие рекомендации

1.1. Ограничьте доступ посторонних лиц к компьютеру, с установленным АРМ Клиента;

1.2. Установите пароль на вход в операционную систему;

1.3. Блокируйте Рабочий стол компьютера при перерывах в работе с Системой;

1.4. Подключите услугу «SMS-оповещение» или «E-mail-оповещение» . Это позволит Вам в реальном времени получать информацию об операциях по счетам и своевременно предпринять меры по приостановке несанкционированного распоряжения;

1.5. При увольнении ответственного сотрудника, имевшего доступ к Закрытому ключу ЭАСП/Ключу доступа, проводите внеплановую перегенерацию Закрытого ключа ЭАСП. Для этого позвоните в Банк по телефону (495) 913-77-59 (пн. – чт. с 9:00 до 18:00, пт. с 9:00 до 17:00);

1.6. Рекомендуем также выделить отдельный компьютер (ноутбук), который будет использоваться только для работы с Системой;

1.7. Не сообщайте свои пароли третьим лицам, в том числе сотрудникам Банка;

1.8. Не храните пароли в текстовых файлах;

1.9. Меняйте пароли не реже 1 раза в год;

1.10. Не используйте на компьютере с установленным АРМ Клиента сторонние средства удаленного доступа к рабочему столу, таких как TeamViewer или DameWare Remote Control, и удаленное администрирование, чтобы не подвергать АРМ Клиента риску негласного удаленного доступа. Исключением является встроенное средство удаленного доступа к рабочему столу - Удаленный помощник Windows, используемый в том числе Службой технической поддержки Банка для оказания удаленной помощи.

1.11. При появлении предупреждений безопасности обозревателя Internet Explorer немедленно обратитесь в Службу технической поддержки Банка. Так сообщение Internet Explorer «Ошибка в сертификате безопасности этого веб-узла» может говорить о том, что вы попали на ложный (фальсифицированный) ресурс.

2. Рекомендации по защите Закрытого ключа ЭАСП/Ключа доступа

2.1. Храните ключевой носитель (USB-флеш накопитель, token) в сейфе или хранилище, обеспечивающем его сохранность;

2.2. Ни в коем случае не храните Закрытый ключ ЭАСП/Ключ доступа на жестком диске (в реестре компьютера);

2.3. Если Вы используете в качестве носителя закрытого ключа ЭАСП USB-флеш накопитель, не используйте его для других целей;

2.4. Подключайте ключевой носитель с Закрытым ключом ЭАСП/Ключом доступа к компьютеру непосредственно перед началом работы с системой ДБО. Завершив работу, сразу извлекайте ключевой носитель из компьютера;

2.5. После использования Закрытого ключа ЭАСП/Ключа доступа, помещайте ключевой носитель в сейф;

2.6. Не передавайте Закрытый ключ ЭАСП/Ключ доступа третьим лицам;

2.7. При изготовлении нового Закрытого ключа ЭАСП\Ключа доступа установите пароль (ПИН) ключевого контейнера;

2.8. При вводе пароля (ПИНа) ключевого контейнера не устанавливайте флажок «запомнить».

2.9. В случае, если у Вас появились основания подозревать, что Закрытый ключ ЭАСП\Ключ доступа утрачен и (или) его используют без Вашего согласия и (или) Закрытый ключ ЭАСП\Ключ доступа скомпрометирован иным образом, срочно обратитесь в Банк по телефону (495) 913-77-59, сообщите Кодовое слово и попросите заблокировать Закрытый ключ ЭАСП\Ключ доступа, после чего в соответствии с Регламентом направьте в Банк Уведомление о компрометации Закрытый ключ ЭАСП\Ключ доступа и инициируйте процесс перегенерации Закрытый ключ ЭАСП\Ключ доступа.

3. Рекомендации по защите Пароля для входа в Систему (далее – «Пароль»)

3.1. Клиенту рекомендуется ограничить круг лиц, знающих Пароль.

