Утверждены
Председателем Правления
ЗАО «Райффайзенбанк»
Мониным С.А.
21.06.2013
Вступают в силу
01.07.2013

ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА СПЕЦИАЛИЗИРОВАННОГО ДЕПОЗИТАРИЯ ЗАО «РАЙФФАЙЗЕНБАНК»

ВЕРСИЯ 4.0.

Содержание

1. Общие положения

1.1. Настоящие Правила электронного документооборота ЗАО «Райффайзенбанк» *(*далее именуемые Правила*)*, а также приложения к ним определяют общий порядок и принципы осуществления электронного документооборота между ЗАО «Райффайзенбанк» *(*далее именуется Организатор СЭД *или* Банк*)* и лицами, присоединившимися к системе электронного документооборота ЗАО «Райффайзенбанк» *(*далее именуемые Участники ЭДО или Участник ЭДО*)*.

1.2. Настоящие Правила разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи», , Постановление Правительства РФ от 16 апреля 2012 года №313 «Об утверждении положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя».

1.3. Настоящие Правила становятся обязательными для Участника ЭДО с момента заключения между Участником ЭДО и Организатором СЭД Договора о присоединении к Правилам ЭДО ЗАО «Райффайзенбанк» (по форме, указанной в Приложении №1 к Правилам) *(*далее именуется Договор*)*.

Документы в электронно-цифровой форме, обмен которыми осуществляется в системе электронного документооборота ЗАО «Райффайзенбанк» (далее именуется СЭД), могут быть подготовлены в соответствии с форматами электронных документов, принятыми и утвержденными Организатором СЭД (в соответствии с перечнем, приведенным в Приложении №2 к Правилам) или сформированы в форматах «.doc», «.xls», «.csv», «.txt», «.bcw» (далее именуются Формализованные документы) либо подготовлены путем сканирования документов в бумажном виде.

1.4. Для обеспечения авторства, целостности и конфиденциальности электронных документов Организатор СЭД и Участники ЭДО используют программное обеспечение, средства криптографической защиты информации (далее именуются СКЗИ), ключи и сертификаты ключей, ключевые носители, предоставляемые Организатором СЭД в порядке, установленном настоящими Правилами.

1.5. СЭД обеспечивает обмен электронными документами между Организатором СЭД и Участником ЭДО.

1.6. Настоящие Правила, включая все Приложения, утверждаются Организатором СЭД. Изменения и дополнения в настоящие Правила и Приложения к ним вносятся в одностороннем порядке по решению Организатора СЭД. Организатор СЭД вправе определять и изменять сроки и порядок вступления в силу изменений и дополнений в настоящие Правила и Приложения к ним.

1.7. Настоящие Правила, включая все приложения к ним, Изменения и дополнения к ним, подлежат обязательному опубликованию в сети Интернет на официальной странице Банка - www.raiffeisen.ru.

1.8. Изменения и дополнения в настоящие Правила и приложения к ним, а также решения о сроках и порядке вступления их в силу, доводятся Организатором СЭД до сведения

Участников ЭДО путем направления электронного сообщения с уведомлением о данном факте не позднее, чем за 5 (Пять) рабочих дней до вступления в силу изменений в Правила и приложения к ним, а также путем опубликования этой информации в сети Интернет на официальной странице Банка - www.raiffeisen.ru. Отправка такого электронного сообщения осуществляется по электронному адресу, указанному Участником ЭДО в Анкете Участника ЭДО (по форме, указанной в Приложении №4 к настоящим Правилам).

2. Список терминов, определений, сокращений

Термин/ Сокращение	Определение
Авторство электронного документа	Принадлежность электронного документа конкретному Участнику ЭДО. Авторство электронного документа определяется принадлежностью электронной подписи конкретному Участнику ЭДО
Агент	Агент по выдаче, погашению и обмену инвестиционных паев
Владелец сертификата ключа проверки электронной подписи (Владелец сертификата ключа подписи)	Лицо, на имя которого удостоверяющим центром выдан сертификат ключа проверки электронной подписи и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы)
Дисциплинарный комитет ПАРТАД	Орган ПАРТАД, созданный и осуществляющий деятельность на основании и в соответствии с положением о нем и настоящим Кодексом
Доставка электронного документа (Доставка)	Процесс перемещения Электронного документа от Отправителя к Получателю, в том числе его получение Получателем
Ключ электронной подписи	Уникальная последовательность символов, предназначенная для создания электронной подписи
Ключ проверки электронной подписи	Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи
Ключевой носитель	Любой носитель информации, содержащий Криптографические ключи
Компрометация криптографического ключа (Компрометация ключа)	Констатация лицом, владеющим Ключом электронной подписи, обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами
Конфиденциальная информация	Документированная и электронная информация, имеющая действительную или потенциальную коммерческую ценность в

	силу неизвестности ее третьим лицам, при отсутствии к ней свободного доступа на законном основании и если обладатель информации принимает меры к ее охране
Криптографический ключ (Ключи)	Общее название ключа электронной подписи и ключа проверки электронной подписи
Оператор Удостоверяющего центра (Оператор УЦ) –	Уполномоченный сотрудник Организатора СЭД, осуществляющий взаимодействие с Участником ЭДО в процессе Управления ключами и сертификатами ключей.
Организатор системы электронного документооборота (Организатор СЭД)	Закрытое акционерное общество «Райффайзенбанк» (ЗАО «Райффайзенбанк»), осуществляющее эксплуатацию СЭД и имеющее лицензии ФСБ России от 28.02.2012, действительные до 28.02.2017: № 11869 Х на осуществление технического обслуживания шифровальных (криптографических) средств, №11870 Р на осуществление распространения шифровальных (криптографических) средств, № 11871 на осуществление предоставления услуг в области шифрования информации и осуществляющее эксплуатацию СЭД
Отправитель электронного документа (Отправитель)	Лицо, которое, или от имени которого, направляется электронный документ
ПАРТАД	Саморегулируемая организация «Профессиональная ассоциация регистраторов, трансфер-агентов и депозитариев»
Плановая смена ключей	Смена Ключей с установленной в СЭД периодичностью, не вызванная Компрометацией ключей
Подтверждение подлинности электронной подписи в электронном документе	Положительный результат проверки принадлежности электронной подписи в электронном документе Владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе. Подтверждение подлинности электронной подписи должно осуществляться соответствующим средством электронной подписи с использованием сертификата ключа проверки электронной подписи
Получатель электронного документа (Получатель)	Лицо, которому предназначен электронный документ, отправленный Отправителем
Сертификат ключа проверки электронной подписи (Сертификат ключа	Электронный документ или документ на бумажном носителе с собственноручной подписью Уполномоченного лица УЦ, выданные Участнику ЭДО удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи Владельцу

проверки ЭП)	сертификата ключа проверки электронной подписи
Система электронного документооборота Специализированного депозитария ЗАО «Райффайзенбанк» (СЭД)	Совокупность правил и программно-технических средств, реализованная в рамках взаимодействия Организатора СЭД с Участниками ЭДО в целях осуществления электронного документооборота и являющаяся корпоративной информационной системой
Средства криптографической защиты информации (СКЗИ)	Совокупность программно-технических средств, обеспечивающих применение электронной подписи и шифрования/расшифрования при организации электронного документооборота. СКЗИ могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение
Удостоверяющий центр (УЦ)	Юридическое лицо, осуществляющее функции по созданию и выдаче сертификатов ключей проверки ЭП, а также иные функции, предусмотренные Федеральным законом №63-ФЗ «Об электронной подписи». В рамках настоящих Правил функции УЦ выполняет Банк
Уполномоченный представитель Участника ЭДО (Уполномоченное лицо Участника ЭДО)	Должностное лицо Участника ЭДО, который в соответствии с учредительными документами вправе действовать от имени Участника ЭДО без доверенности либо лицо, которому предоставлены соответствующие полномочия на основании доверенности
Уполномоченное лицо Удостоверяющего центра (Уполномоченное лицо УЦ)	Уполномоченное лицо Удостоверяющего центра (Уполномоченное лицо УЦ)- должностное лицо Банка наделенное полномочиями по заверению Сертификатов ключей подписей и списков отозванных сертификатов
Управление ключами и сертификатами ключей	Создание (генерация) Ключей и Сертификатов ключей подписи, их хранение, распространение, удаление (уничтожение), учет (ведение реестра), а также действия, необходимые для выполнения функций удостоверяющего центра в соответствии со статьей 13 Федерального закона от 6 апреля 2011 года №63-ФЗ «Об электронной подписи»
Участник электронного взаимодействия (Участник ЭДО)	Лицо, осуществляющие обмен информацией в электронной форме в качестве отправителя и/или получателя электронных документов и заключившее договор о присоединении к Правилам электронного документооборота ЗАО «Райффайзенбанк»
Форматы электронных	Утвержденные Банком форматы электронных документов, используемые в СЭД

