УТВЕРЖДЕНО:

Правлением Банка «Возрождение» (ПАО)
(протокол заседания Правления Банка
«Возрождение» (ПАО) от 20.08.2020 №59-20/П)

Правила
пользования системой электронного взаимодействия
«Защищённая электронная почта
Банка «Возрождение» (ПАО)»
(Версия 3.0)

Москва,

2020

Оглавление

СПИСОК СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
АРМ РКС	Автоматизированное рабочее место разбора конфликтных ситуаций
ЗЭП	Защищённая электронная почта
НКПИ	Носитель ключевой и парольной информации
ПО	Программное обеспечение
Правила	Правила пользования системой электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО)»
СКЗИ	Средство криптографической защиты информации
СКП ЭП	Сертификат ключа проверки электронной подписи
УЦ	Удостоверяющий центр Банк «Возрождение» (ПАО)
ФСБ России	Федеральная служба безопасности Российской Федерации
ЭВ	Электронное взаимодействие
ЭД	Электронный документ
ЭП	Электронная подпись
CRL	Список аннулированных сертификатов

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор безопасности Банка – работник структурного подразделения Банка или Службы информационной безопасности Банка, отвечающий за эксплуатацию СКЗИ и управление ключами ЭП и СКП ЭП. Администратор безопасности Банка отвечает за изготовление ключей ЭП Клиентам, взаимодействие с Клиентами при изготовлении ими своих ключей ЭП и запросов на СКП ЭП, получении СКП ЭП, взаимодействие с Удостоверяющим центром при выпуске и аннулировании СКП ЭП.

Аннулирование сертификата ключа проверки электронной подписи – процедура, выполняемая Удостоверяющим центром Банк «Возрождение» (ПАО) по аннулированию СКП ЭП.

Банк – Банк «Возрождение» (ПАО), организатор Защищённой электронной почты.

Владелец СКП ЭП – лицо, которому в установленном Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи» порядке выдан СКП ЭП.

Внеплановая смена ключей – смена ключей ЭП, вызванная одним из следующих событий: компрометацией ключей ЭП, физической порчей НКПИ; изменением данных, вносимых в СКП ЭП (ФИО владельца сертификата, наименование организации и т.п.).

Доставка электронного документа – физический процесс перемещения ЭД от отправителя к получателю.

Должностные лица Банка, ответственные за работу системы ЗЭП:

Уполномоченный представитель Банка;

Администратор безопасности Банка.

Запрос на СКП ЭП – электронный документ с электронной подписью пользователя УЦ, идентифицирующий обладателя ключа ЭП, включающий ключ проверки ЭП.

Клиент (участник Системы ЗЭП) – юридическое лицо (в том числе кредитная организация), индивидуальный предприниматель, физическое лицо, занимающееся в

установленном законодательством Российской Федерации порядке частной практикой, которое присоединилось к Регламенту и к настоящим Правилам.

Ключ ЭП – уникальная последовательность символов для создания ЭП.

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки подлинности ЭП;

Компрометация ключа ЭП – утрата доверия к тому, что используемые ключи ЭП обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но, не ограничиваясь, следующие:

утрата носителей ключевой информации;

утрата носителей ключевой информации с их последующим обнаружением;

увольнение сотрудников, имевших доступ к ключевой информации;

нарушение правил хранения и уничтожения (после окончания срока действия) ключа электронной подписи;

возникновение подозрений на утечку информации или ее искажение в Системе ЗЭП;

нарушение печати на сейфе с ключевыми носителями;

случаи, когда нельзя достоверно установить, что произошло с носителями ключевой информации (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате чьих-либо несанкционированных действий).

Различают два вида компрометации ключа ЭП: **явную** и **неявную**. Первые четыре события должны трактоваться как явная компрометация ключей. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

КриптоАРМ – программа, предназначенная для шифрования и расшифрования электронных документов, создания и проверки ЭП с использованием ключей ЭП и СКП ЭП.

Плановая смена ключей – смена ключей ЭП с установленной периодичностью, не вызванная компрометацией ключей ЭП.

Прекращение действия сертификата ключа проверки электронной подписи – процедура, выполняемая Банком по прекращению действия СКП ЭП в приложении, использующем СКП ЭП.

Рабочий день – промежуток времени с 09:00 до 18:00 (до 17.00 в предпраздничные дни, 16:45 по пятницам) по московскому времени каждого рабочего дня недели, за исключением выходных и праздничных дней в соответствии с законодательством Российской Федерации.

Регламент Удостоверяющего центра Банк «Возрождение» (ПАО) (далее – Регламент) – утвержденный решением Правления Банка и введенный в действие документ, определяющий условия предоставления и правила пользования услугами УЦ, включая права, обязанности, ответственность УЦ и присоединившихся к Регламенту лиц, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение надлежащего оказания услуг УЦ.

СКП ЭП – ЭД или документ на бумажном носителе, выданные УЦ и подтверждающий принадлежность ключа проверки ЭП владельцу СКП ЭП.

СКП ЭП УЦ – ЭД предназначенный для верификации выпущенных СКП ЭП (цепочки СКП ЭП) пользователей УЦ и верификации выпущенных CRL.

Система электронного взаимодействия Защищённая электронная почта Банка «Возрождение» (ПАО) (Система ЗЭП или Система) – организационно-техническая система, представляющая собой совокупность программно-аппаратного обеспечения Банка и Клиентов, реализующая юридически значимый, защищённый обмен электронными документами между Банком и Клиентами.

Список аннулированных сертификатов – электронный документ с ЭП Удостоверяющего центра, включающий в себя список серийных номеров СКП ЭП, которые на момент времени формирования списка были отозваны или действие которых было приостановлено.

Средства криптографической защиты информации, шифровальные (криптографические) средства – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Структурное подразделение Банка – региональный операционный офис или дополнительный офис Банка.

Тарифы – действующие тарифы Банка, опубликованные на официальном сайте Банка в сети Интернет по адресу: www.vbank.ru.

Удостоверяющий центр – **Банк «Возрождение» (ПАО)**, осуществляющий функции по созданию и выдаче СКП ЭП, а также иные функции, предусмотренные Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Уполномоченный представитель Банка – работник Банка, отвечающий за взаимодействие между Клиентом и Банком в соответствии с настоящими Правилами, а также за оформление документов и документальное сопровождение Системы ЗЭП.

Уполномоченный представитель Клиента – Клиент – индивидуальный предприниматель или физическое лицо, занимающееся в предусмотренном законодательством Российской Федерации порядке частной практикой, а также физическое лицо, представляющее юридическое лицо и наделенное полномочиями выполнять определенные действия от его имени.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к информации в зашифрованном ЭД.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

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

2. ПРЕДМЕТ РЕГУЛИРОВАНИЯ НАСТОЯЩИХ ПРАВИЛ

2.1. Настоящие Правила устанавливают принципы и порядок осуществления электронного взаимодействия между Банком и Клиентом (при совместном

упоминании – Стороны), а также права и обязанности Сторон, в целях обеспечения юридически значимого электронного документооборота с использованием Системы ЭЭП в случаях, предусмотренных договорами Сторон. Требования к содержанию ЭД, порядок их исполнения не являются предметом регулирования настоящих Правил.

2.2. Настоящие Правила являются публичной офертой. Присоединение Клиента к настоящим Правилам осуществляется на основании Заявления о присоединении к Регламенту Удостоверяющего центра и Правилам пользования системой электронного взаимодействия «Защищенная электронная почта Банка «Возрождение» (ПАО)» по форме Приложения 1 к настоящим Правилам. Подписывая указанное Заявление, Клиент в соответствии со ст. 428 ГК РФ полностью и безусловно присоединяется к Регламенту и Правилам и принимает порядок и условия электронного документооборота в рамках Системы ЭЭП. Настоящие Правила и Регламент становятся обязательными для Клиента с момента получения Заявления Банком.

2.3. Настоящие Правила составлены в соответствии с требованиями действующего законодательства РФ в области использования ЭП.

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

3. ЭЛЕКТРОННАЯ ПОДПИСЬ

3.1. Все ЭД, передаваемые в Системе ЭЭП подписываются усиленной неквалифицированной ЭП (далее – усиленная ЭП).

3.2. В случае невозможности использования усиленной ЭП по ГОСТ Р 34.10-2012 в соответствии с п. 3.1, используется усиленная ЭП с использованием алгоритмов sha2RSA. СКП ЭП, применяемые в Системе, заменяются на СКП ЭП соответствующие алгоритмам sha2RSA.

3.3. Стороны признают, что ЭД, подписанные в Системе в соответствии с пунктами 3.1 – 3.2 настоящих Правил, признаются равнозначными совершенным в письменной форме на бумажном носителе, подписанными собственноручной подписью и заверенными печатью (если необходимо). Юридическая значимость указанных документов не может быть оспорена только на том основании, что они совершены в электронном виде.

3.4. Используемые в Системе ЭЭП средства криптографической защиты информации (СКЗИ) имеют подтверждение соответствия требованиям ГОСТ и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1, требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011г. № 796, установленным в соответствии с положениями Федерального закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ, за исключением средств ЭП, применяющих алгоритмы sha2RSA. Их применение в Системе, включая средства ЭП, применяющих алгоритмы sha2RSA, признается Сторонами достаточным для обеспечения конфиденциальности, целостности, авторства и неотказуемости передаваемой между Сторонами информации и невозможности ее фальсификации после момента её подписания.

3.5. Клиент осознает и принимает на себя все риски, связанные с использованием Системы ЭЭП в сети Интернет, которая является незащищенным каналом связи.

4. ПОРЯДОК И УСЛОВИЯ ДОПУСКА КЛИЕНТА К ОСУЩЕСТВЛЕНИЮ ДОКУМЕНТООБОРОТА В СИСТЕМЕ ЭЭП

4.1. Клиент допускается к осуществлению документооборота в Системе ЭЭП после выполнения им и Банком совокупности следующих действий:

предоставления Клиентом и проверки уполномоченным представителем Банка пакета документов, необходимых для формирования ключей ЭП и СКП ЭП уполномоченного представителя Клиента в соответствии с разделом 11.2 настоящих Правил;

выработки администратором безопасности Банка ключей ЭП и СКП ЭП уполномоченного представителя Клиента, подготовки установочного комплекта АРМ Клиента;

установки необходимых аппаратных средств и клиентского программного обеспечения, приведение АРМ Клиента в соответствие требованиям Руководства по обеспечению безопасности использования ЭП и средств ЭП при эксплуатации АРМ Системы ЭЭП (Приложение 8 к настоящим Правилам), оформления двустороннего Акта (Приложение 9 к настоящим Правилам) либо Анкеты (Приложение 10 к настоящим Правилам) о соблюдении Клиентом требований Руководства по обеспечению безопасности использования ЭП и средств ЭП;

получения Клиентом СКП ЭП, подписания Сторонами Акта о передаче и/или оказании услуг по установке и настройке программного обеспечения Системы ЭЭП (Приложение 7 к настоящим Правилам).

