

УТВЕРЖДЕНЫ
Приказом
Общества с ограниченной
ответственностью "РБРУ
Специализированный депозитарий"
№ 17
от 01.11.2022г.

**ПРАВИЛА ЭЛЕКТРОННОГО
ДОКУМЕНТООБОРОТА
Общества с ограниченной ответственностью
"РБРУ Специализированный депозитарий"**

ВЕРСИЯ 1.0

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ	3
2. СПИСОК ТЕРМИНОВ, ОПРЕДЕЛЕНИЙ, СОКРАЩЕНИЙ	4
3. ПОРЯДОК ДОПУСКА УЧАСТНИКА ЭДО К ОСУЩЕСТВЛЕНИЮ ДОКУМЕНТООБОРОТА В СЭД.....	7
4. ОСОБЕННОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТА	8
5. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА	9
6. ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБЩИЕ ТРЕБОВАНИЯ К РЕЖИМУ ЭКСПЛУАТАЦИИ СКЗИ	12
7. СИСТЕМА МЕР УПРАВЛЕНИЯ РИСКАМИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА.....	16
8. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТОВ.....	18
9. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ НАСТОЯЩИХ ПРАВИЛ ДЛЯ ВСЕХ УЧАСТНИКОВ ЭДО	20
10. СПИСОК ПРИЛОЖЕНИЙ	21

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила электронного документооборота Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий" (далее именуемые Правила), а также Приложения к ним определяют общий порядок и принципы осуществления электронного документооборота между Обществом с ограниченной ответственностью "РБРУ Специализированный депозитарий" (далее именуется Организатор СЭД) и лицами, присоединившимися к системе электронного документооборота Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий" (далее именуемые Участники ЭДО или Участник ЭДО).

1.2. Настоящие Правила разработаны в соответствии с требованиями Федерального закона от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 6 апреля 2011 года №63-ФЗ «Об электронной подписи», а также другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

1.3. Настоящие Правила становятся обязательными для Участника ЭДО с момента заключения между Участником ЭДО и Организатором СЭД Договора о присоединении к Правилам ЭДО Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий" (по форме, указанной в Приложении №1 к Правилам) (далее именуется Договор).

Документы в электронной форме, обмен которыми осуществляется в системе электронного документооборота Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий" (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», «.pdf», «.tiff» (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, полученные в Аккредитованном Минкомсвязью РФ Удостоверяющем центре (далее УЦ). Все действия по приобретению и установке СКЗИ участник ЭДО выполняет самостоятельно.

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

1.6. Настоящие Правила, включая все Приложения, утверждаются Организатором СЭД и вступают в силу с момента утверждения, если иное не установлено 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 на официальном сайте Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий" информационно-телекоммуникационной сети «Интернет» по адресу: <http://rbu-depository.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 <http://rbu-depository.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
Аккредитованный Минкомсвязью РФ Удостоверяющий центр (УЦ)	Юридическое лицо, осуществляющее функции по созданию и выдаче Сертификатов ключей проверки Усиленной Квалифицированной ЭП, а также иные функции, предусмотренные Федеральным законом № 63-ФЗ «Об электронной подписи»
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)
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

**ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "РБРУ
СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ", ВЕРСИЯ 1.0**

Термин/ Сокращение	Определение
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
Организатор системы электронного документооборота (Организатор СЭД)	Общество с ограниченной ответственностью "РБРУ Специализированный депозитарий"
Отправитель электронного документа (Отправитель)	Лицо, которое, или от имени которого, направляется электронный документ
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 проверки ЭП)	Электронный документ или документ на бумажном носителе, выданные Участнику ЭДО удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи Владельцу Сертификата ключа проверки электронной подписи
Система электронного документооборота Общества с ограниченной ответственностью "РБРУ"	Совокупность правил, организационных мер и программно-технических средств, включая средства криптографической защиты информации, реализованная в рамках взаимодействия Организатора СЭД с Участниками ЭДО в целях осуществления электронного документооборота и являющаяся корпоративной информационной системой.

**ПРАВИЛА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "РБРУ
СПЕЦИАЛИЗИРОВАННЫЙ ДЕПОЗИТАРИЙ", ВЕРСИЯ 1.0**

Термин/ Сокращение	Определение
Специализированный депозитарий" (СЭД)	
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
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
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, осуществляющее обмен информацией в электронной форме в качестве отправителя и/или получателя электронных документов и заключившее договор о присоединении к Правилам электронного документооборота Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий"
Форматы электронных документов	Утвержденные Организатором СЭД форматы электронных документов, используемые в СЭД
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 — Усиленная Квалифицированная электронная подпись как она определена действующим законодательством Российской Федерации
Электронный	Документ, отвечающий в совокупности следующим требованиям:

Термин/ Сокращение	Определение
документ (Документ)	<ul style="list-style-type: none">· 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 Организатором СЭД 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 СКЗИ на свои программно-технические средства приобретенного за свой счет в Аккредитованном Минкомсвязью Удостоверяющем Центре, который выпускает ЭП, используя СКЗИ КриптоПро CSP. Инсталляция производится сотрудником Участника ЭДО.