документов	
Шифрование	Криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного электронного документа
Электронное сообщение (Сообщение)	Совокупность данных, закодированная способом, позволяющим обеспечить ее обработку программными и/или аппаратными средствами, передачу по каналам связи и хранение на цифровых носителях информации
Электронная подпись (ЭП)	Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Вид электронной подписи, используемой в соответствии с настоящими Правилами, - неквалифицированная электронная подпись как она определена действующим законодательством Российской Федерации.
Электронный документ (Документ)	Документ, отвечающий в совокупности следующим требованиям: - - информация в документе представлена в электронной форме; документ подготовлен в соответствии с указанными в настоящих Правилах требованиями к Формализованным документам либо путем сканирования документов в бумажном виде; документ подписан электронной подписью.
Электронный документооборот (ЭДО)	Обмен Электронными документами, зашифрованными и подписанными ЭП, в соответствии с настоящими Правилами и приложениями к нему, посредством электронной почты или с помощью иных способов передачи документов в электронной форме в процессе осуществления Банком своей деятельности

3. Порядок допуска Участника ЭДО к осуществлению документооборота в СЭД

3.1. Участник ЭДО и Организатор СЭД должны выполнить поэтапно следующие действия, необходимые для получения допуска к осуществлению ЭДО в СЭД:

- заключение договора с Организатором СЭД о присоединении к настоящим
Правилам;
- установка Участником ЭДО выданного Организатором СЭД СКЗИ на свои программно-технические средства. Инсталляция производится сотрудником Участника ЭДО, который удовлетворяет требованиям п. 7.4 настоящих Правил;
- выполнение Оператором УЦ процедуры генерации криптографических ключей Участника ЭДО;
- изготовление Уполномоченным лицом УЦ сертификата ключа проверки ЭП для уполномоченного лица Участника ЭДО. Сертификат ключа проверки ЭП выдается в форме электронного документа и в форме документа на бумажном носителе. Сертификат ключа проверки ЭП в форме

документа на бумажном носителе формируется в 2 (двух) экземплярах, которые заверяются собственноручными подписями уполномоченного лица Участника ЭДО и Уполномоченного лица УЦ, а также печатьюУЦ.

3.2. После выполнения действий, указанных в п. 3.1 настоящих Правил, производится тестовая эксплуатация СЭД. Срок тестовой эксплуатации - не более 30 (тридцати) рабочих дней с момента начала эксплуатации. По окончании тестовой эксплуатации Организатор СЭД и Участник ЭДО подписывают Акт о начале электронного документооборота (по форме, указанной в Приложении №3 к настоящим Правилам) в двух экземплярах по одному для каждой из сторон.

3.3. Перед началом обмена Электронными документами в СЭД Участник ЭДО и Организатор СЭД обмениваются Анкетами (по форме, указанной в Приложении № 4 и № 5 к настоящим Правилам). В дальнейшем в случае каких-либо изменений данных Анкеты одна сторона предоставляет другой стороне новую Анкету. При этом предыдущая Анкета утрачивает силу.

3.4. Участник ЭДО из числа своих сотрудников назначает ответственных лиц, имеющих право работать со СКЗИ с указанием их полномочий и срока действия этих полномочий.

4. Особенности Электронного документа

4.2. Требования к Электронному документу и порядок использования Электронного документа.

4.1.1. Электронный документ, сформированный в рамках СЭД, имеет юридическую силу и влечет предусмотренные для данного документа правовые последствия в случае его надлежащего оформления в соответствии с настоящими Правилами.

4.1.2. Электронное сообщение приобретает статус Электронного документа при его соответствии настоящим Правилам.

4.1.3. Электронный документ должен быть подготовлен в соответствии с указанными в настоящих Правилах требованиями к Формализованным документам либо путем сканирования документов в бумажном виде.

4.1.4. Все действия с Электронными документами, оформленными, переданными и/или полученными в соответствии с настоящими Правилами признаются Участниками ЭДО совершенными в письменной форме и не могут быть оспорены только на том основании, что они совершены в электронном виде.

4.1.5. Документы, передаваемые в рамках СЭД, должны содержать сведения, в точности соответствующие сведениям, содержащимся в документах, оформленных в бумажном виде.

4.1.6. Управляющая компания и/или Агент, передавая Электронные документы для формирования и ведения реестра владельцев инвестиционных паев, в том числе анкеты, заявления, учредительные документы, заявки на выдачу/погашение/обмен инвестиционных паев, платежные документы, подтверждает, что:

1. Управляющей компанией и/или ее Агентами были приняты соответствующие документы в бумажном виде;
2. Управляющая компания и/или ее Агенты осуществили все необходимые проверки (достоверность принимаемых ею первичных документов, правильность оформления данных документов, наличие образца подписи пайщика на анкете и наличие подписи

(пайщика или его представителя) в других документах, и т.д.);

3. на всех документах, принятых от заявителя имеются необходимые отметки, заверенные печатью и подписью уполномоченного представителя Управляющей компании;
4. сведения в передаваемых специализированному депозитарию документах, подписанных электронной подписью, полностью соответствуют сведениям, содержащимся в документах, оформленных в бумажном виде.

4.1.7. В случае передачи Электронного документа исключительно в соответствии с Форматами электронных документов, Управляющая компания и/или Агент гарантирует корректность оформления соответствующего документа на бумажном носителе, в том числе заполнение всех обязательных полей в документе, наличие подписи и образца подписи (в случае передачи Анкеты зарегистрированного физического лица).

4.1.8. В случае если в исходном бумажном документе отсутствуют необходимые образцы подписей либо нарушены обязательные требования к оформлению документа, в том числе не заполнены обязательные для заполнения поля, передаче подлежит Электронный документ, подготовленный путем сканирования документа в бумажном виде.

4.3. Порядок использования электронной подписи и шифрования.

4.2.1. Электронный документ должен быть подписан ключом ЭП, который соответствует ключу проверки ЭП, указанному в действующем Сертификате ключа проверки подписи, содержащем область использования, применение которой допускается в СЭД.

4.2.2. Действительность ключей ЭП на момент проверки не влияет на юридическую силу Электронного документа, если он был подписан действующим на момент подписания ключом ЭП в соответствии с настоящими Правилами. Моментом подписания Электронного документа считается время и дата, включаемые Отправителем в подписываемый электронный документ. Все передаваемые Электронные документы должны содержать время и дату подписания документа. Достоверность времени и даты подписания Электронного документа контролируется на стороне Получателя.

4.2.3. Для подписания исходящих от него Электронных документов Уполномоченное лицо Участника ЭДО должно иметь свой индивидуальный ключ ЭП.

4.2.4. Любой Электронный документ должен быть зашифрован.

4.2.5. Полученный зашифрованный Электронный документ должен быть расшифрован, после чего проводится проверка ЭП.

4.2.6. Электронный документ принимается к дальнейшей обработке и исполнению только после положительного результата проверки ЭП.

4.3.7. Участниками ЭДО используются программное обеспечение, СКЗИ, а также ключи ЭП и ключи проверки ЭП и соответствующие сертификаты ключей, полученные от Организатора СЭД в порядке, установленном настоящими Правилами.

4.4. Порядок признания подлинника Электронного документа.

4.3.1. Все экземпляры Электронного документа, зафиксированные у Организатора СЭД и Участников ЭДО, являются подлинниками данного Электронного документа.

4.3.2. Подлинником Электронного документа считается документ с воспроизведенным содержанием и ЭП.