4.2. Банк приостанавливает или прекращает использование Клиентом Системы ЭЭП на основании полученного от Клиента уведомления об отказе от использования Системы ЭЭП или по инициативе Банка при нарушении Клиентом порядка использования Системы ЭЭП в соответствии с настоящими Правилами в следующих случаях:

непредставления информации и документов, либо представления ненадлежащим образом оформленных документов согласно требованиям настоящих Правил;

невыполнения Клиентом обязанностей, предусмотренных разделом 10.1 настоящих Правил;

в иных случаях, когда использование Системы ЭЭП может нанести вред Клиенту или Банку.

4.3. Клиент вправе в одностороннем порядке отказаться от использования Системы ЭЭП в любое время.

4.4. Уведомление о приостановлении/прекращении использования Системы ЭЭП, в соответствии с порядком, установленным п.п. 4.2 – 4.3 Правил, направляется одной Стороной другой Стороне на бумажном носителе не менее, чем за пять рабочих дней до даты предполагаемого отказа (приостановления/прекращения) от использования Системы ЭЭП.

5. ПОРЯДОК ВСТУПЛЕНИЯ В СИЛУ НАСТОЯЩИХ ПРАВИЛ, ВНЕСЕНИЯ В НИХ ИЗМЕНЕНИЙ И ПРЕКРАЩЕНИЯ ДЕЙСТВИЙ НАСТОЯЩИХ ПРАВИЛ

5.1. Настоящие Правила, включая все Приложения, утверждаются Правлением Банка и публикуются на сайте Банка – http://www.vbank.ru

5.2. Изменения и дополнения в настоящие Правила вносятся Банком в одностороннем порядке и утверждаются Правлением Банка. Правление Банка вправе

определять сроки и порядок вступления в силу изменений и дополнений в настоящие Правила.

5.3. Настоящие Правила прекращают свое действие на основании решения Правления Банка. Прекращение действия настоящих Правил и приложений к ним не влияет на статус ЭД, которыми Стороны обменивались до прекращения действия настоящих Правил и приложений к ним.

6. ПОРЯДОК УВЕДОМЛЕНИЯ О ВНЕСЕНИИ ИЗМЕНЕНИЙ В НАСТОЯЩИЕ ПРАВИЛА

6.1. Если иное не предусмотрено решением Правления Банка, изменения и дополнения в настоящие Правила и приложения к ним, а также сроки и порядок вступления в силу вносимых в настоящие Правила изменений и дополнений публикуются на сайте Банка «Возрождение» (ПАО) – http://www.vbank.ru и считаются доведенными до сведения Клиентов по истечении пяти рабочих дней с даты размещения такой публикации.

6.2. Клиент имеет право запрашивать копии текстов Правил и Приложений к ним, а также копии изменений и дополнений к Правилам на бумажном носителе. Указанные в настоящем пункте документы представляются Банком Клиенту в течение 15 (пятнадцати) рабочих дней после получения соответствующего запроса.

7. ОБЩИЕ ПОЛОЖЕНИЯ

7.1. Подразделениями и уполномоченными представителями Банка, обеспечивающими управление СКП ЭП в Системе ЭЗП, являются Удостоверяющий центр Банк «Возрождение» (ПАО), отдел криптографической защиты информации Службы информационной безопасности и администраторы безопасности структурных подразделений Банка, ответственные за работу Системы ЭЗП.

7.2. Применяемые в Системе ЭЗП СКЗИ и программные средства работы с ЭП и СКП ЭП в процессе их использования автоматически выполняют контроль срока действия СКП ЭП. Срок действия СКП ЭП определяется действующей редакцией Регламента УЦ.

7.3. Банк обеспечивает эксплуатацию СКЗИ в Системе ЭЗП с обязательным использованием НКПИ, предоставляемых Банком. НКПИ является персональным средством аутентификации и хранения данных. **Запрещается** использовать один и тот же НКПИ для хранения данных разных Уполномоченных представителей Клиента.

7.4. Банк и Клиенты используют в Системе ЭЗП сертифицированные ФСБ России СКЗИ КриптоПро CSP, ПО КриптоАРМ, предоставляемые Банком, за исключением средств ЭП, применяющих алгоритмы sha2RSA. Формируемые Клиентом ключи ЭП имеют признак – «не экспортируемые». Применяемые в Системе ЭЗП СКЗИ и НКПИ обеспечивают невозможность копирования (экспорта) ключа ЭП с носителя – на другой НКПИ. В случае, если в программном обеспечении клиента присутствуют технические ограничения, не позволяющие применять «не экспортируемые» ключи ЭП клиенту вырабатываются ключи ЭП с признаком «экспортируемые». Для получения ключей ЭП с признаком «экспортируемые» уполномоченное лицо клиента должно сообщить об этом факте уполномоченному представителю Банка.

7.5. Плановая смена ключа ЭП и СКП ЭП Уполномоченного представителя Клиента (перегенерация) производится Банком в соответствии с разделом 11.3.

7.6. Участники Системы ЭЗП признают, что используемые в Системе ЭЗП СКЗИ и НКПИ обеспечивают достаточную конфиденциальность электронного взаимодействия

и позволяют идентифицировать владельца ключа ЭП, а также установить отсутствие искажения информации в ЭД.

7.7. Клиент не обязан получать дополнительную лицензию на право эксплуатации используемых в Системе ЭЭП СКЗИ, так как является участником Системы ЭЭП Банка, имеющего необходимую лицензию.

В соответствии с требованиями к лицензиатам, как участник Системы ЭЭП, Клиент обязан:

использовать на АРМ с Системой ЭЭП только лицензионное ПО;

соблюдать требования лицензионного соглашения на СКЗИ;

обеспечить возможность контроля со стороны уполномоченных федеральных органов исполнительной власти соблюдения лицензионных требований осуществления лицензируемой деятельности в отношении шифровальных (криптографических) средств.

7.8. Услуги Банка по изготовлению ключей ЭП, СКП ЭП, предоставлению СКЗИ, НКПИ и иных программно-технических средств в соответствии с Правилами, являются платными. Размер платы за эти услуги утверждается Банком в Тарифах Банка. Порядок оплаты регулируется договорами, предусматривающими осуществление электронного документооборота между Банком и Клиентами.

7.9. Банк оставляет за собой право перехода на другие СКЗИ, НКПИ в связи с изменением технологии работы или другими обстоятельствами.

7.10. В процессе эксплуатации АРМ Системы ЭЭП Клиент обязан выполнять требования Руководства по обеспечению безопасности использования ЭП, средств ЭП и минимизации рисков связанных с использованием ЭП при эксплуатации Клиентом АРМ Системы ЭЭП (Приложение 8 настоящих Правил). Согласие Клиента выполнять требования Руководства по обеспечению информационной безопасности оформляется Актом (Приложение 9 к настоящим Правилам) или Анкетой (Приложение 10 к настоящим Правилам) о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ЭЭП. При невыполнении или неполном выполнении Клиентом обязательных требований по обеспечению информационной безопасности АРМ Системы ЭЭП, Клиент принимает на себя риски возможных потерь (ущерба).

7.11. Владельцами СКП ЭП в Системе ЭЭП являются Клиенты и Банк.

Полномочия Уполномоченных лиц Клиентов-юридических лиц действовать от имени Клиента подтверждаются выданными доверенностями для работы с СКП ЭП, подписанными Клиентом (руководителем организации Клиента) и заверенными печатью (при наличии) Клиента, иными предусмотренными законодательством документами.

Полномочия уполномоченных представителей Банка действовать от имени Банка подтверждаются Приказами о назначении на должность.

7.12. Банк обеспечивает хранение СКП ЭП Клиентов в соответствии с Регламентом УЦ.

8. ЭЛЕКТРОННЫЙ ДОКУМЕНТ

8.1. Требования, предъявляемые к электронному документу

8.1.1. ЭД, передаваемый в Системе ЭЭП в соответствии с настоящими Правилами и Регламентом, имеет юридическую силу и влечет предусмотренные для данного

документа правовые последствия в соответствии с действующим законодательством и договорами, заключенными между Банком и Клиентами. ЭД, передаваемый в Системе ЗЭП, считается надлежащим образом оформленным, при условии его соответствия договору, Регламенту и настоящим Правилам.

8.1.2. ЭД, оформленный с нарушением правил, установленных договором, настоящими Правилами и Регламентом не принимается в обработку и не влечет никаких правовых последствий для Сторон.

8.2. Использование электронной подписи и шифрования в электронном документообороте

8.2.1. ЭД, передаваемые в системе ЗЭП, подписываются усиленной ЭП.

8.2.2. Смена ключей ЭП не влияет на статус ЭД, если он был подписан действующим на момент подписания ключом ЭП в соответствии с Регламентом и настоящими Правилами.

8.2.3. После подписания ЭД шифруется с использованием СКП ЭП получателей и отправляется по электронной почте получателю.

8.2.4. ЭД становится юридически значимым с момента формирования получателем положительного результата проверки ЭП уполномоченного представителя отправителя, подписавшего ЭД.

9. ОРГАНИЗАЦИЯ ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

9.1. Обмен электронными документами

9.1.1. Обмен ЭД включает:

формирование ЭД;

подпись ЭД;

шифрование ЭД;

отправку и доставку ЭД;

расшифрование ЭД;

проверку ЭД;

подтверждение получения ЭД;

отзыв ЭД;

хранение ЭД (ведение архивов ЭД);

создание дополнительных экземпляров ЭД;

создание бумажных копий ЭД.

9.2. Формирование электронного документа

9.2.1. Формирование ЭД осуществляется в следующем порядке:

формирование ЭД;

подписание сформированного ЭД ЭП;

шифрование ЭД.

9.3. Отправка и доставка электронного документа

9.3.1. В отношениях между отправителем и получателем ЭД считается исходящим от отправителя, если ЭД отправлен с помощью электронной почты:

самим отправителем;

представителем, уполномоченным действовать от имени отправителя в отношении данного ЭД.

9.3.2. Документ считается доставленным получателю, если отправитель получил подтверждение о доставке.

9.4. Проверка подлинности доставленного электронного документа

9.4.1. Проверка ЭД включает:

проверку всех ЭП ЭД;

проверку ЭД на соответствие формату, установленному договором между Банком и Клиентом (если применимо).

9.4.2. В случае положительного результата проверки ЭД принимается к исполнению или подлежит дальнейшей обработке. В противном случае данный ЭД считается не полученным, о чем получатель должен послать уведомление отправителю с указанием причины неполучения ЭД.

9.4.3. При получении зашифрованного ЭД, для проведения проверки подлинности ЭД сначала выполняется расшифрование ЭД. В случае невозможности расшифрования ЭД получатель должен послать уведомление отправителю с указанием причины неполучения ЭД.

9.5. Хранение электронных документов

9.5.1. Все ЭД, переданные в Системе ЗЭП Банком и Клиентами, должны храниться в течение сроков, предусмотренных нормативными документами. Срок хранения ЭД не может быть менее трех лет.