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 Приложениях №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.

4. ОСОБЕННОСТИ ЭЛЕКТРОННОГО ДОКУМЕНТА

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

4.1.1. Электронный документ, сформированный в рамках СЭД, имеет юридическую силу бумажного документа и влечет предусмотренные для данного документа правовые последствия в случае его надлежащего оформления в соответствии с настоящими Правилами. Любое вложение в Электронный документ, в том числе скан-образ, также признаются Сторонами Электронными документами.

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. Участники ЭДО, 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, подтверждают, что:

- Участники ЭДО обладают соответствующими документами в бумажном виде, а сведения в передаваемых специализированному депозитарию Электронных документах полностью соответствуют сведениям, содержащимся в документах, оформленных в бумажном виде;
- Участники ЭДО осуществили все необходимые проверки (достоверность принимаемых ими 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.);
- на всех документах, принятых от заявителя, имеются необходимые отметки, заверенные печатью и подписью уполномоченного представителя Участников ЭДО.

4.1.7. В случае передачи Электронного документа исключительно в соответствии с Форматами электронных документов, Участники ЭДО гарантируют корректность оформления соответствующего документа на бумажном носителе, в том числе заполнение всех обязательных полей в документе, наличие подписи и образца подписи и т.д.

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.

4.2. 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, 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.

4.2.7. Участниками ЭДО используются программное обеспечение, СКЗИ, а также ключи ЭП и ключи проверки ЭП и соответствующие Сертификаты ключей, полученные от Аккредитованного Минкомсвязью Удостоверяющего Центра.

4.3. 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 электронной 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. 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;
- подписание ЭП Электронного документа;
- отправка Электронного документа;

- доставка Электронного документа;
- проверка подлинности и целостности Электронного документа;
- подтверждение получения Электронного документа Участником ЭДО;
- 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 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 содержит следующие сведения:

- дата и время получения Электронного документа;
- отправитель;
- получатель;
- тема электронного сообщения.

5.5.3 Запись в журнале учета исходящих Электронных документов содержит следующие сведения:

- дата и время отправления Электронного документа;
- отправитель;

- получатель;
- тема электронного сообщения.

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 ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОБЩИЕ ТРЕБОВАНИЯ К РЕЖИМУ ЭКСПЛУАТАЦИИ СКЗИ

6.1 Система обеспечения информационной безопасности при взаимодействии Организатора СЭД и Участников ЭДО.

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

- СКЗИ «Крипто ПРО CSP» производства ООО «КриптоПРО»;
- Средство электронной подписи «КриптоАРМ» производства ООО «Цифровые технологии».

6.1.2. СКЗИ «КриптоПро CSP» с открытым распределением Ключей используются для обеспечения криптографической защиты информации в СЭД. 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.

6.1.3. 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.

6.1.4. 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.).

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

6.1.6. Соблюдение требований информационной безопасности при организации ЭДО обеспечивает:

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

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

6.1.8. К программным средствам относятся:

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

6.1.9. 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.).

6.1.10. 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.

6.1.11. 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;
- указывают на лицо, с использованием Ключа ЭП которого подписаны Электронные документы.

6.2. Требования к режиму эксплуатации СКЗИ и Криптографических ключей.

6.2.1. Общие требования:

- учет Ключевых носителей и хранение лицензионных ключей, непосредственная работа с Ключевыми носителями поручается руководством Участника ЭДО специально назначенным работникам. Эти работники несут 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.

6.2.2. 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.

6.2.3. 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 именуется 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.

6.3. Требования по обеспечению безопасности Криптографических ключей.

6.3.1. 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.

6.3.2. В случае отсутствия у сотрудника, работающего с СКЗИ, индивидуального хранилища Криптографические ключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

6.3.3. 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.

6.3.4. 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.

6.5. Порядок действий при Компрометации Криптографических ключей.

6.5.1. Порядок действий Сторон при Компрометации Криптографических ключей Участника ЭДО.

6.5.1.1. В случае возникновения Компрометации Криптографических ключей Участник ЭДО обязан незамедлительно уведомить об этом УЦ в соответствии с регламентом УЦ для осуществления отзыва Сертификатов ключей проверки ЭП скомпрометированных Криптографических ключей. После этого Участник ЭДО обязан в течение одного рабочего дня направить Организатору СЭД по электронной почте, указанной в Анкете, Уведомление о факте Компрометации криптографических ключей.