4.3.3. Подлинник Электронного документа не существует, если нет ни одного учтенного Организатором СЭД или Участником ЭДО экземпляра данного Электронного документа.

4.3.4. Подлинник Электронного документа не существует, если получение или восстановление экземпляра данного Электронного документа невозможно.

4.3.5. Подлинник Электронного документа не существует, если нет способа установить подлинность электронно-цифровой подписи.

4.3.6. Электронный документ не может иметь копий в электронном виде.

4.3.7. Электронный документ может иметь неограниченное количество экземпляров.

4.4. Порядок формирования копии Электронного документа на бумажном носителе.

4.4.1. Копии Электронного документа на бумажном носителе должны быть заверены собственноручной подписью Уполномоченного представителя Участника ЭДО или Организатора СЭД.

4.4.2. Копии Электронного документа на бумажном носителе должны содержать обязательную отметку, свидетельствующую о том, что это копия.

4.4.3. Информация, содержащаяся в копии Электронного документа на бумажном носителе, должна быть идентична информации, содержащейся в самом Электронном документе.

5. Особенности организации электронного документооборота

5.1. Этапы Электронного документооборота

ЭДО включает в себя следующие действия с Электронным документом:

- формирование Электронного документа;
- отправка Электронного документа;
- Доставка Электронного документа;
- проверка целостности Электронного документа;
- подтверждение о Доставке Электронного документа;
- отзыв Электронного документа;
- учет Электронных документов;
- ведение архива Электронных документов;
- создание дополнительных экземпляров Электронного документа;
- создание бумажных копий Электронного документа.

5.2. Порядок формирования Электронного документа и его регистрации.

5.2.1. Электронный документ составляется в соответствии с указанными в настоящих Правилах требованиями к Формализованным документам либо путем сканирования документов в бумажном виде.

5.2.2. Сформированный Электронный документ в обязательном порядке должен содержать указание на тип документа (Справка о стоимости чистых активов, Заявка на приобретение паев, Отчет агента и т.п.), дату документа, наименование инвестиционного фонда (если применимо), при наличии - номер документа (далее совместно именуемые Реквизиты электронного документа).

5.2.3. Сформированный Электронный документ подписывается ЭП и зашифровывается; дата и время подписи Электронного документа должны включаться в подписываемый Электронный документ.

5.3. Порядок отправки и Доставки электронного документа

5.3.1. Электронный документ отправляется Отправителем или лицом, уполномоченным на это Отправителем.

5.3.2. Участник ЭДО посредством специального программного модуля, предоставленного Организатором СЭД, подписывает документы ЭП и осуществляет их Шифрование.

5.3.3. Отправка Электронного документа Участником ЭДО или Организатором СЭД осуществляется посредством электронной почты стандартными программными средствами, в которых предусмотрена возможность генерировать и возвращать отправителю сообщения о получении письма, либо сообщения об ошибке при Доставке электронного документа в случае, если Электронный документ был отправлен, но не доставлен Получателю. Отправка электронного сообщения, а также подтверждения о получении Электронных документов, осуществляется с адреса электронной почты, указанного в Анкете.

5.3.4. Тема электронного сообщения с вложенным в него Электронным документом должна в обязательном порядке содержать тип Электронного документа.

5.3.5. Отправитель самостоятельно контролирует Доставку электронного сообщения Получателю. После отправки Электронного документа Участник ЭДО обязан удостовериться в отсутствии сбоев при Доставке. В случае сбоя при Доставке Электронный документ не считается отправленным, а Участник ЭДО должен повторить процедуру подготовки и/или отправки Электронного документа.

5.3.6. Полученный Электронный документ проверяется на целостность, т.е. его Доставку в неискаженном (по отношению к первоначальному) виде, путем расшифрования и обязательной проверки ЭП. Получателем также проверяется достоверность информации о дате и времени подписания и Шифрования Электронного документа.

5.3.7. В случае положительного результата проверок, указанных в пункте 5.3.6 настоящих Правил Электронный документ признается документом, равнозначным документу на бумажном носителе. В случае невозможности расшифрования Электронного документа, при отрицательном результате проверки целостности Электронного документа и подлинности ЭП или при выявлении явных несоответствий в информации о дате или времени подписания и Шифрования Электронного документа текущему времени/дате Электронный документ считается не полученным и не подлежит дальнейшей обработке и исполнению. В этом случае Получатель Электронного документа направляет по электронным каналам связи Электронное сообщение, подписанное ЭП, об ошибке при расшифровании или проверке целостности или подлинности ЭП Электронного документа с указанием Реквизитов электронного документа.

5.3.8. Участник ЭДО должен хранить все полученные и отправленные Электронные сообщения с файлом, содержащим Электронный документ, в течение сроков, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации для хранения соответствующих документов. Участник ЭДО должен принять меры по периодическому резервному копированию полученных и отправленных электронных сообщений с файлом, содержащим Электронный документ.

5.4. Порядок отзыва Электронного документа

5.4.1. Отправитель имеет право отозвать отправленный Электронный документ путем отправки Получателю Электронного документа, подписанного ЭП Отправителя, с уведомлением об отзыве.

5.4.2. В уведомлении об отзыве указывается основание отзыва Электронного документа, а также Реквизиты электронного документа.

5.4.3. Электронный документ может быть отозван только до начала его исполнения

Получателем.

5.4.4. Электронный документ считается отозванным после получения Отправителем подтверждения о получении отправленного уведомления об отзыве электронного документа.

5.5. Порядок учета Электронных документов

5.5.1. Участник ЭДО осуществляет учет Электронных документов путем ведения журнала учета входящих Электронных документов и журнала учета исходящих Электронных документов. Ведение учетных журналов осуществляется с использованием электронной базы данных с возможностью их формирования на бумажных носителях.

5.5.2. Запись в журнале учета входящих Электронных документов должна содержать:

- дата и время получения Электронного документа;
- тип документа;
- идентификатор Отправителя электронного документа;

5.5.3 Запись в журнале учета исходящих Электронных документов должна содержать:

- тип документа;
- идентификатор Отправителя электронного документа;
- идентификатор Получателя электронного документа;
- дата и время отправки электронного документа;

5.5.4 Организатор СЭД и Участники ЭДО обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения учетных данных, содержащихся в журналах учета Электронных документов.

5.6 Порядок подтверждения получения Электронного документа

5.6.1. В качестве подтверждения получения Электронного документа Получатель направляет Отправителю журнал учета входящих Электронных документов Получателя, полученных от Отправителя в текущем дне, подписанный ЭП Получателя, не реже чем раз в день не позднее 11:00 дня, следующего за днем, по состоянию на который составляется журнал. В случае несоответствия состава документов в журнале учета исходящих Электронных документов, переданных Получателю, с составом документов в журнале учета входящих документов Получателя, переданного в качестве подтверждения получения Электронных документов, Отправитель электронного документа выясняет причину несоответствия и при необходимости незамедлительно осуществляет повторную отправку Электронных документов

5.6.2. В случае получения электронного документа с уведомлением об отзыве, Получатель незамедлительно направляет Отправителю подтверждение о получении этого электронного документа с указанием информации об электронном документе, содержащейся в Журнале учета входящих документов.

5.6.3. Электронный документ считается не полученным, если электронный адрес Отправителя или Получателя не соответствует электронному адресу, указанному в Анкете.

5.7. Порядок ведения архива Электронных документов

5.7.1. Все Электронные документы, сформированные, отправленные и полученные Участниками ЭДО, хранятся в течение сроков, установленных действующим законодательством для соответствующих документов в бумажном виде. Электронные документы, для которых законодательством не установлены сроки их хранения, хранятся в

течение 5 (Пяти) лет.

5.7.2. Электронные документы должны храниться в формате, в котором они были получены.

5.7.3. В состав архивов должны входить Электронные документы с электронной подписью, сертификаты ключей проверки ЭП хранимых документов, электронные или бумажные журналы учета входящих и исходящих ЭД.

5.7.4. При ведении архива Электронных документов, Ключей ЭП и Сертификатов ключей ЭП реализуются принципы резервного копирования и восстановления информации.

5.7.5. Организатор СЭД и Участники ЭДО должны обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения архивных данных.

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГ ПО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ В СЭД ЗАО «Райффайзенбанк»

6.1. Общие положения.