9.5.2. ЭД должны храниться либо в электронных архивах, либо в виде копий электронных документов на бумажных носителях, заверенных уполномоченным представителем Стороны.

9.5.3. ЭД должны храниться в незашифрованном виде в том же формате, в котором они были сформированы, отправлены или получены.

9.5.4. Хранение ЭД должно быть организовано с ведением соответствующих электронных или бумажных журналов учета, и хранением СКП ЭП и программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки ЭП хранимых ЭД.

9.5.5. При хранении ЭД должна быть обеспечена привязка (синхронизация) ЭД и соответствующих СКП ЭП для проведения процедуры разбора конфликтных ситуаций.

9.5.6. Для выполнения текущих работ по ведению электронных архивов Клиентам рекомендуется назначить ответственных лиц.

9.5.7. Электронные архивы и архивы бумажных копий ЭД подлежат защите от несанкционированного доступа и непреднамеренного уничтожения и/или искажения.

10. ОРГАНИЗАЦИЯ ОБСЛУЖИВАНИЯ КЛИЕНТОВ ЧЕРЕЗ СИСТЕМУ ЗЭП

10.1. Условия осуществления электронного взаимодействия

10.1.1. С целью обеспечения гарантированного ознакомления Клиента, с действующей редакцией настоящих Правил, Клиент обязан не реже одного раза в пять рабочих дней обращаться на Интернет-сайт Банка по адресу http://www.vbank.ru/ за сведениями об изменениях и дополнениях в Правила и Регламент.

10.1.2. Клиент обязан установить необходимые для обеспечения работы в Системе ЗЭП аппаратные средства, клиентское программное и информационное обеспечение, а также поддерживать их в работоспособном состоянии.

10.1.3. Уполномоченный представитель Клиента обязан выполнить всю совокупность действий, необходимых для получения допуска к осуществлению ЭВ, предусмотренных Регламентом и Правилами, своевременно выполнять плановую смену ключей и своевременно уведомлять Банк о компрометации своих ключей, а также соблюдать требования Руководства по обеспечению безопасности использования ЭП, средств ЭП и минимизации рисков связанных с использованием ЭП при эксплуатации Клиентом АРМ Системы ЗЭП (Приложение 8 к настоящим Правилам), организационно-технические требования по обеспечению безопасности информации, установленные в Регламенте и Правилах.

10.1.4. Клиент обеспечивает использование ключей ЭП в Системе ЗЭП только Уполномоченными лицами Клиента, указанными в соответствующем СКП ЭП. Клиенту запрещается использовать для подписи документов скомпрометированные ключи ЭП. Клиент немедленно извещает Банк о фактах компрометации по телефону и в письменной форме путем направления заявления на аннулирование соответствующих СКП ЭП.

10.1.5. Клиент обязан использовать полученные в Банке программно-технические средства только для целей осуществления ЭВ в рамках Системы ЗЭП и не передавать без письменного согласия Банка данные средства третьим лицам.

10.1.6. Уполномоченный представитель Клиента обязан незамедлительно сообщать уполномоченному представителю Банка о ставших известными попытках третьих лиц совершить действия, способные привести к нарушению целостности Системы ЗЭП.

10.1.7. При возникновении в Системе ЗЭП ситуаций, признаваемых форс-мажорными в соответствии с Регламентом, Клиент признает и исполняет решения, принимаемые Банком в соответствии с Регламентом и Правилами.

10.1.8. Клиент соблюдает порядок урегулирования спорных ситуаций, установленный разделом 13 настоящих Правил.

10.2. Порядок оплаты услуг за подключение к Системе ЗЭП

10.2.1. Клиент оплачивает услуги по подключению к Системе ЗЭП в соответствии с Тарифами Банка.

10.2.2. Оплата комиссий за предоставление комплекта Системы ЗЭП осуществляется не позднее следующего рабочего дня после подписания Акта о передаче и/или оказании услуг по установке и настройке программного обеспечения Системы ЗЭП (Приложение 7). Порядок и сроки оформления Акта установлены Приложением 7 к настоящим Правилам.

10.2.3. Оплата комиссий за смену (перегенерацию) ключа ЭП и получение СКП ЭП осуществляется не позднее следующего рабочего дня после подписания Акта о плановой смене (перегенерации) ключа ЭП и получении СКП ЭП (Приложение 12).

10.2.4. Оплата комиссий осуществляется одним из следующих способов:

списание комиссии производится на основании заранее данного акцепта с банковского счета Клиента в российских рублях в Банке, указанного в Заявлении о присоединении к Регламенту Удостоверяющего центра и Правилам пользования системой электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО) (Приложение 1 к настоящим Правилам);

внесение Клиентом наличных денежных средств в кассу Банка;

перечисление Клиентом денежных средств платежным поручением со счетов, открытых в иной кредитной организации.

10.2.5. Датой принятия оказанных услуг считается дата подписания Акта о передаче и/или оказании услуг по установке и настройке программного обеспечения системы ЗЭП/ Акта о плановой смене (перегенерации) ключа ЭП и получении СКП ЭП.

11. СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

11.1. Средства обеспечения информационной безопасности

11.1.1. Информация, содержащая персональные данные, и конфиденциальная информация, передаваемая с использованием Системы ЗЭП, подлежит защите.

11.1.2. Соблюдение требований информационной безопасности при организации электронного взаимодействия обеспечивает:

конфиденциальность информации (получить доступ к информации могут только уполномоченные представители Сторон);

целостность передаваемой информации (гарантирование, что данные передаются без искажений, и исключается возможность подмены информации);

аутентификацию участников ЭВ (возможность получения передаваемой информации только тем лицом, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).

11.1.3. Соблюдение требований по информационной безопасности при организации электронного взаимодействия реализуются посредством применения программно-технических средств и организационных мер.

11.1.4. К программно-техническим средствам относятся:

программные средства, специально разработанные для осуществления защищённого электронного взаимодействия;

система паролей и идентификаторов для ограничения доступа пользователей к техническим и программным средствам Системы ЗЭП;

средства криптографической защиты информации;

средства ЭП;

программно-аппаратные средства защиты от несанкционированного доступа;

средства защиты от компьютерных вирусов;

средства защиты от атак на вычислительные системы.

11.1.5. К организационным мерам относятся:

размещение технических средств в помещениях с контролируемым доступом;

административные ограничения доступа к этим средствам;

задание режима использования пользователями и операторами паролей и идентификаторов;

допуск к осуществлению ЭВ только уполномоченных на то представителей Сторон;

поддержание программно-технических средств в исправном состоянии;

резервирование программно-технических средств;

обучение технического персонала;

защита технических средств от повреждающих внешних воздействий (пожар, воздействие воды и т.п.).

11.1.6. Порядок использования СКЗИ в Системе ЗЭП, определяется Регламентом и настоящими Правилами.

11.2. Порядок формирования ключей ЭП и СКП ЭП уполномоченного представителя Клиента

11.2.1. Клиент передает в Банк пакет документов, необходимых для формирования ключей ЭП и СКП ЭП.

11.2.2. Пакет документов включает:

а) подписанное Клиентом Заявление о присоединении к Регламенту Удостоверяющего центра и Правилам пользования системой электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО). (Приложение 1 к настоящим Правилам);

б) Заявление на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО), оформленное в соответствии с требованиями Приложения 2 или Приложения 2а к настоящим Правилам) и, подписанное Уполномоченным представителем Клиента, который будет указан в соответствующем СКП ЭП, и, если применимо, руководителем Клиента-юридического лица и заверенное печатью Клиента (при наличии);

в) документы, подтверждающие полномочия Уполномоченного представителя Клиента – юридического лица для работы с СКП ЭП. Если Уполномоченный представитель Клиента – юридического лица действует на основании доверенности, то доверенность должна быть составлена по форме Приложения 3 к настоящим Правилам или содержать аналогичные полномочия. Срок действия доверенностей, определяющих полномочия Уполномоченных представителей Клиента-юридического лица, должен быть больше срока действия СКП ЭП;

г) копии страниц документа, удостоверяющего личность Уполномоченных представителей Клиента, содержащих информацию о фамилии, имени, отчестве, серии и номере документа, дате выдачи, выдавшем органе, дате рождения, дате и адресе последней регистрации;

д) учредительные документы Клиента – юридического лица (нотариально заверенную копию или электронный документ, подписанный квалифицированной электронной подписью налогового органа);

е) доверенность уполномоченному представителю Клиента на получение ключей ЭП, СКП ЭП, документов, программного и информационного

обеспечения для работы с СКП ЭП (Приложение 4 к настоящим Правилам);

ж) Заявление на установку (настройку) АРМ Системы ЗЭП (Приложение 6 к настоящим Правилам);

з) Анкета (Приложение 10 к настоящим Правилам) о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ЗЭП (Приложение 8 к настоящим Правилам) – в случае, если в Заявлении на установку (настройку) АРМ Системы ЗЭП Клиентом указано, что установка системы будет произведена Клиентом самостоятельно.

В случае установки (настройки) АРМ Системы ЗЭП уполномоченным представителем Банка двусторонний Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования ЭП, средств ЭП и минимизации рисков связанных с использованием ЭП при эксплуатации Клиентом АРМ Системы ЗЭП (Приложение 9 к настоящим Правилам) составляется во время установки.

Документы, перечисленные в подпунктах г) – е) настоящего пункта, предоставляются в случае их отсутствия в Банке.

11.2.3. Уполномоченный представитель Банка осуществляет проверку правильности указанных Клиентом данных в переданных документах и, при необходимости, – по требованию Удостоверяющего центра – вправе затребовать иные документы.

11.2.4. При положительном результате проверки в течение пяти рабочих дней, следующих за днем представления пакета документов, Банком формируется установочный комплект АРМ Клиента, который включает в себя:

на каждого Уполномоченного представителя Клиента, имеющего доступ к Системе ЗЭП – конверт, содержащий:

НКПИ содержащий ключ ЭП и СКП ЭП Уполномоченного представителя Клиента;

администраторский и пользовательские пароли (PIN-коды) доступа к НКПИ в пинконвертах;

лицензии на бумажном носителе на право использования КриптоПро CSP и КриптоАРМ (на каждый АРМ Системы ЗЭП);

опись конверта;

диск CD-ROM содержащий:

дистрибутив СКЗИ КриптоПро CSP, КриптоАРМ, программное обеспечение для работы с сертифицированными НКПИ, эксплуатационная документация к СКЗИ;

корневые СКП ЭП Удостоверяющего центра;

руководство пользователя;

руководство администратора.

11.2.5. Установка АРМ Системы ЗЭП у Клиента осуществляется уполномоченными представителями Банка либо Клиентом самостоятельно на персональный компьютер, соответствующий требованиям Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ЗЭП (Приложение 8 к настоящим Правилам).

11.2.6. При невыполнении или неполном выполнении Клиентом обязательных требований по обеспечению информационной безопасности АРМ Системы ЗЭП, Клиент принимает на себя риски возможных потерь (ущерба).