3.2. Рекомендуется самостоятельно изменять Пароль не реже 1 раза в год, а также в случае изменения должностных обязанностей лиц, знающих Пароль.

4. Рекомендации по использованию списков доступа на основе MAC- и IP-адресов АРМ Клиента

4.1. При подключении к Системе Банк регистрирует локальный и публичный IP-адреса, а также MAC-адрес компьютера с которого осуществляется доступ в Систему и автоматически заносит их в список допустимых адресов Клиента. MAC-адрес является уникальным идентификатором сетевого интерфейса компьютера. Публичный IP-адрес компьютера изменяется в зависимости от точки подключения к Интернет, а локальный IP-адрес зависит от настроек локальной сети. Таким образом, внесение MAC-адреса в список доступа исключает доступ к АРМ Клиента с другого компьютера, внесение публичного IP-адреса исключает доступ из другой точки подключения к Интернет, внесение локального IP-адреса исключает доступ к АРМ Клиента при изменении сетевых параметров локальной вычислительной сети. Изменение списка доступа производится Службой технической поддержки Банка по запросу Клиента. Все три адреса отображаются на главной страницы АРМ Клиента. Попытка входа в Систему с компьютера или точки его подключения к Интернет, адреса которых не внесены в список доступа будет автоматически блокирована. В этом случае необходимо обратиться в Службу технической поддержки Банка и назвать Кодовое слово, чтобы новые адреса АРМ Клиента были добавлены в список доступа. Рекомендуется составлять список адресов доступа к АРМ Клиента таким образом, чтобы максимально исключить возможность несанкционированного доступа к Системе:

4.1.1. Если АРМ Клиента установлен на стационарный компьютер со статическим IP-адресом следует внести в список доступа все три адреса компьютера;

4.1.2. Если АРМ Клиента установлен на стационарный компьютер с динамическим IP-адресом следует внести в список доступа MAC-адрес и публичный IP-адрес компьютера;

4.1.3. Если АРМ Клиента установлен на переносной компьютер, работа с Системой на котором производится с ограниченного числа мест, например либо из дома, либо из офиса следует внести в список доступа MAC-адрес компьютера и публичные IP-адреса компьютера для каждого из подключений к Интернет;

4.1.4. Если АРМ Клиента установлен на переносной компьютер, работа с Системой на котором производится с неограниченного числа мест, следует внести в список доступа только MAC-адрес компьютера.

4.2. Не забывайте обратиться в Службу технической поддержки Банка когда вы перестали использовать компьютер или используемую ранее точку подключения к Интернет, чтобы исключить ее из списка доступа.

5. Рекомендации по антивирусной защите

5.1. Самая эффективная защита от вирусов (вредоносных программ) - использование при работе на компьютере учетной записи с правами рядового пользователя, т.е. не обладающей правами администратора компьютера. Для этого необходимо убедиться, что учетная запись, с использованием которой происходит вход в Windows, входит только в одну группу «Пользователи»;

5.2. Используйте при работе на компьютере брандмауэр и антивирусную программу и следите за ее регулярным обновлением;

5.3. Не устанавливайте программы, полученные (загруженные) из ненадежных источников. Используйте лицензионное программное обеспечение;

5.4. Не посещайте интернет-сайты сомнительного содержания;

5.5. Не открывайте неизвестные файлы, не переходите по неизвестным ссылкам присланным на e-mail, через соцсети, в них могут содержаться вирусы;

5.6. Периодически анализируйте какие процессы (диспетчер задач Windows) и сетевые подключения (команда «netstat –b») в Windows активны во время работы с АРМ Клиента, какие программы и службы Windows настроены на автоматический запуск (команда «msconfig»). При обнаружении подозрительных программ и активности, примите меры по их удалению с компьютера.

6. Рекомендации по эксплуатации СКЗИ

6.1. Установка СКЗИ допускается только с дистрибутивного диска Системы, полученного в Банке или другого дистрибутива, полученного по доверенному каналу.

6.2. При эксплуатации СКЗИ необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К).