6.1.1. В СЭД ЗАО «Райффайзенбанк» используются только сертифицированные ФСБ средства криптографической защиты информации (СКЗИ).

6.1.2. После подписания Участником ЭДО договора о присоединении к настоящим Правилам Организатор СЭД передает ему программное обеспечение, СКЗИ и Ключевые носители для целей использования только в СЭД ЗАО «Райффайзенбанк», а также обеспечивает ключевой информацией, необходимой для работы.

6.1.3. Программное обеспечение, СКЗИ и Ключевые носители, предоставляемые Участнику ЭДО, принадлежат Организатору СЭД и являются его собственностью.

6.1.4. Для обеспечения криптографической защиты информации в СЭД используются СКЗИ с открытым распределением Ключей. При этом каждый Уполномоченный представитель Участника ЭДО имеет свой Ключ ЭП, а также соответствующий ему Ключ проверки ЭП, который не является секретным и доступен другим участникам информационного обмена. При формировании Ключа ЭП с помощью специализированного программного обеспечения одновременно формируется соответствующий ему Ключ проверки ЭП. После издания в УЦ Криптографических ключей производится распечатка Сертификата ключа проверки ЭП, на которой имеются все атрибуты Ключа проверки ЭП. Подписанный Уполномоченным представителем Участника ЭДО и заверенный печатью Сертификат ключа проверки ЭП является документом, который подтверждает принадлежность Криптографического ключа Уполномоченному представителю Участника ЭДО. Один экземпляр Сертификата ключа проверки ЭП хранится в УЦ.

6.1.5. Для Шифрования информации Отправителю необходим только Ключ проверки ЭППолучателя информации. Для подписания документа необходим только собственный Ключ ЭП. Для расшифрования информации Получателем используется только собственный Ключ ЭП подписи Получателя. Для проверки подписи документа необходим только Ключ проверки ЭП Отправителя.

6.1.6. Реализованные в СКЗИ алгоритмы Шифрования и подписи гарантируют невозможность вычисления Ключа ЭП Отправителя из ЭП или из его Ключа проверки ЭП и позволяют установить факт изменения подписанного Электронного документа после момента его подписания, что обеспечивает целостность, подлинность и конфиденциальность переданной Отправителем информации.

6.1.7. Ключ ЭП Уполномоченного представителя Участника ЭДО находится только на Ключевом носителе, передаваемом Участнику ЭДО.

6.1.8. При работе в СЭД каждый Участник ЭДО использует необходимое количество действующих Криптографических ключей.

6.1.9. Порядок работы с Ключевыми носителями лиц, непосредственно работающих с СКЗИ, определяется самим Участником ЭДО с учетом настоящих Правил.

6.1.10.Ключевая информация, необходимая для работы СКЗИ в СЭД, вырабатывается Оператором Удостоверяющего центра (УЦ). Непосредственная генерация Криптографических ключей и запись их на носители производится также Оператором УЦ на «Автоматизированном рабочем месте (АРМ) Администратора УЦ».

6.1.11.Участник ЭДО обязуется выполнять указанные в настоящих Правилах требования порядка предоставления услуг по криптографической защите, порядка обеспечения информационной безопасности и общих требований к режиму эксплуатации СКЗИ, указанные в п.7 настоящих Правил.

6.1.12.Участник ЭДО обязуется выполнять требования эксплуатационной документации на СКЗИ.

6.1.13.По окончании срока действия договора о присоединении к настоящим Правилам или в случае его расторжения Участник ЭДО обязуется провести деинсталляцию установленного программного обеспечения и СКЗИ и вернуть Организатору СЭД полученные от него лицензии программного обеспечения и СКЗИ и Ключевые носители.

6.2. Порядок предоставления СКЗИ и передачи Криптографических ключей.

6.2.1. Порядок получения СКЗИ и регистрации Уполномоченного представителя Участника ЭДО в УЦ.

6.2.1.1. Для получения СКЗИ Участнику ЭДО необходимо оформить и предоставить Организатору ЭДО Заявку на предоставление программного обеспечения, СКЗИ и ключевых носителей (по форме, указанной в Приложении №6 к настоящим Правилам), а также доверенность на получение программного обеспечения, СКЗИ и ключевых носителей на Уполномоченного представителя Участника ЭДО (по форме, указанной в Приложении №7 к настоящим Правилам).

6.2.1.2. Под регистрацией понимается внесение регистрационной информации о физическом лице, являющемся Уполномоченным представителем Участника ЭДО и намеревающемся получить в УЦ Организатора ЭДО Ключ ЭП и Сертификат ключа проверки ЭП.

6.2.1.3. Регистрация уполномоченного представителя Участника ЭДО осуществляется на основании Заявления на регистрацию (по форме, указанной в Приложении № 8 к настоящим Правилам), составленного в двух экземплярах, при личном прибытии физического лица, проходящего процедуру регистрации в офис Организатора ЭДО.

6.2.1.4. Если Уполномоченный представитель Участника ЭДО не может прибыть в УЦ Организатора ЭДО лично, Заявление на регистрацию может быть принято от уполномоченного Участником ЭДО лица, прибывающего в УЦ лично и действующего на основании доверенности (по форме, указанной в Приложении № 9 к настоящим Правилам).

6.2.1.5. При проведении процедуры регистрации УЦ Организатора ЭДО вправе запросить документы, подтверждающие:

- место регистрации и адрес места жительства Уполномоченного представителя Участника ЭДО;
- сведения, необходимые для идентификации Уполномоченного представителя Участника ЭДО, а именно: фамилию, имя, отчество, наименование документа, удостоверяющего личность, номер этого документа, дату и место его выдачи;
- информацию о должности Уполномоченного представителя Участника ЭДО.

6.2.1.6. При положительном исходе идентификации Уполномоченного представителя Участника ЭДО по паспорту или иному документу, удостоверяющему личность, Оператор УЦ осуществляет регистрацию Уполномоченного Участника ЭДО.

6.2.1.7. При регистрации Уполномоченного представителя Участника ЭДО Оператор УЦ вносит специальную парольную фразу в соответствующий реестр УЦ Организатора ЭДО и передает ее в запечатанном конверте, выполняет действия по внесению иной регистрационной информации в реестры УЦ Организатора ЭДО.

6.2.2. Порядок передачи СКЗИ, изготовления и получения Криптографических ключей и Сертификатов ключа проверки электронной подписи.

6.2.2.1. Создание Ключа ЭП и Сертификата ключа проверкиЭП осуществляется УЦ Организатора ЭДО при личном прибытии Владельца Сертификата ключа ЭП в УЦ Организатора ЭДО на основании следующих документов:

- Заявления на получение Криптографических ключей (по форме, указанной в Приложении № 10 к настоящим Правилам), подаваемого в двух экземплярах;
- документа, подтверждающего права Уполномоченного представителя Участника ЭДО на подписание определенного типа информации: нотариально заверенной копии учредительных документов или доверенности, выданной на имя Уполномоченного представителя Участника ЭДО (по форме, указанной в Приложении №11 к настоящим Правилам), на подписание определенного типа информации в соответствии с Областью действия сертификатов криптографических ключей Пользователя (по форме, указанной в Приложении №12 к настоящим Правилам).

6.2.2.2. В случае если Владелец сертификата ключа подписи не может прибыть в УЦ Организатора ЭДО лично, Заявления на получение Криптографических ключей может быть принято от уполномоченного Участником ЭДО лица, прибывающего в УЦ Организатора ЭДО лично и действующего на основании доверенности (по форме, указанной в Приложении № 9 к настоящим Правилам).

6.2.2.3. Оператор УЦ выполняет идентификацию Владельца Сертификата ключа проверки ЭП (или иного должным образом уполномоченного лица) путем установления его личности по паспорту или иному документу, удостоверяющему личность.

6.2.2.4. При положительном исходе идентификации Оператор УЦ принимает документы, подтверждающие соответствующие полномочия, на рассмотрение.

6.2.2.5. УЦ может быть отказано в изготовлении Криптографических ключей и Сертификатов ключей проверки ЭП в следующих случаях:

- представление Заявления на получение Криптографических ключей, не соответствующего требованиям настоящего Порядка;
- несоответствие информации, указанной в Заявлении на получение Криптографических ключей, информации, содержащейся в документах, представленных вместе с Заявлением на получение Криптографических ключей;
- отсутствие соответствующих полномочий у лица, представившего Заявление на получение Криптографических ключей.