11.2.7. В случае, если Клиент в Заявлении на установку (настройку) АРМ Системы ЗЭП (Приложение 6 к настоящим Правилам) указал, что установка системы будет произведена уполномоченным представителем Банка, уполномоченный представитель Банка в течение пяти рабочих дней производит установку (настройку) Клиенту АРМ Системы ЗЭП, составляет и подписывает с Клиентом двусторонний Акт о соблюдении Клиентом требований Руководства по обеспечению безопасности использования ЭП, средств ЭП и минимизации рисков связанных с использованием ЭП при эксплуатации Клиентом АРМ Системы ЗЭП (Приложение 9 к настоящим Правилам), а также передает Клиенту установочный комплект АРМ Клиента и проводит консультацию Клиента по работе с программным обеспечением.

11.2.8. При самостоятельной установке АРМ Системы ЗЭП уполномоченный представитель Клиента прибывает в Банк для получения установочного комплекта АРМ Клиента.

11.2.9. В случае получения установочного комплекта АРМ Клиента представителем, не указанном в СКП ЭП, Уполномоченный представитель Клиента должен предъявить уполномоченному представителю Банка доверенность на получение ключей ЭП, СКП ЭП, документов, программного и информационного обеспечения для работы с СКП ЭП (Приложение 4 к настоящим Правилам).

11.2.10. Клиент просматривает информацию в СКП ЭП на полученном у уполномоченного лица Банка НКПИ, сравнивает серийный номер в СКП ЭП с номером в Акте (Приложение 7 к настоящим Правилам), самостоятельно распечатывает Акт в 2-х экземплярах, подписывает и передает Акты уполномоченному представителю Банка.

11.2.11. Уполномоченный представитель Банка заполняет реквизиты и поля, подлежащие ручному заполнению, подписывает и утверждает оба экземпляра Акта. Один экземпляр Акта возвращается Клиенту.

11.2.12. Клиент оплачивает услуги Банка в соответствии с Тарифами Банка в порядке, установленном разделом 10.2 настоящих Правил.

11.2.13. Участники Системы ЗЭП признают, что подпись Уполномоченного представителя Клиента в Акте о передаче и или оказании услуг по установке и настройке программного обеспечения Системы ЗЭП (Приложение 7 к настоящим Правилам) означает, что Клиенту СКП ЭП Удостоверяющим центром выдан СКП ЭП, что он ознакомлен с содержанием СКП ЭП и владеет соответствующим ключом ЭП, позволяющим с помощью средства ЭП создавать свою ЭП в ЭД (подписывать ЭД).

11.2.14. Каждому ключу ЭП, записанному в НКПИ, соответствует только один СКП ЭП с указанием одного Уполномоченного представителя Клиента. Сертифицированный ФСБ России программно-аппаратный комплекс УЦ Банка гарантирует уникальность значения ключа проверки ЭП и серийного номера СКП ЭП в каждом выпущенном УЦ СКП ЭП.

11.2.15. Каждому ключу ЭП, выработанному с использованием алгоритмов SHA2RSA, записанному в НКПИ, соответствует только один СКП ЭП с указанием одного Уполномоченного представителя Клиента.

11.2.16. Клиент для каждого Уполномоченного представителя Клиента в Системе ЗЭП имеет только один действующий ключ ЭП, записанный в НКПИ, и только один соответствующий ему действующий СКП ЭП.

11.2.17. При невозможности самостоятельного восстановления Клиентом программного обеспечения, испорченного по его вине (вирусы, техническая неисправность компьютера и др.), оно восстанавливается уполномоченными представителями Банка. Восстановление АРМ Системы ЗЭП уполномоченными представителями Банка оплачивается Клиентом в соответствии с действующими Тарифами Банка.

11.2.18. СКП ЭП Клиента и Банка в форме документов на бумажном носителе предоставляются Клиентам по их запросу, оформленному в электронном виде или на бумажном носителе и переданному уполномоченному представителю Банка (Приложение 11 к настоящим Правилам).

11.3. Проведение плановой (внеплановой) смены ключей ЭП и СКП ЭП

11.3.1. Плановая смена ключей ЭП и СКП ЭП должна быть выполнена не позднее, чем за две недели до завершения срока действия СКП ЭП. Внеплановая смена ключей ЭП и СКП ЭП выполняется вне установленной периодичности. Клиент должен предоставить в Банк:

а) НКПИ содержащий ключ ЭП и СКП ЭП. По согласованию с уполномоченным представителем Банка, новый ключ ЭП и СКП ЭП Клиента может быть сгенерирован на новый НКПИ, а НКПИ с истекающим ключом ЭП и СКП ЭП будет возвращен Клиентом в Банк после выдачи нового НКПИ Клиенту;

б) Заявление на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО) (Приложение 2 или Приложение 2а к настоящим Правилам), оформленное в соответствии с требованиями Приложения 2б к настоящим Правилам и подписанное Уполномоченным представителем Клиента, который будет указан в соответствующем СКП ЭП, и, если применимо, руководителем Клиента-юридического лица и заверенное печатью Клиента (при наличии);

в) документы, подтверждающие полномочия Уполномоченного представителя Клиента – юридического лица для работы с СКП ЭП. Если Уполномоченный представитель Клиента – юридического лица действует на основании доверенности, то доверенность должна быть составлена по форме Приложения 3 к настоящим Правилам или содержать аналогичные полномочия. Срок действия доверенностей, определяющих полномочия Уполномоченных представителей Клиента-юридического лица, должен быть больше срока действия СКП ЭП;

г) устав/изменения в устав (иной уставной документ) Клиента – юридического лица (нотариально заверенную копию или электронный документ, подписанный квалифицированной электронной подписью налогового органа), если в ранее предоставленный имеющийся в Банке устав (иной уставной документ) были внесены изменения;

д) доверенность уполномоченному представителю Клиента на получение ключей ЭП, СКП ЭП, документов, программного и информационного обеспечения для работы с СКП ЭП (Приложение 4 к настоящим Правилам);

е) Анкету (Приложение 10 к настоящим Правилам) о соблюдении Клиентом требований Руководства по обеспечению безопасности использования

электронной подписи и средств электронной подписи при эксплуатации АРМ Системы ЭЭП (Приложение 8 к настоящим Правилам).

Документы, перечисленные в подпунктах в) и г) настоящего пункта, предоставляются в случае их отсутствия в Банке.

11.3.2. Уполномоченный представитель Банка осуществляет проверку правильности указанных Клиентом данных в переданных документах.

11.3.3. При положительном результате проверки в течение пяти рабочих дней, следующих за днем представления пакета документов, Банком проводятся мероприятия по формированию и записи нового ключа ЭП и СКП ЭП на НКПИ.

11.3.4. Уполномоченный представитель Банка заполняет реквизиты и поля, подлежащие ручному заполнению, подписывает оба экземпляра Акта (Приложение 7 к настоящим Правилам).

11.3.5. Клиент просматривает информацию в СКП ЭП на НКПИ, сравнивает серийный номер в СКП ЭП с номером в Акте (Приложение 7 к настоящим Правилам) и подписывает Акт. Один экземпляр Акта возвращается Клиенту. После подписания Сторонами Акта о плановой смене (перегенерации) ключа ЭП и получении СКП ЭП для использования в Системе ЭЭП (Приложение 12 к настоящим Правилам) процесс перегенерации ключей ЭП считается завершённым. Клиент переходит на работу с использованием нового ключа ЭП.

11.4. Порядок действий при компрометации ключей ЭП или физической порче носителя ключевой информации

11.4.1. В случае компрометации ключа ЭП или физической поломке НКПИ владелец скомпрометированного ключа ЭП или сломанного НКПИ обязан действовать в соответствии с порядком, установленном настоящими Правилами.

11.4.2. При получении ЭД, подписанного скомпрометированным ключом ЭП (реквизиты СКП ЭП находятся в CRL), данный ЭД считается неполученным, о чем получатель обязан отправить уведомление отправителю с указанием причины неполучения ЭД.

11.4.3. В случае принятия решения Клиентом о компрометации своих ключей ЭП Уполномоченный представитель Клиента обязан по телефону сообщить уполномоченному представителю Банка о факте компрометации используемых ключей ЭП и прекратить использование скомпрометированных ключей ЭП.

11.4.4. С целью проверки информации о компрометации ключей ЭП Клиента уполномоченный представитель Банка выполняет ответный звонок Уполномоченному представителю Клиента. В случае положительной проверки уполномоченный представитель Банка дает указание Администратору безопасности о прекращении действия СКП ЭП, то есть об удалении соответствующих СКП ЭП из настроек КриптоАРМ на АРМ Системы ЭЭП.

11.4.5. В течение того же рабочего дня, когда Клиент уведомил уполномоченного представителя Банка по телефону о компрометации ключей, Клиент обязан направить на имя управляющего структурным подразделением Банка или на имя Председателя Правления Банка Заявление на аннулирование сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра Банка (далее – Заявление), подписанное Клиентом и заверенное печатью (при наличии) Клиента (Приложение 5 к настоящим Правилам). После получения Заявления уполномоченным представителем Банка Заявление регистрируется в Банке в установленном порядке и помещается в юридическое дело Клиента.

11.4.6. Уполномоченный представитель Банка в день регистрации Заявления дает указание Администратору безопасности осуществить аннулирование СКП ЭП. Администратор безопасности аннулирует СКП ЭП.

11.4.7. В соответствии с Регламентом Банк осуществляет аннулирование СКП ЭП не позднее рабочего дня, следующего за днем, в течение которого Заявление было зарегистрировано Банком (Приложение 5 к настоящим Правилам) путем издания Списка аннулированных сертификатов (CRL), содержащего серийный номер аннулированного СКП ЭП.

11.4.8. Официальным уведомлением о факте аннулирования СКП ЭП является опубликование CRL, содержащего сведения об аннулированном сертификате. Временем аннулирования СКП ЭП признается время издания CRL, изданного ранее всех последующих CRL и содержащего сведения об аннулированном сертификате, указанное в поле «thisUpdate» (действителен с) CRL.

11.4.9. Информация о размещении CRL заносится в изданные Удостоверяющим центром СКП ЭП в поле CRLDistributionPoint.

11.4.10. СКП ЭП, соответствующий скомпрометированным ключам ЭП, из ключевой базы Организатора Системы ЗЭП не удаляется и хранится постоянно после аннулирования СКП ЭП для проведения (в случае необходимости) разбора конфликтных ситуаций, связанных с применением ЭП.

11.4.11. Для возобновления ЭВ с Банком после аннулирования СКП ЭП Клиент должен представить в Банк новое Заявление на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО), оформленное в соответствии с требованиями Приложения 2 или Приложения 2а к настоящим Правилам, получить НКПИ с новыми ключами ЭП и новыми СКП ЭП и выполнить действия, предусмотренные пунктом 11.3.5 настоящих Правил.