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

6.4. В целях обеспечения безопасности информации при ее защите СКЗИ, Клиенту, осуществляющему эксплуатацию сертифицированных средств СКЗИ, рекомендуется руководствоваться требованиями ФАПСИ/ФСБ по обеспечению безопасности информации при ее защите по уровню “С” (на уровне потребителя), изложенными ниже.

6.5. Защита информации по уровню “С” означает применение процедур электронной цифровой подписи и хеширования сертифицированных ФАПСИ/ФСБ средств криптографической информации, реализующих алгоритмы ГОСТ Р34.11-94, ГОСТ Р34.10-94 и ГОСТ 28147-89.

6.6. Требования по организационному обеспечению эксплуатации СКЗИ

6.6.1. У Клиента выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СКЗИ.

6.6.2. У Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ.

6.6.3. К работе со СКЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СКЗИ.

6.7. Требования по размещению СКЗИ и режиму охраны

6.7.1. Помещения, в которых размещаются программно-технические средства со встроенными СКЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ.

6.7.2. Размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств.

6.7.3. Размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

6.7.4. Входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время.

6.7.5. Окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией.

6.7.6. Размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна.

6.7.7. В режимные помещения допускаются Руководство Пользователя, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов.

6.7.8. Системные блоки ЭВМ со СКЗИ оборудуются средствами контроля вскрытия.

6.7.9. Ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СКЗИ (возможно согласование с Организатором Системы)

6.8. Требования по обеспечению безопасности ключевой информации

6.8.1. Ключевой носитель СКЗИ и инсталляционные дискеты с ПО СКЗИ берутся Клиентом на поэкземплярный учет в выделенных для этих целей журналах.

6.8.2. Учет и хранение Ключевых носителей СКЗИ Клиент организует самостоятельно.

6.8.3. Для хранения Ключевых носителей СКЗИ выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации.

6.8.4. Хранение Ключевых носителей СКЗИ и инсталляционных дискет с ПО СКЗИ допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

6.8.5. При транспортировке Ключевого носителя СКЗИ обеспечиваются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

Приложение 7

Информационное письмо об уполномоченном сотруднике/лице и изменении
сочетания *электронных аналогов собственноручной подписи* (ЭАСП),
необходимых для подписания документов, содержащих распоряжение Клиента
в Системе «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

Настоящим, [наименование Клиента — юридического лица, ОГРН, ИНН, в лице уполномоченного лица, действующего на основании учредительного документа или Ф.И.О., место жительства и паспортные данные Клиента — физического лица] уведомляет АКБ «Кросна-Банк» (ОАО) о том, что уполномоченным сотрудником/лицом, уполномоченным распоряжаться денежными средствами с использованием электронного аналога собственноручной подписи в Системе «ЭЛЕКТРОННЫЙ БАНК КЛИЕНТ» АКБ «Кросна-Банк» (ОАО) является с «___» _____ 20__ г:

Ф.И.О.:	
Данные документа, удостоверяющего личность:	
Должность:	
Основание:	
Статус ЭАСП	☐ - одна подпись; ☐ - две подписи
Возможные сочетания ЭАСП с другими подписями Владельцев ЭАСП, необходимых для подписания электронного документа	**1.**_____; _____. **2.**_____; _____.
Приложения:	1. копия приказа № _____ от _____ на ____ л.;
	2. копия доверенности № _____ от _____ на _____ л.;

_____ _____ _____
(должность руководителя юридического лица) (подпись) (Ф.И.О.)

М. П. _____ 20 _____ г.

Приложение 7а

Информационное письмо о лице, уполномоченном использовать Ключ доступа

к **с**истеме «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

Настоящим, [наименование Клиента — юридического лица, ОГРН, ИНН, в лице уполномоченного лица, действующего на основании учредительного документа или Ф.И.О., место жительства и паспортные данные Клиента — физического лица] уведомляет АКБ «Кросна-Банк» (ОАО) о том, что уполномоченным сотрудником/лицом, уполномоченным использовать Ключ доступа к Системе «ЭЛЕКТРОННЫЙ БАНК КЛИЕНТ» АКБ «Кросна-Банк» (ОАО) является с «___» _____ 20__ г:

Ф.И.О.:	
Данные документа, удостоверяющего личность:	
Приложения:	

(должность руководителя юридического лица)	(подпись)	(Ф.И.О.)