6.2.2.6. В случае отказа в изготовлении Криптографических ключей и Сертификатов ключей проверки ЭП Заявление на получение Криптографических ключей вместе с приложениями возвращается заявителю с отметкой УЦ Организатора ЭДО о причинах отказа.

6.2.2.7. При принятии положительного решения Оператор УЦ выполняет следующие действия:

- генерирует в соответствии с настоящим Порядком, ключевую пару Владельца

Сертификата ключа проверки ЭП;

- записывает ключевую пару в электронной форме на отчуждаемый Ключевой носитель;
- формирует в электронной форме запрос на выпуск Сертификата ключа проверки ЭП и передает Уполномоченному лицу УЦ для изготовления Сертификата ключа проверки ЭП.
- после изготовления Сертификата ключа проверки ЭПУполномоченным лицом УЦ Оператор УЦ записывает Сертификат ключа проверки ЭП в электронной форме на отчуждаемый носитель;
- изготавливает два бланка Сертификата ключа проверки ЭП (по форме, указанной в Приложении № 13 к настоящим Правилам). Все экземпляры бланка Сертификата ключа проверки ЭП на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру изготовления Криптографических ключей и Сертификатов ключей проверки ЭП (или собственноручной подписью его должным образом уполномоченного лица), а также собственноручной подписью Уполномоченного лица УЦ и печатью УЦ.

6.2.2.8. По окончании выполнения действий, указанных в пункте 6.2.2.7 настоящих Правил, Оператор УЦ выдает:

- Криптографические ключи на отчуждаемом Ключевом носителе по Акту формирования и передачи криптографических ключей (по форме, указанной в Приложении №14 к настоящим Правилам). Акт составляется в двух экземплярах по одному для каждой из сторон;
- Сертификат ключа проверки ЭП в электронной форме на отчуждаемом носителе электронной информации;
- один экземпляр бланка Сертификата ключа проверки ЭП;
- копию Сертификата ключа проверки ЭП Уполномоченного лица УЦ в электронном виде на отчуждаемом носителе информации;
- серийные номера лицензий программного обеспечения, СКЗИ, а также Ключевые носители по Акту приема - передачи программного обеспечения, СКЗИ и ключевых носителей (Приложение №15 к настоящим Правилам). Акт составляется в двух экземплярах по одному для каждой из сторон.

6.2.2.9. В течение 30 (тридцати) рабочих дней со дня передачи программного обеспечения, СКЗИ и криптографических ключей Участник ЭДО обязан:

- Осуществить инсталляцию и проверку работоспособности программного обеспечения и СКЗИ;
- установить новые Сертификаты ключей проверки ЭП в локальные хранилища сертификатов Участника ЭДО;
- произвести сверку параметров выданных Криптографических ключей с данными, указанными в Сертификатах ключей проверки ЭП;
- предоставить Организатору СЭД подписанный Акт о начале электронного документооборота (по форме, указанной в Приложении №3 к настоящим Правилам).

6.2.2.10. В случае нарушения условий пункта 6.2.2.9 настоящих Правил, а также отсрочки тестовой эксплуатации СЭД Участником ЭДО более чем на 30 (тридцать) дней, Акт о начале электронного документооборота подписывается Организатором ЭДО в одностороннем порядке.

6.2.2.11. По истечении срока действия документа, подтверждающего права Уполномоченного представителя Участника ЭДО на подписание определенного типа информации в СЭД, в случае непредоставления Участником ЭДО документа,

подтверждающего новые сроки полномочий Уполномоченного лица Участника ЭДО, Оператор УЦ блокирует Криптографический ключ Уполномоченного представителя Участника ЭДО и заносит серийный номер соответствующего ему открытого ключа в список отозванных сертификатов.

6.2.3. Плановая смена Криптографических ключей в СЭД

6.2.3.1. Плановая смена Криптографических ключей в СЭД производится один раз в год, поэтому срок действия Криптографических ключей при генерации устанавливается равным одному году.

6.2.3.2. О дате проведения Плановой смены ключей Оператор УЦ уведомляет Участников ЭДО путем направления электронного сообщения не позднее, чем за 10 (Десять) рабочих дней. Отправка такого электронного сообщения осуществляется по электронному адресу, указанному Участником ЭДО в Анкете Участника ЭДО.

6.2.3.3. Формирование и выдача Участнику ЭДО новых комплектов Криптографических ключей осуществляется Организатором СЭД в следующем порядке:

- Участник ЭДО должен направить Организатору СЭД Заявление на получение Криптографических ключей (по форме, указанной в Приложении №10 к настоящим Правилам) в соответствии с п. 6.2.2.1 настоящих Правил. Новые Криптографические ключи записываются на уже имеющиеся у Участника ЭДО Ключевые носители;
- порядок получения Криптографических ключей Участником ЭДО аналогичен порядку, изложенному в п. 6.2.2 настоящих Правил.

6.2.3.4. В течение 5 (пяти) рабочих дней со дня получения Ключевых носителей и Ключей проверки ЭП Участник ЭДО обязан установить новые Сертификаты ключей подписи в локальные хранилища сертификатов Участника ЭДО и произвести сверку параметров новых Криптографических ключей с данными, указанными в Сертификатах ключей проверки ЭП.

7. ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБЩИЕ ТРЕБОВАНИЯ К РЕЖИМУ ЭКСПЛУАТАЦИИ СКЗИ

7.1 Система обеспечения информационной безопасности при взаимодействии Организатора СЭД и Участников ЭДО

7.1.1. С целью защиты информации Организатор СЭД и Участники ЭДО применяют сертифицированное программное обеспечение:

- СКЗИ «КриптоПро CSP» производства ООО КриптоПРО;
- Программно-аппаратный комплекс «КриптоПРО УЦ» производства ООО КриптоПРО;
- Средство электронной подписи КриптоАРМ производства ООО «Цифровые технологии».

7.1.2. Удостоверяющий центр ПАК КриптоПро УЦ соответствует требованиям ФСБ России к информационной безопасности класса КС2 УЦ систем ЭДО, предназначенных для обработки информации, не содержащей сведений, составляющих государственную тайну, с применением средств электронной цифровой подписи.

7.1.3. Программа для Шифрования и электронной цифровой подписи «КриптоАРМ»

предназначена для защиты корпоративной информации, передаваемой по незащищенным каналам связи.

7.1.4. ПО КриптоАРМ предназначено для защиты корпоративной информации, передаваемой по незащищенным каналам связи и обеспечивает следующие функциональные возможности:

- Шифрование данных:
- Шифрование данных;
- расшифрование данных.
- Электронная подпись (ЭП):
- подпись данных;
- проверка корректности ЭП;
- добавление нескольких подписей к одному документу;
- заверение подписи подписью другого человека;
- два варианта ЭП (ЭП, отделенная от исходных данных и совмещенная с данными);
- расширенные свойства ЭП (время создания подписи, комментарий пользователя и др.).

7.1.5. Организатор ЭДО и Участники ЭДО осуществляют защиту информации, содержащей персональные данные и Конфиденциальную информацию в СЭД.

7.1.6. Соблюдение требований информационной безопасности при организации ЭДО обеспечивает:

- целостность и криптографическую защиту информации;
- защиту информации от несанкционированного доступа.

7.1.7. Система обеспечения информационной безопасности реализуется посредством применения программных средств и организационных мер.

7.1.8. К программным средствам относятся:

- программные средства, используемые для осуществления ЭДО;
- средства аутентификации;
- СКЗИ;
- средства обеспечения безотказной работы, включая антивирусные средства.

7.1.9. К организационным мерам относятся:

- размещение программных средств в помещении с контролируемым доступом;
- административные ограничения доступа к этим средствам;
- допуск только специально обученных и уполномоченных лиц;
- защита от повреждающих внешних воздействий (пожар и т.п.).

7.1.10. При создании ЭП Средства электронной подписи в Системе СЭД:

- показывают лицу, подписывающему Электронный документ, содержание информации, которую он подписывает;
- создают ЭП только после подтверждения лицом, подписывающим Электронный документ, операции по созданию ЭП;
- однозначно показывают, что ЭП создана.