12. ОТВЕТСТВЕННОСТЬ СТОРОН. ОБСТОЯТЕЛЬСТВА, ИСКЛЮЧАЮЩИЕ ОТВЕТСТВЕННОСТЬ СТОРОН (ФОРС-МАЖОР)

12.1. Стороны несут ответственность за действия своих уполномоченных представителей, а также иных лиц, получивших или имеющих доступ к используемым ими аппаратным средствам, программному, информационному обеспечению, криптографическим ключам ЭП и иным средствам, обеспечивающим ЭВ в соответствии с действующим законодательством Российской Федерации.

12.2. Стороны освобождаются от ответственности за частичное или полное неисполнение своих обязательств в соответствии с Регламентом и настоящими Правилами, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникших после присоединения к Регламенту и настоящим Правилам, или в результате событий чрезвычайного характера, а также сбоев, неисправностей и отказов оборудования; сбоев и ошибок программного обеспечения; сбоев, неисправностей и отказов систем связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения, не позволяющих осуществлять эксплуатацию необходимого для выполнения электронного взаимодействия оборудования, которые Стороны не могли предвидеть или предотвратить.

12.3. В случае возникновения обстоятельств непреодолимой силы срок выполнения Сторонами своих обязательств в соответствии с настоящими Правилами отодвигается соразмерно времени, в течение которого действуют такие обстоятельства и их последствия.

12.4. Сторона, для которой стало невозможным выполнение своих обязательств в виду действия обстоятельств непреодолимой силы, обязана в течение трех календарных дней сообщить другой Стороне о начале и прекращении действия обстоятельств, воспрепятствовавших выполнению договорных обязательств.

12.5. Обязанность доказывать существование обстоятельств непреодолимой силы лежит на Стороне, которая ссылается на их действие.

12.6. По прошествии обстоятельств непреодолимой силы Стороны обязуются принять все меры для ликвидации последствий и уменьшения причиненного реального ущерба.

13. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ

13.1. В случае возникновения между Сторонами спорных ситуаций при использовании Системы ЗЭП, Стороны обязаны предпринять все меры для их разрешения путем переговоров.

13.2. При возникновении спорной ситуации Клиент направляет в Банк соответствующее заявление. В срок не более тридцати дней со дня получения такого заявления, уполномоченный представитель Банка предоставляет Клиенту информацию о результатах рассмотрения заявления, в том числе в письменной форме.

13.3. До создания технической комиссии Стороны самостоятельно проводят проверку спорного ЭД на АРМ Системы ЗЭП с использованием программного обеспечения КриптоАРМ. По результатам проверки Стороны проводят переговоры.

13.4. Если Сторонам не удастся разрешить спорные ситуации путем переговоров, совместным решением обеих Сторон для проведения **технической экспертизы** создается техническая комиссия из уполномоченных представителей Сторон с равным количеством членов комиссии с каждой Стороны. Указанное решение принимается Сторонами в течение трех рабочих дней с момента обращения одной Стороны к другой. В случае уклонения одной из Сторон от принятия данного решения другая Сторона вправе самостоятельно привлечь экспертов для разрешения конфликтной ситуации.

13.5. По согласованию Сторон к участию в работе технической комиссии могут привлекаться эксперты в области защиты информации. Стороны согласны с тем, что в качестве экспертов должны привлекаться сотрудники организаций:

разработчика средства криптографической защиты информации;

разработчика программного обеспечения КриптоАРМ;

ФСБ России.

13.6. Стороны согласны с тем, что оплачивать услуги привлеченных экспертов в области защиты информации должна Сторона, предъявившая претензию.

13.7. Техническая комиссия осуществляет свою работу на территории Банка.

13.8. Техническая комиссия приступает к работе в течение трех рабочих дней со дня поступления письменного заявления к одной из Сторон. Бремя доказательства лежит на Стороне, заявившей о нарушении ее прав и законных интересов.

13.9. Для разбора спорной ситуации техническая комиссия использует программный комплекс разбора конфликтных ситуаций КриптоПро УЦ. Разбор конфликтной ситуации проводится на АРМ разбора конфликтных ситуаций запуском соответствующей программы для электронного документа, авторство или содержание которого оспаривается. Протокол проверки ЭП, формируемый указанной программой,

является основным документом работы комиссии и должен быть подписан всеми членами комиссии.

Проверка подписанного электронного документа включает в себя выполнение следующих действий:

определение СКП ЭП или нескольких СКП ЭП, необходимых для проверки ЭП;

проверка ЭП электронного документа с использованием каждого СКП ЭП;

определение даты формирования каждой ЭП в электронном документе;

проверка ЭП каждого СКП ЭП, путем построения цепочки СКП ЭП до СКП ЭП Главного УЦ;

проверка действительности СКП ЭП на текущий момент времени;

проверка отсутствия СКП ЭП в CRL.

Если СКП ЭП, необходимый для проверки ЭП документа, отозван УЦ, комиссия принимает решение о действительности ЭП документа, используя дату создания документа и дату аннулирования СКП ЭП в CRL.

13.10. Все действия, предпринимаемые комиссией для выяснения фактических обстоятельств, а также выводы, сделанные комиссией, заносятся в Протокол работы технической комиссии. Протокол работы технической комиссии должен содержать следующие данные:

состав комиссии с указанием сведений о квалификации каждого из членов комиссии;

краткое изложение обстоятельств возникшей конфликтной ситуации;

мероприятия, проводимые комиссией для установления причин и последствий возникшей конфликтной ситуации, с указанием даты времени и места их проведения;

выводы, к которым пришла комиссия в результате проведенных мероприятий;

подписи всех членов комиссии.

13.11. При проведении технической экспертизы соответствие АРМ Системы ЭЗП Клиента требованиям Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи (Приложение 8 к настоящим Правилам) должно быть подтверждено Актом о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи (Приложение 9 к настоящим Правилам). Акт подписывается членами комиссии.

13.12. В случае если мнение члена (или членов) комиссии относительно порядка, методики, целей проводимых мероприятий не совпадает с мнением большинства членов комиссии, об этом в Протоколе составляется соответствующая запись, которая подписывается членом (или членами комиссии), чье особое мнение отражает соответствующая запись.

13.13. Протокол составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу. Экземпляры Протокола хранятся у Банка и Клиента.

13.14. По итогам работы технической комиссии составляется акт, в котором содержится краткое изложение выводов технической комиссии. Помимо изложения выводов о работе технической комиссии, акт должен также содержать следующие данные:

состав комиссии;

дату и место составления Акта;

даты и время начала и окончания работы комиссии;

краткий перечень мероприятий, проведенных комиссией;

подписи членов комиссии;

указание на особое мнение члена (или членов комиссии), в случае наличия такового.

Акт составляется на бумажном носителе в двух экземплярах, имеющих одинаковую силу. Экземпляры акта хранятся у Банка и Клиента.

К акту может прилагаться особое мнение члена (или членов комиссии), не согласных с выводами технической комиссии, указанными в акте. Особое мнение составляется в произвольной форме и составляет приложение к акту.

13.15. В случае не достижения Сторонами согласия, а также в случае отказа одной из Сторон от участия в создании, работе или исполнения решения технической комиссии, спор подлежит разрешению в Арбитражном суде г. Москвы.

14. ПОРЯДОК ДЕЙСТВИЙ КЛИЕНТА ПРИ ВЫЯВЛЕНИИ ПОДОЗРЕНИЙ НА МОШЕННИЧЕСКИЕ ДЕЙСТВИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ЗЭП

Клиент обязуется:

14.1. Сообщить уполномоченному представителю Банка о ставших известными ему попытках третьих лиц совершить действия, способные привести к нарушению целостности Системы ЗЭП, – незамедлительно, но не позднее рабочего дня, следующего за днем выявления факта;

14.2. Установить факт наличия/отсутствия отправленных ЭД в период неработоспособности ПК с установленной Системой ЗЭП.

14.3. Прекратить работу на персональном компьютере (далее – ПК), с использованием которого, по мнению Клиента, совершены мошеннические действия, в том числе не допустить проверку ПК антивирусными средствами, либо другие действия, которые способны внести изменения в информацию, содержащуюся на жестком диске, до снятия его образа, так как это уничтожит временные атрибуты файлов и, возможно, тела вредоносного программного обеспечения, что сделает невозможным проведение полноценного исследования.

14.4. Завершить работу ПК путем отключения его электропитания, обеспечить невозможность включения ПК и его физическую недоступность до прибытия сотрудников правоохранительных органов или специалистов из организаций, специализирующихся в расследовании компьютерных преступлений.

14.5. Собрать и представить в Банк дополнительную информацию по инциденту при наличии журналов сетевого доступа, а также возможно других журналов из информационной структуры Клиента.

Председатель Правления
Банка Возрождение «(ПАО) Г.В. Солдатенков

Приложение 1. Заявление о присоединении к Регламенту Удостоверяющего центра и Правилам пользования системой электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО)

В Удостоверяющий центр Банк «Возрождение» (ПАО)

Заявление о присоединении

_____

(наименование юридического лица, включая организационно-правовую форму, ИНН, ОГРН)

в лице _____

(должность, фамилия, имя, отчество)

действующее на основании _____

в соответствии со ст. 428 ГК РФ полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра - Банк «Возрождение» (ПАО) и Правилам пользования системой электронного взаимодействия - «Защищённая электронная почта Банка «Возрождение» (ПАО)», условия которых определены Банком «Возрождение» (ПАО) и опубликованы на сайте Банка «Возрождение» (ПАО) и принимаю порядок и условия электронного документооборота. Об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки проинформирован(а).

Оплата комиссии за предоставление/установку комплекта системы ЭП, оплата комиссии за смену (перегенерацию) ключа ЭП и получение СКП ЭП осуществляется путем:

☐ списания Банком комиссии с банковского счета Клиента №_____.

Клиент дает свое согласие (заранее данный акцепт) на списание Банком указанной комиссии в соответствии с Тарифами, действующими на момент списания.

☐ внесения наличных денежных средств в кассу Банка

☐ безналичной оплаты платежным поручением Клиента

_____

(Должность и Ф.И.О. руководителя организации)

_____

(Подпись руководителя организации)

«____» _____20__г.

(дата подписания заявления)

(М.П.)

Приложение 2. Форма заявления на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия

В Удостоверяющий центр Банка «Возрождение» (ПАО)

Заявление

на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия
Защищенная электронная почта

Прошу

1. Зарегистрировать меня в качестве пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовить ключ электронной подписи (ЭП), сертификат ключа проверки электронной подписи (СКП ЭП), в том числе на бумажном носителе❑*, в соответствии с указанными идентификационными данными:

E-mail	Электронная почта
Title (T)	Должность
Common name (CN)/FQDN	Фамилия, имя, отчество /Имя сервера или TLS-клиента
Organization (O)	Сокращённое наименование организации
Country (C)	RU
State (S)	Регион
Locality (L)	Населённый пункт
INN	ИНН
Alt name 1	Альтернативное имя узла 1
Alt name 2	Альтернативное имя узла 2
Alt name 3	Альтернативное имя узла 3

2. Настоящим Я, _____(фамилия, имя, отчество)____ предоставляю Банку «Возрождение» (ПАО) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» свое: согласие на обработку моих персональных данных для целей заключения и исполнения договоров, в том числе на осуществление банковских операций и предоставление всех видов банковских услуг, иных договоров с Банком.