М. П. _____ 20 _____ г.

Приложение 8

ТРЕБОВАНИЯ К ПРОГРАММНО-АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

ДЛЯ УСТАНОВКИ СИСТЕМЫ «ЭЛЕКТРОННЫЙ БАНК-КЛИЕНТ» АКБ «КРОСНА-БАНК» (ОАО)

Требования к компьютеру АРМ Клиента

Аппаратные требования:

Видеосистема, обеспечивающая область экрана не менее 1024x768 пикселей;

USB-порт или накопитель на гибких магнитных дисках;

Модем (для резервного подключения к Системе по коммутируемым каналам связи);

Требования к программному обеспечению (ПО):

операционная система Microsoft Windows версий XP x86, Vista x86, Windows Server 2008, Windows 7 x86/x64, Windows 8 x86/x64;

ПО для работы с Токеном (в случае использования его в качестве *ключевого носителя*);

32-разрядный интернет-обозреватель Internet Explorer версий 7.0, 8.0, 9.0, 10;

Перечень программного обеспечения (ПО) АРМ Клиента

СКЗИ КриптоПро CSP 3.6 R3.

Содержание дистрибутивного диска АРМ Клиента

\CryptoPro 3.6 R3 - СКЗИ КриптоПро CSP версии 3.6 и документация к СКЗИ;

\Docs – документация:

\Docs\Руководство по внеплановой смене ключей ЭП.pdf;

\Docs\Руководство по изготовлению нового ключа ЭП.pdf;

\Docs\Руководство по настройке модемного соединения.pdf;

\Docs\Руководство по плановой смене ключей ЭП.pdf;

\Docs\Руководство по подключению к Системе.pdf;

\Docs\Руководство по проверке подлинности ЭД.pdf;

\Docs\Руководство по уничтожению закрытого ключа ЭП.pdf;

\Docs\Руководство по использованию ДБО BS-Client.pdf;

\eToken - ПО для работы с Токеном;

\ Пригласить техподдержку x64.exe – установочный пакет для оказания удаленной помощи для 64-разрядной версии Windows;

\ Пригласить техподдержку x86.exe – установочный пакет для оказания удаленной помощи для 32-разрядной версии Windows.

Режим работы

Вид работ	Режим
Доступ в Систему	Круглосуточно
Прием ЭД	Круглосуточно
Обработка ЭД	В соответствии с договором банковского обслуживания
Техническая поддержка	пн-чт 9:00 – 18:00 пт 9:00 – 17:00
Технологические перерывы доступа в Систему	Ежедневно продолжительностью не более 10-ти минут около 19:00 и около 00:00

Технические характеристики

Наименование характеристики	Значение характеристики
Применяемая разработка	Система "ДБО BS-Client v.3"
Разработчик	ООО “Банк’с софт системс”
Сайт разработчика	http://bssys.com
Стандарт ЭАСП и аутентификации сервера	ГОСТ Р 34.11/34.10-2001
Длина ключа ЭАСП и ключа аутентификации сервера, бит	512
Протокол шифрования и аутентификации сервера	HTTPS/TLS
Стандарт шифрования	ГОСТ 28147-89 с обменом ключей по алгоритму Диффи-Хеллмана и хэширования в соответствии с ГОСТ 34.11-94
Удостоверяющий центр, выпустивший сертификат аутентификации сервера Системы	УЦ КРИПТО-ПРО
Стандарт аутентификации сервера Системы	ГОСТ Р 34.11/34.10-2001
Длина ключа аутентификации сервера Системы, бит	512
Максимальный объем прикрепленных к ЭД файлов, Мб	3
Способы подключения к Системе	Интернет, Коммутируемый удаленный доступ (модемное соединение)