7.1.11. При проверке ЭП Средства электронной подписи в Системе СЭД:

- показывают содержание Электронного документа, подписанного ЭП;
- показывают информацию о внесении изменений в подписанный ЭП Электронный документ;
- указывать на лицо, с использованием Ключа ЭП которого подписаны Электронные документы.

7.2. Требования к режиму эксплуатации СКЗИ и Криптографических ключей

7.2.1. Общие требования:

- учет и хранение Ключевых носителей и лицензионных ключей, непосредственная работа с ними поручается руководством Участника ЭДО специально выделенному работнику. Этот работник несет персональную ответственность за сохранность Криптографических ключей и лицензионных ключей;
- все поступающие для использования Криптографические ключи и лицензионные ключи должны браться в организации на поэкземплярный учет (регистрация их выдачи сотрудникам для работы, возврата и уничтожения) в выделенных для этих целей журналах;
- Ключевые носители с записанными на них Криптографическими ключами, лицензионные ключи СКЗИ и эксплуатационная документация должна храниться в хранилищах (металлических шкафах, сейфах, ячейках), оборудованных внутренними замками.

7.2.2. Требования по организационному обеспечению безопасности СКЗИ:

- руководством организации должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ (далее – Уполномоченные лица);
- вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководством организации с учетом эксплуатационной документации на СКЗИ;
- в организациях должны быть созданы условия, обеспечивающие сохранность Конфиденциальной информации, обрабатываемой с помощью СКЗИ, а также ключевой информации.

7.2.3. Требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ:

- размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее именуются Помещения), должны обеспечивать безопасность информации, СКЗИ и Криптографических ключей, сведение к минимуму возможности неконтролируемого доступа к СКЗИ неуполномоченными лицами;
- порядок допуска в помещения должен определяться внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации;
- размещение и установка СКЗИ осуществляется в соответствии с требованиями эксплуатационной документации на СКЗИ;
- Уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов.

7.3. Требования по обеспечению безопасности Криптографических ключей.

7.3.1. Криптографические ключи на Ключевых носителях должны храниться в индивидуальных хранилищах (сейфах, металлических шкафах, ячейках) владельцев записанных на них Криптографических ключей. В случае хранения Ключевых носителей в совместно используемых хранилищах, они должны храниться в опечатанном виде.

7.3.2. В случае отсутствия у сотрудника, работающего с СКЗИ, индивидуального хранилища Криптографические ключи по окончании рабочего дня должны

сдаваться лицу, ответственному за их хранение.

7.3.3. При нахождении Ключевых носителей вне сейфов, в процессе их использования владельцем записанных на них Криптографических ключей должны быть приняты меры, исключающие возможность несанкционированного доступа к Ключевым носителям.

7.3.4. При использовании Ключевого носителя не допускается:

- снимать несанкционированные копии с Ключевого носителя;
- разглашать содержимое Ключевого носителя;
- передавать Ключевой носитель кому-либо, не являющемуся уполномоченным руководством организации работником;
- выводить Ключи ЭП, записанные на Ключевом носителе на дисплей, принтер или другие внешние устройства отображения информации;
- вставлять Ключевой носитель в устройство считывания в режимах, не предусмотренных штатным режимом его работы;
- записывать на Ключевой носитель постороннюю информацию;
- вскрывать оболочку Ключевого носителя.

7.3.5. Ключи ЭП Владельцев сертификатов ключей ЭП записываются при их генерации на отчуждаемые носители ключевой информации.

7.3.6. В качестве отчуждаемых носителей ключевой информации используются только носители, указанные в документации на СКЗИ.

7.3.7. После использования СКЗИ ключевой материал не должен присутствовать в персональной электронно-вычислительной машине (далее - ПЭВМ).

7.4. Требования к сотрудникам, осуществляющим эксплуатацию и установку СКЗИ.

7.4.1. Руководством организации должны быть назначены сотрудники, ответственные за установку и эксплуатацию СКЗИ.

7.4.2. К работе с СКЗИ допускаются решением руководства организации только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию СКЗИ.

7.4.3. Руководитель организации или уполномоченное им лицо должен иметь представление о возможных угрозах при обработке, передаче и хранении информации, методах и средствах защиты информации.

7.5. Порядок действий при Компрометации Криптографических ключей

7.5.1. Порядок действий Сторон при Компрометации Криптографических ключей Участника ЭДО

7.5.1.1. К Компрометации Криптографических ключей относятся, включая, но не ограничиваясь, следующие случаи:

а. утрата (в том числе хищение) Ключевых носителей;
б. утрата Ключевого носителя с последующим обнаружением;
в. увольнение сотрудника или перевод на другой участок работы сотрудника, имевшего доступ к ключевой информации, с лишением его полномочий на использование ключевой информации;

г. нарушение правил хранения и уничтожения (после окончания срока действия) Ключа ЭП;
д. передача ключевой информации по линии связи в открытом виде;
е. возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
ж. нарушение печати на сейфе с Ключевыми носителями;
з. несанкционированное копирование Ключевых носителей;
и. случаи, когда нельзя достоверно установить, что произошло с Ключевыми носителями (в том числе случаи, когда Ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

7.5.1.2. Случаи с «а» по «г», указанные в пункте 7.5.1.1. Правил, относятся к явной Компрометации ключей. Случаи, с «д» по «и», указанные в пункте 7.5.1.1. Правил, и иные случаи Компрометации относятся к неявной Компрометации ключа и требуют специального рассмотрения Участником ЭДО в каждом конкретном случае.

7.5.1.3. При неявной Компрометации ключа, в случае если Участник ЭДО принимает решение о наличии факта Компрометации ключа, он действует в соответствии с пунктом 7.5.1.4 и пунктом 7.5.1.5 настоящих Правил. В противном случае Участник ЭДО продолжает использование Криптографического ключа.

7.5.1.4. При Компрометации криптографических ключей Участник ЭДО, являющийся Владельцем Сертификатов ключей проверки ЭП, прекращает обмен Электронными документами с использованием скомпрометированных Криптографических ключей.

7.5.1.5. В случае возникновения Компрометации Криптографических ключей Участник ЭДО обязан незамедлительно уведомить об этом Оператора УЦ для осуществления отзыва Сертификатов ключей проверки ЭП скомпрометированных Криптографических ключей. Для этого Уполномоченное лицо Участника ЭДО, указанное в Анкете Участника ЭДО, должно связаться с Оператором УЦ и назвать себя, назвать полное наименование организации Участника ЭДО, сообщить пароль и сообщить о факте Компрометации ключей. После этого Участник ЭДО обязан в течение одного рабочего дня предоставить Организатору СЭД письменное Заявление на аннулирование (отзыв) криптографических ключей (по форме, указанной в Приложении №16 к настоящим Правилам), оформленное в двух экземплярах и заверенное собственноручной подписью Владельца Сертификата Ключа проверки ЭП и (или) подписью единоличного исполнительного органа соответствующего Участника ЭДО.

7.5.1.6. Датой и временем Компрометации криптографических ключей считается дата и время получения Организатором СЭД Уведомления о факте Компрометации криптографических ключей.

7.5.1.7. При получении Электронного документа, подписанного отозванным (аннулированным) Ключом ЭП данный электронный документ считается неполученным.

7.5.1.8. Криптографический ключ считается отозванным (аннулированным) с даты занесения серийного номера соответствующего ему Ключа проверки ЭП в список отозванных сертификатов.

7.5.1.9. Получив сообщение о факте Компрометации криптографических ключей Участника ЭДО, Уполномоченное лицо УЦ должно убедиться в его достоверности в соответствии с пунктом 7.4.1.2. и незамедлительно заблокировать Криптографические ключи Участника ЭДО в СЭД (пометить их как скомпрометированные).

7.5.1.10. Организатор СЭД предоставляет Участнику ЭДО новый Криптографический ключ в соответствии с порядком, указанным в п. 6.2 настоящих Правил после получения от Участника ЭДО всех документов, необходимых для выпуска нового Криптографического ключа. Новый Криптографический ключ записывается на уже имеющийся у Участника ЭДО Ключевой носитель.