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

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

6.5.1.4. В случае Компрометации Криптографических ключей Участника ЭДО работа Участника ЭДО приостанавливается на срок, необходимый для формирования новых Криптографических ключей в этом или ином УЦ.

7. СИСТЕМА МЕР УПРАВЛЕНИЯ РИСКАМИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

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

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

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

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

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

7.1.5. 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.

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

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

7.2.1. Обеспечение соответствия СКЗИ, используемых при осуществлении ЭДО, требованиям законодательства Российской Федерации (Организатор СЭД, участник ЭДО).

7.2.2. Обеспечение признания Участниками ЭДО равнозначности ЭЦП и собственноручной подписи (Организатор СЭД).

7.2.3. Установление подлинности ЭП (Организатор СЭД, участник ЭДО).

7.2.4. Установление порядка разрешения конфликтов, связанных с использованием ЭДО (Организатор СЭД).

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

7.3.1. Установление прав и обязанностей Участников ЭДО, связанных с осуществлением ЭДО (Организатор СЭД).

7.3.2. Установление функциональных обязанностей подразделений Организатора СЭД, принимающих участие в осуществлении ЭДО (Организатор СЭД).

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

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

7.4.2. Обеспечение использования Участниками ЭДО СКЗИ при осуществлении ЭДО (Организатор СЭД, участник ЭДО).

7.4.3. Обеспечение Участниками ЭДО и Организатором СЭД целостности СЭД, регистрации отправленных и полученных Электронных документов, хранению отправленных и полученных Электронных документов (Организатор СЭД, участник ЭДО).

7.4.4. Установление требований к порядку осуществления ЭДО Участниками ЭДО (Организатор СЭД).

7.4.5. Обеспечение исполнения требований к форматам и реквизитам электронного документа электронного документа (Организатор СЭД).

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

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

7.5. Меры снижения операционных рисков ЭДО, применяемые в СЭД.

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

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

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

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

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

7.5.6. Установление требований к техническому сопровождению, замене вышедших из строя СКЗИ Участников ЭДО.

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

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

7.6.2. Определение порядка действий Владельцев Сертификатов ключей проверки ЭП в случае Компрометации Ключей ЭП (Организатор СЭД).

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

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

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

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

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

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

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

7.8.1. Собственные средства Участников ЭДО и Организатора СЭД.

7.9. Управление рисками электронного документооборота.

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

7.9.2. 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.

8. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТОВ

8.1. Возникновение конфликтов.

8.1.1. 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.

8.1.2. 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.

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

8.2.1. 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 иницилирующей создание данной комиссии стороной второй стороны о необходимости претензионного урегулирования спорной ситуации.

8.2.2. 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.

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

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

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

8.2.6. 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;
- свой экземпляр Уведомления об отмене действия ключа ЭП (при наличии);

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

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

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

8.2.10. В случае наличия Заявления на аннулирование (отзыв) криптографических ключей, предназначенного для проверки ЭП спорного Электронного документа, комиссия обращается в УЦ, выдавший сертификат, за подтверждением статусов сертификатов и дат отзыва (аннулирования) криптографических ключей. В случае идентичности указанных значений Ключа проверки ЭП и, 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 завершенной.

8.2.11. 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 завершенной.

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

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

8.2.13. 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.

8.2.14. 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.

8.2.15. 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.

8.3. Согласительный порядок разрешения конфликтов.

8.3.1. 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. Сторона, права которой нарушены, вправе направить претензию другой Стороне (Сторонам). Сторона (Стороны), получившая претензию, обязана(ы) ответить на неё в срок, не превышающий 10 (Десять) рабочих дней с момента её получения.

8.3.2. Если по итогам проведения переговоров конфликтная ситуация, спор или разногласие остается полностью или частично неурегулированными, Стороны вправе передать неурегулированный спор и разногласия для рассмотрения в суд в соответствии с законодательством Российской Федерации.

9. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ НАСТОЯЩИХ ПРАВИЛ ДЛЯ ВСЕХ УЧАСТНИКОВ ЭДО

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

9.2. 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.

10. СПИСОК ПРИЛОЖЕНИЙ

- Приложение №1 Договор о присоединении к Правилам ЭДО Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий"
- Приложение №2 Форматы электронных документов, используемые в системе электронного документооборота Общества с ограниченной ответственностью "РБРУ Специализированный депозитарий"
- Приложение №3 Акт о начале электронного документооборота
- Приложение №4 Анкета Участника ЭДО
- Приложение №5 Анкета Организатора СЭД