Приложение 9

Опись
комплекта для подключения к Системе «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО), передаваемых АКБ «Кросна-Банк» (ОАО) Клиенту

В соответствии с Регламентом банковского обслуживания с применением Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО) для установки Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО) передает уполномоченному представителю [*наименование Клиента*] следующие Средства доступа к Системе:

дистрибутивный диск АРМ Клиента — 1 шт.;

eToken [*серийный номер*] — 1 шт.;

конверт с паролями — 1 шт.;

код активации СКЗИ Крипто-Про CSP 3.6 – 1 шт.;

заверенная копия Акта признания открытого ключа ЭП Банка — 1 экз.

Передал:	Принял:
Уполномоченный представитель Банка	Уполномоченный представитель Клиента
(Ф.И.О., должность, подпись)	(Ф.И.О., должность, реквизиты доверенности, подпись)
« » 20 г.	« » 20 г.

Приложение 10

Уведомление о компрометации закрытого ключа ЭАСП
Системы «Электронный Банк-Клиент» АКБ «Кросна-Банк» (ОАО)

Настоящим, [наименование Клиента — юридического лица, ОГРН, ИНН, в лице уполномоченного лица, действующего на основании соответствующего документа или Ф.И.О., место жительства и паспортные данные Клиента — физического лица] уведомляет АКБ «Кросна-Банк» (ОАО) о том, что « ___» _____ 20_____ г. произошла компрометация Закрытого ключа ЭАСП [наименование *Владельца ЭАСП*]/Ключа доступа.

Просим зарегистрировать новые Ключи ЭАСП для [наименование *Владельца ЭАСП*]/Ключ доступа в Системе «Электронный Банк-Клиент».

Уполномоченный представитель Клиента

(Ф.И.О., должность, реквизиты доверенности, подпись, печать)

« ___» _____ 20____ г.

Приложение 11

Акт выполненных работ
специалистом АКБ «Кросна-Банк» (ОАО)

АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «КРОСНА-БАНК» (ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО) в лице [*должность, Ф.И.О. лица, обладающего правом подписывать настоящий Акт электронной подписью Банка*], действующего на основании [*реквизиты приказа или доверенности*], именуемый в дальнейшем «Банк», с одной стороны, и [*наименование Клиента — юридического лица, ОГРН, ИНН, в лице уполномоченного лица, действующего на основании соответствующего документа или Ф.И.О., место жительства и паспортные данные Клиента — физического лица*], именуемый в дальнейшем «Клиент», с другой стороны, совместно именуемые «Стороны», составили настоящий Акт о нижеследующем:

Специалист Банка выполнил а Клиент принял выполнение следующих работы по оказанию технической поддержки по месту установки *АРМ Клиента:*
_____
_____
_____;

Клиент не имеет претензий к Банку.

Настоящий Акт составлен в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

Уполномоченный представитель Банка	Уполномоченный представитель Клиента
(Ф.И.О., должность, подпись)	(Ф.И.О., должность, реквизиты доверенности, подпись)
« » 20 г.	« » 20 г.

Приложение 12

ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ

ОБЩИЕ ПОЛОЖЕНИЯ

1. Любые споры между Банком и Клиентом, предметом которых является установление факта отправки или подлинности ЭД Клиента или Банка передаются для разрешения специально создаваемой Экспертной комиссии. Для консультации могут привлекаться независимые эксперты.

2. В соответствии с настоящим Приложением к Регламенту подлежат разрешению конфликтные ситуации следующих типов:

1 тип - утверждение Клиента о факте отправки ЭД, который отсутствует у Банка;

2 тип – утверждение Клиента о факте отсутствия ЭД, который направил Клиенту Банк

2 А тип -утверждение Банка о направлении ЭД Клиенту, получение, которого Клиент отрицает.

3 тип – отрицание Клиентом факта отправки ЭД, который получил и обработал Банк.