7.5.1.11. Криптографический ключ записывается на новый Ключевой носитель в случае невозможности использования ранее переданных Участнику ЭДО Ключевых носителей (включая, но не ограничиваясь, случаями утраты ключевого носителя, выхода из строя Ключевого носителя).

7.5.1.12. Организатор СЭД предоставляет Участнику ЭДО Криптографический ключ, записанный на новый Ключевой носитель, в соответствии с порядком, указанным в п. 6.2 настоящих Правил, после получения от Участника ЭДО всех документов, необходимых для выпуска нового Криптографического ключа и получения нового Ключевого носителя.

7.5.2. Порядок действий Сторон при Компрометации ключей Уполномоченного лица УЦ

7.5.2.1 В случае Компрометации Криптографических ключей Уполномоченного лица УЦ работа СЭД приостанавливается на срок, необходимый для формирования новых Криптографических ключей Уполномоченного лица УЦ и выдачи Участникам ЭДО новых Криптографических ключей.

7.5.2.2 Оповещение Участников ЭДО производится путем уведомления Уполномоченных лиц Участников ЭДО, указанных в Анкетах.

8. СИСТЕМА МЕР УПРАВЛЕНИЯ РИСКАМИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

8.1. Виды рисков, связанных с осуществлением ЭДО в рамках СЭД

8.1.1. Правовые риски – риски возникновения конфликтных ситуаций, вызванных правовой неурегулированностью вопросов применения ЭП и отношений Участников ЭДО.

8.1.2. Организационные риски – риски необеспечения (ненадлежащего обеспечения) ЭДО вследствие неэффективности СЭД.

8.1.3. Технологические риски – риски необеспечения (ненадлежащего обеспечения) порядка осуществления ЭДО вследствие неэффективности и/или неадекватности технологий, порядка и способов осуществления ЭДО.

8.1.4. Операционные риски – риски возникновения нарушений при осуществлении ЭДО вследствие ненадлежащих действий сотрудников, ненадлежащего функционирования используемых СКЗИ и иного аппаратно-программного обеспечения.

8.1.5. Криминальные риски – риски совершения сотрудниками Участников ЭДО, иными лицами, умышленных действий в целях неправомерного получения и использования Конфиденциальной информации, связанной с осуществлением ЭДО, а также нарушения деятельности Участников ЭДО.

8.1.6. Форс-мажорные риски – риски нарушения деятельности Участников ЭДО, целостности СЭД, вследствие возникновения непредотвратимых (форс-мажорных) чрезвычайных ситуаций техногенного, природного и социального характера.

8.2. Меры снижения правовых рисков, связанных с осуществлением ЭДО**,** применяемые в СЭД **(**с указанием ответственной стороны**)**

8.2.1. Обеспечение соответствия СКЗИ, используемых при осуществлении ЭДО, требованиям законодательства Российской Федерации (Организатором СЭД).

8.2.2. Обеспечение признания Участниками ЭДО равнозначности ЭЦП и собственноручной подписи (Организатором СЭД).

8.2.3. Установление подлинности ЭП (Организатором СЭД).

8.2.4. Установление порядка разрешения конфликтов, связанных с использованием ЭДО (Организатором СЭД).

8.3. Меры снижения организационных рисков ЭДО**,** применяемые в СЭД **(**с указанием ответственной стороны**)**

8.3.1. Установление прав и обязанностей Участников ЭДО, связанных с осуществлением ЭДО (Организатором СЭД).

8.3.2. Установление функциональных обязанностей подразделений Организатора СЭД, принимающих участие в осуществлении ЭДО (Организатором СЭД).

8.4. Меры снижения технологических рисков ЭДО**,** применяемые в СЭД **(**с указанием ответственной стороны**)**

8.4.1. Установление требований к назначению и составу СКЗИ, используемых при осуществлении ЭДО (Организатором СЭД).

8.4.2. Обеспечение использования Участниками ЭДО СКЗИ при осуществлении ЭДО (Организатором СЭД).

8.4.3. Обеспечение однозначной идентификации Владельца сертификата ключа подписи, уникальности регистрационной информации о Владельце сертификата ключа подписи (Организатором СЭД).

8.4.4. Обеспечение Участниками ЭДО и Организатором СЭД целостности СЭД, регистрации отправленных и полученных Электронных документов, хранению оправленных и полученных Электронных документов.

8.4.5. Установление требований к порядку осуществления ЭДО Участниками ЭДО (Организатором СЭД).

8.4.6. Обеспечение исполнения требований к форматам и реквизитам электронного документа электронного документа (Организатором СЭД).

8.4.7. Определение порядка действий Участников ЭДО (Организатором СЭД) по формированию, Доставке электронного документа, а также его отзыву.

8.4.8. Определение порядка действий Участников ЭДО (Организатором СЭД) по проверке действительности и области действия ЭП, подлинности, целостности электронного документа и его соответствия установленным форматам.

8.5. Меры снижения операционных рисков ЭДО, применяемые в СЭД

8.5.1. Разделение полномочий и служебных обязанностей сотрудников Участников ЭДО и Организатора СЭД, участвующих в осуществлении ЭДО.

8.5.2. Осуществление контроля за надлежащим исполнением сотрудниками Участников ЭДО и Организатора СЭД своих служебных обязанностей, связанных с осуществлением ЭДО.

8.5.3. Определение порядка выявления ошибок (ошибочных действий), совершенных сотрудниками Участников ЭДО и Организатора СЭД и порядка их устранения.

8.5.4. Установление квалификационных требований к сотрудникам (руководителям подразделений) Участников ЭДО и Организатора СЭД, участвующих в осуществлении ЭДО.

8.5.5. Определение порядка обнаружения и устранения отказов, сбоев, нарушений работы СКЗИ, используемых Участниками ЭДО при осуществлении ЭДО.

8.5.6. Установление требований к техническому сопровождению, замене вышедших из

строя СКЗИ Участников ЭДО (Организатором СЭД).

8.6. Меры снижения криминальных рисков ЭДО**,** применяемые в СЭД **(**с указанием ответственной стороны**)**

8.6.1. Установление требований (Организатором СЭД) по обеспечению Участниками ЭДО защиты Конфиденциальной информации, связанной с осуществлением ЭДО, от несанкционированного доступа.

8.6.2. Установление требований (Участником ЭДО) по обеспечению Владельцами Сертификатов ключей проверки ЭП сохранности в тайне Ключей ЭП.

8.6.3. Определение порядка действий Владельцев Сертификатов ключей проверки ЭП (Организатором СЭД, Участниками ЭДО) в случае Компрометации Ключей ЭП.

8.6.4. Определение порядка (Организатором СЭД) расследования случаев неправомерного предоставления и/или использования Конфиденциальной информации, неисполнения (ненадлежащего исполнения) своих служебных обязанностей сотрудниками Участников ЭДО и Организатора СЭД.

8.7. Меры снижения форс-мажорных рисков ЭДО, применяемые в СЭД

8.7.1. Обеспечение Участниками ЭДО и Организатором СЭД целостности ЭДО, защиты Конфиденциальной информации, связанной с осуществлением ЭДО, в случае возникновения чрезвычайных ситуаций.

8.7.2. Определение порядка действий сотрудников Участников ЭДО и Организатора СЭД в случае возникновения чрезвычайных ситуаций.

8.7.3. Применение Участниками ЭДО и Организатором СЭД резервных источников питания, систем бесперебойного питания, средств безаварийного завершения работы.

8.7.4. Применение Участниками ЭДО и Организатором СЭД средств защиты от поражения компьютерными вирусами и вредоносными программами.

8.9. Компенсационные инструменты, применяемые для покрытия убытков от реализации рисков ЭДО.

8.9.1. Собственные средства Участников ЭДО и Организатора СЭД.

8.10. Управление рисками электронного документооборота.

8.10.1. Ответственным за управление рисками ЭДО в СЭД является Организатор СЭД.