Обработка может осуществляться с использованием и\или без использования средств автоматизации и включает в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Согласие дано на срок 5 лет, и считается продлённым на тот же срок, если не отозвано путём предоставления в УЦ заявления в простой письменной форме.

Уполномоченный представитель

Клиента (владелец СКП ЭП) _____
(подпись) (фамилия, имя, отчество)

Руководитель организации _____
(подпись) (фамилия, имя, отчество)

«____»_____20__г.
(МП) (дата подписания заявления)

* – отметка проставляется для Клиентов, желающих получить так же бумажную копию СКП ЭП

Приложение 2а. Форма заявления на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия на алгоритмах sha2RSA

В Удостоверяющий центр Банка «Возрождение» (ПАО)

Заявление

на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия
Защищенная электронная почта

Прошу

1. Зарегистрировать меня в качестве пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовить ключ электронной подписи (ЭП), сертификат ключа проверки электронной подписи (СКП ЭП), в том числе на бумажном носителе❑*, в соответствии с указанными идентификационными данными:

Common name(CN)/ FQDN	ФИО/Имя сервера или TLS-клиента
Country (C)	RU
State (S)	Регион
Locality (L)	Населённый пункт
Organization (O)	Сокращённое наименование организации
INN	ИНН
Alt name 1	Альтернативное имя узла 1
Alt name 2	Альтернативное имя узла 2
Alt name 3	Альтернативное имя узла 3

2. Настоящим Я, _____(фамилия, имя, отчество)____ предоставляю Банку «Возрождение» (ПАО) в соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных» свое: согласие на обработку моих персональных данных для целей заключения и исполнения договоров, в том числе на осуществление банковских операций и предоставление всех видов банковских услуг, иных договоров с Банком.

Обработка может осуществляться с использованием и\или без использования средств автоматизации и включает в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Согласие дано на срок 5 лет, и считается продлённым на тот же срок, если не отозвано путём предоставления в УЦ заявления в простой письменной форме.

Уполномоченный представитель
Клиента (владелец СКП ЭП)_____
(подпись) (фамилия, имя, отчество)

Руководитель организации _____
(подпись) (фамилия, имя, отчество)

«____»_____20__г.
(МП) (дата подписания заявления)

* – отметка проставляется для Клиентов, желающих получить так же бумажную копию СКП ЭП

Приложение 2б. Требования по заполнению полей заявления на регистрацию пользователя Удостоверяющего центра Банк «Возрождение» (ПАО) и изготовление ключа ЭП и СКП ЭП для использования в системе электронного взаимодействия

E-mail	Адрес электронной почты – указывается адрес электронной почты владельца СКП ЭП или организации – Пользователя УЦ, например: **zep@vbank.ru**. Для СКП ЭП сервера или TLS-клиента поле не заполняется.
Title (T)	Должность – (только для юридических лиц) в случае выпуска СКП ЭП на должностное лицо – его должность, например: **Главный бухгалтер**. Для СКП ЭП сервера или TLS-клиента поле не заполняется.
Common name (CN)/FQDN	Фамилия, Имя, Отчество – должны быть указаны, полностью так, как записаны в документе, удостоверяющем личность, например: **Иванов Иван Иванович /** имя сервера или TLS-клиента, например: **vbank.ru**
Alt name 1/2/3…	Альтернативные имена узла, допускается указать IP адрес – указываются альтернативные доменные имена сервера или его дополнительные IP, например: **vbank2.ru** или **192.168.1.2**. Поле заполняется только для СКП ЭП сервера.
Organization (O)	Сокращенное наименование организации – (только для юридических лиц) указывается сокращенное наименование организации Пользователя УЦ, включая организационно-правовую форму в соответствии с уставными и регистрационными документами, например: **ООО «СК Буревестник»**
Country (C)	Всегда должен быть записан двухсимвольный код Российской Федерации – две прописные латинские буквы **«RU»**
State (S)	Регион – указывается номер региона (см. Справочник кодов регионов пункт 12.5 Регламента) 2 цифры (лидирующий ноль указывать обязательно) и через 1 пробел - название региона с заглавной буквы по адресу местонахождения юридического лица/по адресу регистрации физического лица, например: **77 г. Москва** или **50 Московская область**
Locality (L)	Город – указывается с заглавной буквы наименование населенного пункта, по адресу местонахождения юридического лица/по адресу регистрации физического лица – владельца СКП ЭП, например: **Москва** или **Нижний Новгород**
INN	ИНН организации или индивидуального предпринимателя – 12 цифр. Для организации должен содержать два лидирующих нуля. Пример: **00**1234567890. Для СКП ЭП сервера или TLS-клиента поле не заполняется.

Все поля заявления за исключением номера и даты составления заявления, номера и подписей должны быть заполнены машинописным способом. Структура заявления не должна быть нарушена. Поля заполняются строчными буквами, за исключением – первое слово в строке и имена собственные пишутся с заглавной буквы, каждое слово должно быть отделено одним пробелом, шрифт Arial, начертание: обычный, размер: 10pt. Не разрешается использовать пробел в начале и в конце текста.

Если в фамилии, имени или отчестве в написании присутствует «дефис», то в заявлении слово указывается с дефисом без пробелов (например, **Салтыков-Щедрин**).

Если организация не имеет печати, в заявлении указывается - б/п.

Заявления на изготовление СКП ЭП, оформленные с нарушением данных требований, УЦ к обработке не принимаются.

Приложение 3. Форма доверенности на уполномоченного представителя Клиента для работы с СКП ЭП

Доверенность № _____

г. _____ «____» _____ 20__г.

(наименование юридического лица, включая организационно-правовую форму, ИНН, ОГРН)

в лице _____

(должность)

_____

(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта, кем и когда выдан)

выступать в роли **Пользователя Удостоверяющего центра** Банк «Возрождение» (ПАО) и совершать действия в рамках Регламента Удостоверяющего центра Банк «Возрождение» (ПАО), установленные для Пользователя УЦ Банк «Возрождение» (ПАО), от имени и в интересах организации использовать ключ ЭП и соответствующий ему СКП ЭП, владельцем которого является указанное доверенное лицо, в соответствии со сведениями указанными в СКП ЭП в системе электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО).

Уполномоченный представитель клиента наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Доверенность действительна по «____» _____ 20__ г.

Образец подписи уполномоченного
представителя клиента _____

(фамилия, имя, отчество)

_____

(должность и ФИО руководителя организации)

(подпись руководителя организации)

(печать организации)

Приложение 4. Форма доверенности уполномоченному представителю Клиента на получение ключей ЭП, СКП ЭП, документов, программного и информационного обеспечения для работы с СКП ЭП

Доверенность № _____

г. _____ «____» _____20___г.

(наименование юридического лица, включая организационно-правовую форму, ИНН, ОГРН)

в лице (должность)

(фамилия, имя, отчество)

действующего на основании

уполномочивает (фамилия, имя, отчество)

(серия и номер паспорта, кем и когда выдан)

1.Предоставить в Удостоверяющий центр Банк «Возрождение» (ПАО) необходимые документы, определенные Регламентом Удостоверяющего центра Банк «Возрождение» (ПАО) для изготовления ключа электронной подписи и соответствующего ему сертификата ключа проверки электронной подписи Пользователя УЦ_____

(фамилия, имя, отчество)

2.Получить, изготовленные для данного Пользователя УЦ, носитель ключевой информации с ключом ЭП, PIN-код доступа к носителю ключевой информации, СКП ЭП Пользователя УЦ, СКП ЭП УЦ Банк «Возрождение» (ПАО), при необходимости - СКП ЭП Пользователя УЦ на бумажном носителе.

3._____ наделяется

(фамилия, имя, отчество)

правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Доверенность действительна по «____» _____ 20__ г.

Образец подписи уполномоченного
представителя организации

(фамилия, имя, отчество)

(должность, подпись и ФИО руководителя организации)

(печать организации)

Приложение 5. Форма заявления на аннулирование сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра Банк «Возрождение» (ПАО)

В Банк «Возрождение» (ПАО)

Заявление

на аннулирование сертификата ключа проверки электронной подписи Пользователя Удостоверяющего центра

Банк «Возрождение» (ПАО)

В связи с _____прошу аннулировать сертификат ключа проверки электронной подписи Пользователя УЦ с указанными идентификационными данными:

Serial number (SN)	Серийный номер СКП ЭП
Common name (CN)	Фамилия, Имя, Отчество
Organization (O)	Организация

_____

(должность и ФИО руководителя организации)

_____

(подпись руководителя организации)

«____» _____20__г.

(дата подписания заявления)

(печать организации)

Приложение 6. Форма заявления на установку (настройку) АРМ системы ЗЭП

В Банк «Возрождение» (ПАО)
_____ _._.

ЗАЯВЛЕНИЕ
на установку (настройку) АРМ системы ЗЭП

_____
(наименование юридического лица, включая организационно-правовую форму, ИНН, ОГРН)

На основании Заявления о присоединении к Правилам пользования системой электронного взаимодействия «Защищённая электронная почта Банка «Возрождение» (ПАО)» от ___._____.20__г. для обслуживания по системе ЗЭП просим

установить (модернизировать) систему в следующей конфигурации *(необходимое отметить)*:

☐ **установка комплекта АРМ системы ЗЭП**

☐ **Восстановление работоспособности АРМ системы ЗЭП**

Установленная на АРМ операционная система (Windows 7, Windows 10 и др.):
_____

Установленный на АРМ почтовый клиент:_____

Установлено ли на АРМ СКЗИ «КриптоПро» (если да, указать версию) _____

Установка системы будет произведена *(необходимое отметить)*:

❒ Участником самостоятельно

❒ с выездом уполномоченного представителя Банка к Участнику по указанному ниже адресу установки

Контактное лицо (Ф.И.О.): _____

Телефон (ы):_____E-mail:_____

Время работы: _____ перерыв _____

Адрес места установки АРМ системы ЗЭП:
_____

Дополнительные сведения: _____

Руководитель: ***Заявление принял (а):***

__ _____ _____ _____

/подпись/ /Ф.И.О./ /подпись/ /Ф.И.О./

Дата заполнения: « _ » _____ 20__ год

Приложение 7. Форма Акта о передаче и/или оказании услуг по установке и настройке программного обеспечения системы ЗЭП

«Утверждаю» от Клиента	«Утверждаю» от Банка
_____ (должность Руководителя организации Клиента) _____ (подпись, фамилия, инициалы Руководителя организации Клиента) М.П.	_____ (должность уполномоченного представителя Банка) _____ (подпись, фамилия, инициалы уполномоченного представителя Банка) М.П.