4 тип – отрицание Клиентом подлинности ЭД, который получен и обработан Банком;

3. В связи с тем, что Стороны установили, что выписки по Счету считаются подтвержденными, если КЛИЕНТ не представит письменные замечания в течение 10 (Десяти) календарных дней с даты предоставления выписки, претензии по конфликтным ситуациям ТИП 1, ТИП 3,ТИП 4 полученные Банком по истечении указанного срока не принимаются и не рассматриваются.

4. Претензии по конфликтным ситуациям направляются:

ТИП 2 - не позднее 14 (Четырнадцати) рабочих дней с момента, когда Клиент узнал о направлении Банком ЭД;

ТИП 2а – не позднее 14 (Четырнадцати) рабочих дней с момента, когда Банк узнал о неполучении Клиентом ЭД;

Претензии направленные по истечении указанных сроков не принимаются и не рассматриваются.

5. Экспертная комиссия созывается Банком по своей инициативе и/или на основании письменной претензии Клиента. В указанной претензии Клиент, помимо реквизитов оспариваемого ЭД, также должен указать лиц, уполномоченных представлять интересы Клиента в составе Экспертной комиссии. При отсутствии в претензии сведений о представителях Клиента претензия к рассмотрению не принимается.

6. Письменная претензия направляется заказным письмом с уведомлением о вручении, либо курьером.

7. Не позднее 7 (Семи) рабочих дней с момента получения надлежаще оформленной претензии Банк назначает своих представителей в Экспертную комиссию и дату и время начала работы Экспертной комиссии. Банк письменно, не позднее чем за 3 (три) рабочих дня, уведомляет Клиента о своих представителях в Экспертной комиссии и назначенной дате и времени начала работы Экспертной комиссии. Экспертная комиссия осуществляет свою работу на территории Банка.

8. Если причиной возникновения конфликта является нарушение целостности программного обеспечения, произошедшего в результате сбоев аппаратуры, действия компьютерных вирусов или программ, в том числе полученных через сеть Интернет, то Банк имеет право отказать в создании Экспертной комиссии.

9. Экспертная комиссия может созываться Банком по своей инициативе на основании письменного документа о создании Экспертной комиссии, направляемого Банком Клиенту. В указанном документе Банк, помимо реквизитов оспариваемого ЭД, также должен указать лиц, уполномоченных представлять интересы Банка в составе Экспертной комиссии и назначить дату и время начала работы Экспертной комиссии.

10. Полномочия членов Экспертной комиссии подтверждаются доверенностями.

Состав Экспертной комиссии формируется в равных пропорциях из представителей Банка и Клиента, при этом он должен быть не менее чем 4 человека и не более чем 10 человек. Со стороны Банка в состав Экспертной комиссии в обязательном порядке входит не менее 1 сотрудника Службы технической поддержки Банка.

11. Экспертиза ЭД осуществляется на предоставленном Банком персональном компьютере, конфигурация и характеристики которого соответствуют требованиям, зафиксированным в Регламенте.

12. Экспертиза оспариваемого ЭД осуществляется в присутствии всех членов Экспертной комиссии.

13. Стороны договариваются, что для разбора конфликтных ситуаций комиссия принимает на рассмотрение ЭД и подтверждения по ним и обязана использовать следующие, признаваемые сторонами, эталонные данные:

- ЭД в виде файлов .dat и .sig;

- подписанный Акт признания открытого ключа ЭАСП;

- дистрибутив СКЗИ, полученный по доверенному каналу от разработчика СКЗИ;

- дистрибутив Средства проверки ЭАСП, полученный по доверенному каналу от разработчика Средства проверки ЭАСП.

14. При рассмотрении споров Стороны руководствуются настоящим Регламентом и действующим законодательством, а так же тем, что математические свойства алгоритма ЭАСП, реализованного в соответствии с требованиями стандартов Российской Федерации ГОСТ Р 34.10-94 и ГОСТ Р 34.11-94, свидетельствуют о невозможности подделки значения ЭАСП любым лицом, не обладающим Закрытым ключом ЭАСП.