8.10.2. Основными функциями Организатора СЭД в области управления рисками ЭДО являются:

- анализ текущей и планируемой деятельности Организатора СЭД с целью выявления новых рисков ЭДО, установление источников и причин их реализации, оценка последствий реализации выявленных рисков;
- контроль за практическим применением Организатором СЭД мер, препятствующих реализации рисков ЭДО;
- мониторинг событий, способных привести к реализации рисков ЭДО, анализ эффективности применяемых Организатором СЭД способов снижения рисков;
- расследование случаев реализации рисков ЭДО, установление причин несрабатывания, применяемых Организатором СЭД способов снижения рисков;

- оценка эффективности сформированных Организатором СЭД компенсационных инструментов, применяемых при покрытии убытков, в случае реализации рисков ЭДО;
- разработка предложений по повышению эффективности системы мер снижения рисков ЭДО.

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТОВ

9.1. Возникновение конфликтов

9.1.1. В случае возникновения конфликтов при использовании Электронных документов в СЭД, в частности, спора между Участниками ЭДО в отношении Авторства электронных документов, подлинности или целостности Электронных документов, подписанных ЭП, применяется порядок разрешения конфликтов, предусмотренный настоящими Правилами.

9.1.2. При возникновении конфликта Участник ЭДО, оспаривающий подлинность, целостность или Авторство Электронного документа в СЭД, извещает Организатора СЭД об этом событии любым способом, позволяющим однозначно установить Отправителя.

9.2.. Порядок разрешения конфликтных ситуаций, связанных с получением или неполучением Электронного документа, подписанного ЭП.

9.2.1. При возникновении между Участниками ЭДО (далее - Стороны) конфликтов и разногласий, связанных с не поступлением Электронного документа подписанного ЭП, поступлением документа подписанного ЭП с отрицательным результатом проверки Стороны создают комиссию для претензионного урегулирования спорной ситуации. Комиссия создается по инициативе одной из Сторон в течение четырнадцати календарных дней с даты уведомления официальным письмом инициирующей создание данной комиссии стороной вторую сторону о необходимости претензионного урегулирования спорной ситуации.

9.2.2. В состав комиссии должно входить равное количество представителей от каждой из Сторон. Состав комиссии должен быть зафиксирован в Акте, который является итоговым документом, отражающим результаты работы комиссии. Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке. Срок работы комиссии составляет не более пяти рабочих дней. При необходимости этот срок может быть увеличен до одного месяца.

9.2.3. Стороны способствуют работе комиссии и не допускают отказа от предоставления необходимых документов.

9.2.4. Комиссия определяет корректность или некорректность ЭП спорного Электронного документа с помощью процедуры технической экспертизы, которая проводится в соответствии с нижеследующим порядком:

9.2.5. Комиссия получает и устанавливает необходимое для работы программное обеспечение.

9.2.6. Стороны предъявляют комиссии:

- свою электронную архивную копию спорного Электронного документа с ЭП;
- свою электронную архивную копию Ключа проверки ЭП, предназначенного для проверки ЭП спорного Электронного документа;
- свою архивную копию распечатки Сертификата ключа проверки ЭП, заверенную

обеими Сторонами;

- свой экземпляр Уведомления об отмене действия ключа ЭП (при наличии);

9.2.7. В случае не предъявления комиссии одной из Сторон какого-либо из вышеперечисленных документов к рассмотрению принимается экземпляр указанного документа, представленный другой Стороной.

9.2.8. Комиссия устанавливает идентичность значений электронной архивной копииКлюча проверки ЭП, с помощью которого проверялась ЭП спорного Электронного документа, архивной копии распечатки соответствующего Сертификата ключа проверки ЭП.

9.2.9. В случае неидентичности хотя бы одного из значений указанного Ключа проверки ЭП ЭП спорного Электронного документа признается некорректной и процедура технической экспертизы считается завершенной.

9.2.10. В случае наличия Заявления на аннулирование (отзыв) криптографических ключей, предназначенного для проверки ЭП спорного Электронного документа, комиссия устанавливает идентичность значений Ключа проверки ЭП, которые содержатся в электронной архивной копии Ключа ЭП и в архивной копии Заявления на аннулирование (отзыв) криптографических ключей, а также дату отзыва (аннулирования) Ключа ЭП и дату регистрации этого заявления. В случае идентичности указанных значений Ключа проверки ЭПи если Электронный документ подписан ЭП позже даты отзыва (аннулирования) ключа и даты регистрации Заявления на аннулирование (отзыв) криптографических ключей, ЭП спорного Электронного документа признается некорректной и процедура технической экспертизы считается завершённой.

9.2.11. Комиссия с помощью соответствующего программного обеспечения криптографической защиты производит проверку ЭП копии спорного Электронного документа с использованием электронной архивной копии Ключа проверки ЭП. После установления комиссией корректности или некорректности ЭП спорного Электронного документа процедура технической экспертизы считается завершённой.

9.2.12. По итогам работы комиссии составляется Акт, в котором в обязательном порядке отражаются:

- установленные обстоятельства;
- действия членов комиссии;
- выводы комиссии;
- основания для формирования выводов.

9.2.13. Составленный комиссией Акт утверждается Сторонами и является основанием для принятия Сторонами окончательного решения в рамках претензионного урегулирования спорной ситуации. Акт составляется в необходимом количестве экземпляров по одному для каждой из сторон.

9.2.14. В случае если Стороны в рамках претензионного урегулирования спорной ситуации пришли к взаимоприемлемому соглашению, то они в течение четырнадцати календарных дней с даты окончания работы комиссии составляют соответствующий двусторонний Акт, условия которого являются обязательными для выполнения каждой из Сторон.

9.2.15. В случае если Стороны в рамках претензионного урегулирования спорной ситуации не пришли к взаимоприемлемому соглашению, то заинтересованная Сторона вправе обратиться в суд и в качестве доказательства в судебном споре обязана представить Акт, составленный в соответствии с настоящим Порядком. Представленный в суд Акт имеет равную силу с другими доказательствами, представленными Сторонами.

9.3. Согласительный порядок разрешения конфликтов

9.3.1. Все конфликтные ситуации, которые могут возникнуть в связи с применением, нарушением, толкованием настоящих Правил, признанием недействительными настоящих Правил или их части, Стороны будут стремиться разрешить путем переговоров.

9.3.2. В случае, если конфликтная ситуация не урегулирована в процессе переговоров и конфликтная ситуация содержит признаки дисциплинарных нарушений, стороны вправе обратиться в Дисциплинарный Комитет ПАРТАД, для разрешения конфликтной ситуации в соответствии с Кодексом мер дисциплинарного воздействия ПАРТАД.

10. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ НАСТОЯЩИХ ПРАВИЛ ДЛЯ ВСЕХ УЧАСТНИКОВ ЭДО

10.1. Настоящие Правила прекращают свое действие на основании решения исполнительного органа Организатора СЭД.

10.2. Прекращение действия настоящих Правил и приложений к ним не влияет на юридическую силу и действительность Электронных документов, которыми Организатор СЭД и Участники ЭДО обменивались до прекращения действия настоящих Правил и приложений к ним.

11. ПРИЛОЖЕНИЯ

- Приложение № 1 Договор о присоединении к Правилам ЭДО ЗАО «Райффайзенбанк»
- Приложение № 2 Форматы электронных документов, используемые в системе электронного документооборота ЗАО «Райффайзенбанк»
- Приложение № 3 Акт о начале электронного документооборота
- Приложение № 4 Анкета Участника ЭДО
- Приложение № 5 Анкета Организатора СЭД
- Приложение № 6 Заявка на предоставление программного обеспечения, СКЗИ и ключевых носителей
- Приложение № 7 Доверенность (на получение программного обеспечения, СКЗИ и Ключевых носителей)
- Приложение № 8 Заявление на регистрацию Пользователя в Удостоверяющем центре
- Приложение № 9 Доверенность (на передачу заявлений Пользователя УЦ и получение Криптографических ключей)
- Приложение № 10 Заявление на получение Криптографических ключей
- Приложение № 11 Доверенность (подписание документов ЭП в СЭД)
- Приложение № 12 Область действия Сертификатов криптографических ключей пользователя
- Приложение № 13 Сертификат ключа проверки ЭП
- Приложение № 14 Акт формирования и передачи Криптографических ключей
- Приложение № 15 Акт приема-передачи программного обеспечения, СКЗИ и Криптографических ключей»
- Приложение № 16 Заявление на аннулирование (отзыв) Криптографических ключей