Акт № -

о передаче и/или оказании услуг по установке и настройке программного обеспечения системы ЗЭП

г. _____ Дата «_____» «_____» 20__ г.

Мы, нижеподписавшиеся, уполномоченный представитель Банка «Возрождение» (ПАО) в лице _____ с одной стороны и уполномоченный представитель: _____
в лице _____,
действующий (ей) на основании _____, с другой стороны, составили
настоящий акт о том, что уполномоченный представитель Банка передал и/или оказал услуги, а уполномоченный представитель Клиента получил и/или принял услуги:

№ п/п	Переданные средства (оказанные услуги)	Отметка о передаче и/или оказании услуги
1	Сменный МНИ (диск CD-ROM) № ___ с дистрибутивом СКЗИ, ПО КриптоАРМ, эксплуатационной и технической документацией, ПО для работы с сертифицированными НКПИ, СКП ЭП УЦ, СКП ЭП уполномоченных представителей Банка, СКП ЭП уполномоченных представителей Клиента.	☐
2	Лицензия на использование СКЗИ КриптоПро CSP версии _._ серийный номер – _____.	☐
3	Лицензия на использование КриптоАРМ серийный номер – _____.	☐
4	USB-ключ НКПИ в комплекте, ID _____ с ключом ЭП и конверт(ы) с PIN кодом(ами) доступа пользователя (администратора).	☐
5	Уполномоченным представителем Клиента получен ключ ЭП и СКП ЭП серийный № _____. С информацией, содержащейся в СКП ЭП, ознакомлен.	☐
6	Программное обеспечение системы ЗЭП установлено/восстановлено (нужное подчеркнуть) на компьютер(ы) Клиента, находящийся по адресу: _____ уполномоченным представителем Банка с выездом к Клиенту/самостоятельно Клиентом (нужное подчеркнуть) в следующей комплектации (нужное подчеркнуть). Трудозатраты сотрудника Банка составили __ часов.	☐
7	Руководство по обеспечению безопасности использования ЭП, и средств ЭП и минимизации рисков, связанных с использованием ЭП при эксплуатации Клиентом АРМ системы ЗЭП.	☐

Уполномоченный представитель Клиента	Уполномоченный представитель Банка
_____ (должность Уполномоченного представителя Клиента) _____ (подпись, фамилия, инициалы Уполномоченного представителя Клиента)	_____ (должность уполномоченного представителя Банка) _____ (подпись, фамилия, инициалы уполномоченного представителя Банка)

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу – по одному экземпляру для каждой стороны

Инструкция по оформлению Акта об оказании услуг о передаче и/или установке и настройке программного обеспечения системы ЗЭП

1. Акт об оказании услуг оформляется во всех случаях передачи и/или оказании услуг по установке и настройке программного обеспечения, указанных в таблице, и оформляется на каждого представителя Клиента – владельца СКП ЭП и на каждый его новый рабочий СКП ЭП.
2. В графе «Уполномоченный представитель Клиента» в нижней левой части Акта должен расписаться уполномоченный представитель Клиента получивший ключ ЭП и соответствующий СКП ЭП и ознакомившийся с его содержанием.
3. Оформленный Акт об оказании услуг дает право уполномоченному представителю Клиента осуществлять действия в системе ЗЭП Банка с использованием своего ключа ЭП.
4. Акт об оказании услуг формируется уполномоченным представителем Банка и направляется уполномоченному представителю Клиента во вложении по электронной почте. Никакой уполномоченный представитель Клиента не должен получать доступ к системе ЗЭП до предъявления уполномоченному представителю Банка оформленного Акта об оказании услуг.
5. Уполномоченный представитель Клиента просматривает информацию в СКП ЭП, сравнивает сведения о субъекте и серийный номер в СКП ЭП со сведениями о субъекте и серийным номером в Акте, распечатывает Акт об оказании услуг в 2-х экземплярах, подписывает их, утверждает у Руководителя организации, скрепляет печатью организации и передает Акты уполномоченному представителю Банка.
6. Уполномоченный представитель Банка заполняет в обоих экземплярах Акта реквизиты, подлежащие ручному заполнению, в обоих экземплярах Акта об оказании услуг:
   а) В колонке «Отметка о передаче и/или оказании услуги» проставляются отметка «+» или «V» только напротив реально оказанных услуг;
   б) В строке 4 указывается адрес места нахождения АРМ системы ЗЭП Клиента, а так же указываются трудозатраты уполномоченного представителя Банка в часах. Неполный час работы засчитывается за полный;
   в) Подписывает Акт за уполномоченного представителя Банка.
7. Оба экземпляра Акта утверждаются уполномоченным представителем Банка и скрепляются печатью Банка.
8. Один экземпляр Акта возвращается Клиенту.

Приложение 8. Руководство по обеспечению безопасности использования ЭП, средств ЭП и минимизации рисков, связанных с использованием ЭП при эксплуатации Клиентом АРМ системы ЭЭП

Для обеспечения безопасности использования электронной подписи и средств электронной подписи Клиенту необходимо обеспечить соблюдение следующих требований по обеспечению информационной безопасности при эксплуатации Клиентом АРМ системы ЭЭП

№ п/п	Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ системы ЭЭП	Признак обязательности
1	а. АРМ системы ЭЭП обслуживается уполномоченными представителями Клиента.	++
	б. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ системы ЭЭП.	++
	в. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с настоящим Руководством.	++
2	а. Установка, настройка и восстановление системы ЭЭП у Клиента осуществляется уполномоченными представителями обслуживающего его структурного подразделения Банка.	*
	б. На АРМ системы ЭЭП отсутствуют программы удаленного администрирования (например, RAdmin или TeamViewer).	++
	в. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ системы ЭЭП.	++
3	Электронные ключи НКПИ и PIN-коды доступа к ним постоянно находятся исключительно у уполномоченных представителей клиента, не оставляются ими без присмотра и подключаются к USB-порту АРМ только на время сеанса работы с Банком.	++
4	Режим «Включить кэширование» в настройках средства криптографической защиты информации (СКЗИ) КриптоПро CSP не включен.	++
5	При использовании настройки СКЗИ КриптоПро CSP «Запомнить пароль» сразу после завершения сеанса работы с Банком запомненные пароли обязательно удаляются.	++
6	Клиентом предприняты меры, исключающие возможную блокировку администраторских PIN-кодов доступа к электронным ключам НКПИ.	+
7	Дистрибутив СКЗИ КриптоПро CSP и КриптоАРМ получен на учтенном носителе информации по акту приема-передачи, подписанным уполномоченным представителем Банка и уполномоченным представителем Клиента и хранится как эталонная копия. Установка СКЗИ КриптоПро CSP проведена с полученного дистрибутива.	++
8	На АРМ системы ЭЭП установлены все рекомендованные производителем обновления безопасности операционной системы.	++
9	а. Работа на АРМ системы ЭЭП производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КриптоПро и КриптоАРМ.	++
	б. Стандартная учетная запись «Гость» отключена.	++
	в. Выполнены требования по парольной защите, предусмотренные Руководством пользователя по установке и настройке клиентского АРМ: пароль состоит из прописных и строчных латинских букв и цифр, длина пароля – не менее 8 символов, пароль сменен после первого входа, далее пароль меняется каждые 6 месяцев.	++
10	а. На АРМ системы ЭЭП установлено антивирусное ПО в соответствии с требованиями, указанными в формуляре на применяемое СКЗИ. Например, п. 4 раздел 2 Формуляра КриптоПро CSP ЖТЯИ.00050-02 30 01: «СКЗИ ЖТЯИ. 00050-02 должно использоваться со средствами	++

	антивирусной защиты, сертифицированными ФСБ России». Перечень средств защиты информации, сертифицированных ФСБ России: http://clsz.fsb.ru/certification.htm, http://clsz.fsb.ru/files/download/sved_po_sertif.pdf.	
	б. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем.	++
	в. На АРМ системы ЭЭП дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия.	*
	г. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления.	++
	д. Полная проверка АРМ системы ЭЭП на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки.	++
11	На АРМ системы ЭЭП в операционной системе включен режим отображения расширений файлов для анализа файлов-вложений.	+
12	На АРМ системы ЭЭП установлен и настроен персональный межсетевой экран, с помощью которого разрешен доступ только к доверенным ресурсам информационно-телекоммуникационной сети Интернет, необходимым для работы с Банком и для обновления лицензионного ПО и антивирусных баз.	*
13	При уходе пользователя АРМ системы ЭЭП с рабочего места в течение рабочего дня АРМ блокируется пользователем, после завершения рабочего дня – выключается.	*
14	В случае установки на ноутбук ПО АРМ системы ЭЭП, Клиентом обеспечивается раздельное хранение трех компонент: – ноутбука; – НКПИ; – PIN-кодов к НКПИ, логинов и паролей.	++
15	Клиенту известен порядок обращения по вопросам работы системы ЭЭП в рабочее время по телефонам обслуживающего структурного подразделения Банка, круглосуточно – по телефону технической поддержки системы ЭЭП 8-800-777-0-888.	+

Примечания:

- пункты Руководства, отмеченные знаком «++», обязательны и должны быть выполнены Клиентом на момент составления Акта/Анкеты;
- пункты Руководства, отмеченные знаком «+», обязательны и должны быть выполнены Клиентом в течение 2-х недель после составления Акта/Анкеты;
- пункты Руководства, отмеченные знаком «*», имеют рекомендательный характер.

Приложение 9. Форма Акта о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ЗЭП

«Утверждаю» от Клиента	«Утверждаю» от Банка
_____ (должность Руководителя организации Клиента) _____ (подпись, фамилия, инициалы Руководителя организации Клиента) М.П.	_____ (должность уполномоченного представителя Банка) _____ (подпись, фамилия, инициалы уполномоченного представителя Банка) М.П.

Акт № -

о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ЗЭП

г. _____ Дата «_____» «_____» 20__ г.