15. Результаты экспертизы оформляются в виде письменного заключения - Акта Экспертной комиссии, подписываемого всеми членами комиссии. Акт составляется немедленно после завершения экспертизы. В Акте фиксируются результаты всех этапов, проведенной экспертизы, а также все существенные реквизиты оспариваемого ЭД. Акт составляется в двух экземплярах - по одному для представителей Банка и Клиента. Акт комиссии является окончательным и пересмотру не подлежит.

16. Подтверждение факта отправки или подлинности ЭД Клиента, зафиксированное в Акте, будет означать, что этот ЭД имеет юридическую силу и является законным основанием для осуществленных Банком операций по Счету Клиента.

17. В случае отказа от подписания Акта Экспертной комиссии представителями Клиента, в Акте Экспертной Комиссии делается отметка о таком отказе и Акт вступает в силу с момента его подписания только представителями Банка.

18. Стороны признают, что Акт, составленный Экспертной комиссией, является обязательным для Сторон и может служить доказательством при дальнейшем разбирательстве спора в суде.

19. В случае отсутствия согласия по спорным вопросам и добровольного исполнения решения Экспертной комиссии, все материалы по этим вопросам могут быть переданы на рассмотрение суда.

ПОРЯДОК РАЗБОРА КОНФЛИКТНОЙ СИТУАЦИИ

ТИП 1 –«УТВЕРЖДЕНИЕ КЛИЕНТА О ФАКТЕ ОТПРАВКИ ЭД, КОТОРЫЙ ОТСУТСТВУЕТ У БАНКА»

- Если Клиент предъявляет ЭД, конфликтная ситуация разрешается в пользу Клиента.

-Если Клиент не может предъявить ЭД конфликтная ситуация разрешается в пользу Банка.

ТИП 2 «УТВЕРЖДЕНИЕ КЛИЕНТА О ФАКТЕ ОТСУТСТВИЯ ЭД, КОТОРЫЙ НАПРАВИЛ КЛИЕНТУ БАНК»

ТИП 2 А «УТВЕРЖДЕНИЕ БАНКА О НАПРАВЛЕНИИ ЭД КЛИЕНТУ, ПОЛУЧЕНИЕ, КОТОРОГО КЛИЕНТ ОТРИЦАЕТ»

- Если Банк предъявляет спорный ЭД, конфликтная ситуация разрешается в пользу Банка.

- Если Банк не может предъявить спорный ЭД, конфликтная ситуация разрешается в пользу Клиента.

ТИП 3 «ОТРИЦАНИЕ КЛИЕНТОМ ФАКТА ОТПРАВКИ ЭЛЕКТРОННОГО ДОКУМЕНТА, КОТОРЫЙ ПОЛУЧИЛ И ОБРАБОТАЛ БАНК».

- Банк предъявляет спорный ЭД.

- Устанавливается факт правомерности использования ЭАСП на момент подписания спорного ЭД, процедура установления факта правомерности использования ЭАСП включает в себя сопоставление:

соответствия сведений об Открытом ключе ЭАСП, отраженных в Акте признания открытого ключа электронного аналога собственноручной подписи Клиента, Открытому ключу ЭАСП сертификата открытого ключа в формате X.509, содержащемуся в файле подписи (файл .sig), ;

даты начала использования Открытого ключа ЭАСП;

даты отправки спорного ЭД.

Факт правомерности использования ЭАСП на момент подписания спорного ЭД считается установленным, если:

- признано соответствие Открытого ключа ЭАСП и дата отправки спорного ЭД больше или равна дате начала использования Открытого ключа ЭЦП.

Если установлен факт правомерности использования ЭАСП, конфликтная ситуация разрешается в пользу Банка.

Если установлен факт неправомерности использования ЭАСП, конфликтная ситуация разрешается в пользу Клиента.