Мы, нижеподписавшиеся, уполномоченный представитель Банка «Возрождение» (ПАО) в лице _____ с одной стороны и уполномоченный представитель: _____, действующий (ей) на основании _____, с другой стороны, составили настоящий Акт о соответствии АРМ Клиента Требованиям по обеспечению информационной безопасности при эксплуатации Клиентом АРМ системы ЗЭП:

№ п/п	Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ системы ЗЭП	Признак обязательности	Оценка соответствия Требованиям (Да/Нет)
1	а. АРМ системы ЗЭП обслуживается уполномоченными представителями Клиента.	++	
	б. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ системы ЗЭП.	++	
	в. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ системы ЗЭП.	++	
2	а. Установка, настройка и восстановление системы ЗЭП у Клиента осуществляется уполномоченными представителями обслуживающего его структурного подразделения Банка.	*	
	б. На АРМ системы ЗЭП отсутствуют программы удаленного администрирования (например, RAdmin или TeamViewer).	++	
	в. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ системы ЗЭП.	++	
3	а. Электронные ключи НКПИ и PIN-коды доступа к ним постоянно находятся исключительно у их владельцев, не оставляются ими без присмотра и подключаются к USB-порту АРМ только на время сеанса работы с Банком.	++	
4	Режим «Включить кэширование» в настройках средства криптографической защиты информации (СКЗИ) КриптоПро CSP не включен.	++	
5	При использовании настройки СКЗИ КриптоПро CSP «Запомнить пароль» сразу после завершения сеанса работы с Банком запомненные пароли обязательно удаляются.	++	

6	Клиентом предприняты меры, исключающие возможную блокировку администраторских PIN-кодов доступа к НКПИ.	+	
7	Дистрибутив СКЗИ КриптоПро CSP получен на учтенном носителе информации по акту приема-передачи, подписанным уполномоченным представителем Банка и уполномоченным представителем Клиента и хранится как эталонная копия. Установка СКЗИ КриптоПро CSP проведена с полученного дистрибутива.	++	
8	На АРМ системы ЗЭП установлены все рекомендованные производителем обновления безопасности операционной системы.	++	
9	а. Работа на АРМ системы ЗЭП производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КриптоПро и КриптоАРМ.	++	
	б. Стандартная учетная запись «Гость» отключена.	++	
	в. Выполнены требования по парольной защите, предусмотренные Руководством пользователя по установке и настройке клиентского АРМ: пароль состоит из прописных и строчных латинских букв и цифр, длина пароля – не менее 8 символов, пароль сменен после первого входа, далее пароль меняется каждые 6 месяцев.	++	
10	а. На АРМ системы ЗЭП установлено антивирусное ПО в соответствии с требованиями, указанными в формуляре на применяемое СКЗИ. Например, п. 4 раздел 2 Формуляра КриптоПро CSP ЖТЯИ.00050-02 30 01: «СКЗИ ЖТЯИ. 00050-02 должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России». Перечень средств защиты информации, сертифицированных ФСБ России: http://clsz.fsb.ru/certification.htm, http://clsz.fsb.ru/files/download/sved_po_sertif.pdf.	++	
	б. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем.	++	
	в. На АРМ системы ЗЭП дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия.	*	
	г. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления.	++	
	д. Полная проверка АРМ системы ЗЭП на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки.	++	
11	На АРМ системы ЗЭП в операционной системе включен режим отображения расширений файлов для анализа файлов-вложений.	+	
12	На АРМ системы ЗЭП установлен и настроен персональный межсетевой экран, с помощью которого разрешен доступ только к доверенным ресурсам информационно-телекоммуникационной сети Интернет, необходимым для работы с Банком и для обновления лицензионного ПО и антивирусных баз.	*	
13	При уходе уполномоченного представителя с рабочего места	*	

	в течение рабочего дня АРМ системы ЭЭП блокируется, после завершения рабочего дня – выключается.		
14	В случае установки на ноутбук ПО АРМ системы ЭЭП, Клиентом обеспечивается раздельное хранение трех компонент: – ноутбука; – НКПИ; – PIN-кодов к НКПИ, логинов и паролей.	++	
15	Клиенту известен порядок обращения по вопросам работы системы ЭЭП в рабочее время по телефонам обслуживающего структурного подразделения Банка, круглосуточно – по телефону технической поддержки системы ЭЭП 8-800-777-0-888.	+	

Примечания:

- пункты Требований, отмеченные знаком «++», обязательны и должны быть выполнены Клиентом на момент составления Акта;
- пункты Требований, отмеченные знаком «+», обязательны и должны быть выполнены Клиентом в течение 2-х недель после составления Акта;
- пункты Требований, отмеченные знаком «*», имеют рекомендательный характер.

Уполномоченный представитель Клиента	Уполномоченный представитель Банка
_____ (должность уполномоченного представителя Клиента) _____ (подпись, фамилия, инициалы уполномоченного представителя Клиента)	_____ (должность уполномоченного представителя Банка) _____ (подпись, фамилия, инициалы уполномоченного представителя Банка)

Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу – по одному экземпляру для каждой стороны

Приложение 10. Форма Анкеты о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ЗЭП

Анкета № -

о соблюдении Клиентом требований Руководства по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации АРМ системы ЗЭП

г. _____ Дата «_____» «_____» 20__ г.

_____

(полное наименование организации Клиента, включая организационно-правовую форму)

№ п/п	Требования по обеспечению информационной безопасности при эксплуатации Клиентом АРМ системы ЗЭП	Признак обязательности	Оценка соответствия Требованиям (Да/Нет)
1	а. АРМ системы ЗЭП обслуживается уполномоченными представителями Клиента.	++	
	б. Клиентом обеспечивается контроль доступа в помещение, в котором размещен АРМ системы ЗЭП.	++	
	в. Администратор локальной вычислительной сети (ЛВС) и администратор безопасности (при их наличии) ознакомлены с Руководством по обеспечению безопасности использования электронной подписи и средств электронной подписи при эксплуатации Клиентом АРМ системы ЗЭП.	++	
2	а. Установка, настройка и восстановление системы ЗЭП у Клиента осуществляется уполномоченными представителями обслуживающего его структурного подразделения Банка.	*	
	б. На АРМ системы ЗЭП отсутствуют программы удаленного администрирования (например, RAdmin или TeamViewer).	++	
	в. Осуществляется периодический контроль активного программного обеспечения (ПО), установленного на АРМ системы ЗЭП.	++	
3	НКПИ и PIN-коды доступа к ним постоянно находятся исключительно у их владельцев, не оставляются ими без присмотра и подключаются к USB-порту АРМ только на время сеанса работы с Банком.	++	
4	Режим «Включить кэширование» в настройках средства криптографической защиты информации (СКЗИ) КриптоПро CSP не включен.	++	
5	При использовании настройки СКЗИ КриптоПро CSP «Запомнить пароль» сразу после завершения сеанса работы с Банком запомненные пароли обязательно удаляются.	++	
6	Клиентом предприняты меры, исключающие возможную блокировку администраторских PIN-кодов доступа к НКПИ.	+	
7	Дистрибутив СКЗИ КриптоПро CSP получен на учтенном носителе информации по акту приема-передачи, подписанным представителем Банка и уполномоченным представителем Клиента и хранится как эталонная копия. Установка СКЗИ КриптоПро CSP проведена с полученного дистрибутива.	++	

8	На АРМ системы ЭЭП установлены все рекомендованные производителем обновления безопасности операционной системы.	++	
9	а. Работа на АРМ системы ЭЭП производится под учетной записью обычного пользователя. Администраторские права используются только для установки СКЗИ КриптоПро и КриптоАРМ.	++	
	б. Стандартная учетная запись «Гость» отключена.	++	
	в. Выполнены требования по парольной защите: пароль состоит из прописных и строчных латинских букв и цифр, длина пароля – не менее 8 символов, пароль меняется каждые 6 месяцев.	++	
10	а. На АРМ системы ЭЭП установлено антивирусное ПО в соответствии с требованиями, указанными в формуляре на применяемое СКЗИ. Например, п. 4 раздел 2 Формуляра КриптоПро CSP ЖТЯИ.00050-02 30 01: «СКЗИ ЖТЯИ. 00050-02 должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России». Перечень средств защиты информации, сертифицированных ФСБ России: http://clsz.fsb.ru/certification.htm, http://clsz.fsb.ru/files/download/sved_po_sertif.pdf.	++	
	б. Включены настройки антивирусного ПО, установленные разработчиком по умолчанию. Включена защита настроек паролем.	++	
	в. На АРМ системы ЭЭП дополнительно установлены средства защиты от спама, вредоносного ПО и злоумышленного воздействия.	*	
	г. Антивирусные базы обновляются в автоматическом режиме с рекомендуемым разработчиком периодом обновления.	++	
	д. Полная проверка АРМ системы ЭЭП на наличие вирусов и вредоносного ПО производится в автоматическом режиме с рекомендуемым разработчиком периодом проверки.	++	
11	На АРМ системы ЭЭП в операционной системе включен режим отображения расширений файлов для анализа файлов-вложений.	+	
12	На АРМ системы ЭЭП установлен и настроен персональный межсетевой экран, с помощью которого разрешен доступ только к доверенным ресурсам информационно-телекоммуникационной сети Интернет, необходимым для работы с Банком и для обновления лицензионного ПО и антивирусных баз.	*	
13	При уходе уполномоченного представителя Клиента с рабочего места в течение рабочего дня АРМ системы ЭЭП блокируется, а после завершения рабочего дня – выключается.	*	
14	В случае установки на ноутбук ПО АРМ системы ЭЭП, Клиентом обеспечивается раздельное хранение трех компонент: – ноутбука; – НКПИ; – PIN-кодов к НКПИ, логинов и паролей.	++	

15	Клиенту известен порядок обращения по вопросам работы системы ЭЭП в рабочее время по телефонам обслуживающего структурного подразделения Банка, круглосуточно – по телефону технической поддержки системы ЭЭП 8-800-777-0-888.	+	

Примечания:

- пункты Требований, отмеченные знаком «++», обязательны и должны быть выполнены Клиентом на момент составления Анкеты;
- пункты Требований, отмеченные знаком «+», обязательны и должны быть выполнены Клиентом в течение 2-х недель после составления Анкеты;
- пункты Требований, отмеченные знаком «*», имеют рекомендательный характер.

_____ _____ / Фамилия, инициалы/

Должность уполномоченного представителя Клиента (подпись)

М.П.

Приложение 11. Форма Акта о плановой смене (перегенерации) ключа ЭП и получении СКП ЭП

«Утверждаю» от Клиента	«Утверждаю» от Банка
_____ (должность Руководителя организации Клиента) _____ (подпись, фамилия, инициалы Руководителя организации Клиента) М.П.	_____ (должность уполномоченного представителя Банка) _____ (подпись, фамилия, инициалы уполномоченного представителя Банка) М.П.

Акт № -
о плановой смене (перегенерации) ключа ЭП и получении СКП ЭП для использования в системе ЗЭП

г. _____ Дата «_____» «_____» 20__ г.

Мы, нижеподписавшиеся, уполномоченный представитель Банка «Возрождение» (ПАО) в лице _____ с одной стороны и уполномоченный представитель : _____
в лице _____,
действующий (ей) на основании _____, с другой стороны, составили
настоящий акт о том, что уполномоченный представитель Клиента получил и/или принял услуги:

№ п/п	Переданные средства (оказанные услуги)	Отметка о передаче и/или оказании услуги
1	Уполномоченным представителем Клиента выработан ключ ЭП и получен СКП ЭП серийный № _____. С информацией, содержащейся в СКП ЭП, ознакомлен.	☐
2	USB-ключ НКПИ в комплекте, ID _____ с ключом ЭП и конверт(ы) с PIN кодом(ами) доступа пользователя (администратора).	☐

Уполномоченный представитель Клиента	Уполномоченный представитель Банка
_____ (должность уполномоченного представителя Клиента) _____ (подпись, фамилия, инициалы уполномоченного представителя Клиента)	_____ (должность уполномоченного представителя Банка) _____ (подпись, фамилия, инициалы уполномоченного представителя Банка)