ТИП 4 «ОТРИЦАНИЕ КЛИЕНТОМ ПОДЛИННОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТА, КОТОРЫЙ ПОЛУЧЕН И ОБРАБОТАН БАНКОМ».

1. Банк и Клиент определяют спорный документ на основании выписок по Счету Клиента.

1.1. Из Системы на жесткий диск АРМ Клиента или другой носитель с помощью кнопки «Получить квитанцию банка на документ» выгрузить ЭД в виде двух файлов

- электронный документ (файл с расшифровкой .dat)

- электронная подпись (файл с расшифровкой .sig)

1.2. Просмотреть содержимое файла с расширением .dat средствами операционной системы, установленной на АРМ Клиента. Структура файла .dat приведена в Руководстве по проверке подлинности ЭД, которое находится на дистрибутивном диске АРМ Клиента.

2. Устанавливается факт правомерности использования ЭАСП на момент подписания спорного ЭД, процедура установления факта правомерности использования ЭАСП включает в себя сопоставление:

- соответствия сведений об Открытом ключе ЭАСП, отраженных в Акте признания открытого ключа электронного аналога собственноручной подписи Клиента, сведениям об Открытом ключе ЭАСП, зарегистрированном в базе данных Системы на стороне Банка, отраженных в сертификате Открытого ключа ЭАСП в формате X.509, хранящемся на Сервере Банка;
- даты начала использования Открытого ключа ЭАСП;
- даты отправки спорного ЭД.

Если установлен факт правомерности использования ЭЦП, то Экспертная комиссия переходит к п. 3 настоящего порядка. Если установлен факт неправомерности использования ЭЦП, конфликтная ситуация разрешается в пользу Клиента.

3.Устанавливается подлинность ЭАСП под ЭД.

3.1. Установить СКЗИ из дистрибутива, полученного по доверенному каналу от разработчика СКЗИ.

3.2. Установить Средство проверки ЭАСП из дистрибутива, полученного по доверенному каналу от разработчика Средства проверки ЭАСП.

3.3. Подготовить файл ЭД (файл .dat) и файл подписи (файл .sig);

3.4. Произвести Проверку подлинности ЭД с помощью Средства проверки ЭАСП в соответствии с руководством пользователя Средства проверки ЭАСП и использованием файлов .dat, .sig . Средство проверки ЭАСП выдаст результат проверки.

3.5. С помощью Средства проверки ЭАСП просмотреть сертификат открытого ключа в формате X.509, находящегося в файле подписи, и сравнить ключ открытого ключа в сертификате с ключом в Акте признания открытого ключа ЭАСП.

3.6. Распечатать содержимое ЭД (файла .dat) с помощью стандартного текстового редактора Windows – Блокнот.

3.7. Провести анализ содержимого ЭД, используя сведения о структуре ЭД, содержащиеся в Руководстве по проверке подлинности ЭД и консультации разработчика Системы – ООО «Банк’с софт системс» и установить соответствие текстовых и двоичных данных ЭД (файла .dat) визуальным представлениям ЭД, как электронным в интерфейсе Системы, так и на бумажном носителе.

3.8. По результатам анализа данных ЭД воссоздать документ на бумажном носителе, являющийся аналогом ЭД.

Если Средство проверки ЭАСП с использованием ЭАСП и Открытого ключа ЭАСП, содержащегося в сертификате в формате X.509, находящихся в файле .sig, подтверждает целостность ЭД (файла .dat) и соответствие ЭАСП Открытому ключу ЭАСП, а Открытый ключ ЭАСП в сертификате X.509 совпадает с Открытым ключом ЭАСП в Акте признания открытого ключа ЭАСП, то:

- ЭД признается подлинным;

- временем установки ЭАСП является время, отображаемое Средством проверки ЭАСП в результате проверки;

- воссозданный и заверенный Экспертной комиссией документ на бумажном носителе является равнозначным ЭД и порождает аналогичные ему права и обязанности Сторон при выполнении взаимных обязательств по настоящему Регламенту и договорам, во исполнение которых осуществляется обмен ЭД.